

RSA-OAEP IND-CCA2 증명

김동현(wlswudpdlf31@kookmin.ac.kr)

March 18, 2025

Contents

1	논문정보	2
2	보안 개념	3
2.1	OW trapdoor permutation	3
2.2	Partial-domain OW trapdoor permutation	3
2.3	Set partial-domain OW trapdoor permutation	4
2.4	IND security against CCA2	4
2.5	IND security against CCA2 in ROM	5
3	RSA-OAEP	6
4	증명	6

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.

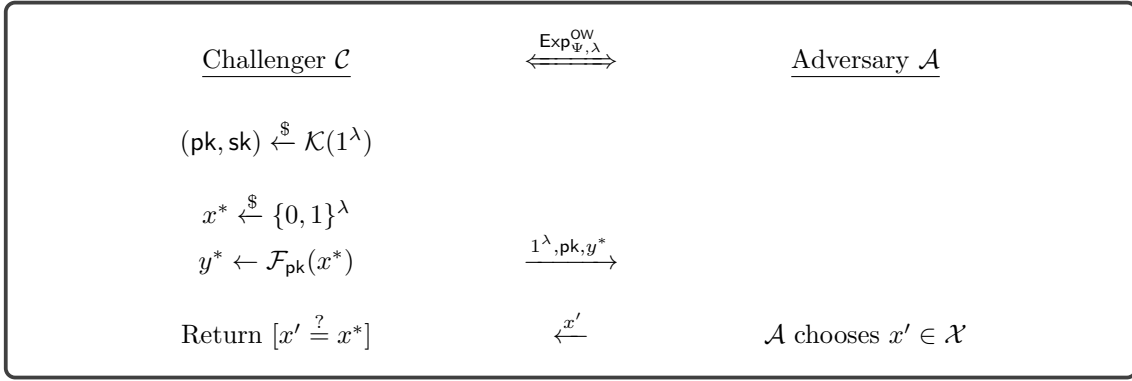
2 보안 개념

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

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



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

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

2.2 Partial-domain OW trapdoor permutation

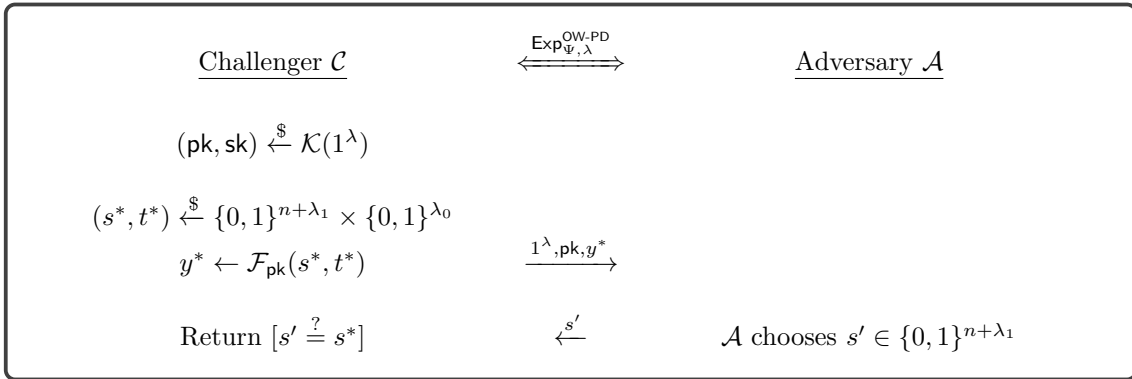
트랩도어 치환 $\Psi = (\mathcal{K}, \mathcal{F}, \mathcal{I})$ 에서, $\mathcal{F}_{pk}(x) : \{0, 1\}^\lambda \rightarrow \{0, 1\}^\lambda$ 를 다음과 같이 표현한다.

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

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

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

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

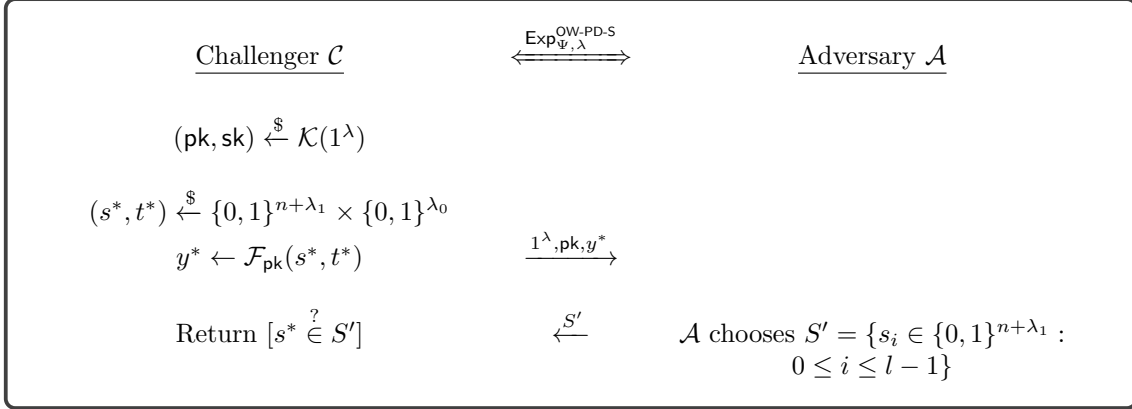


공격자 \mathcal{A} 의 능력치 $\text{Adv}_{\mathcal{A}; \Psi}^{\text{OW-PD}}(\lambda, \tau)$ 를 다음과 같이 정의한다.

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

2.3 Set partial-domain OW trapdoor permutation

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



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

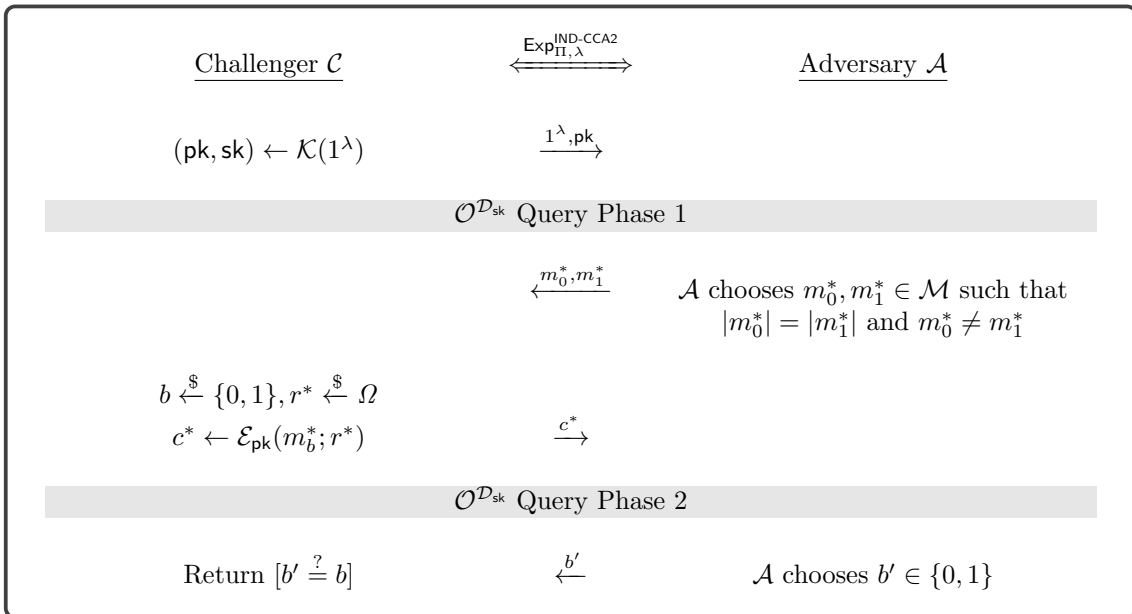
$$\text{Adv}_{\Psi, \lambda}^{\text{OW-PD-S}}(\mathcal{A}; \tau, l) := \Pr[\text{Exp}_{\Psi, \lambda}^{\text{OW-PD-S}}(\mathcal{A}; \tau, l) = 1].$$

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^λ 를 입력 받아 (pk, sk) 를 생성한다.
- $\mathcal{E}_{\text{pk}}(m)$: 암호화 알고리즘으로, pk 와 $m \in \mathcal{M}$ 를 입력 받아 $c \in \mathcal{C}$ 를 출력한다. 확률론적 알고리즘으로, $r \xleftarrow{\$} \Omega$ 를 추가로 입력 받아 $\mathcal{E}_{\text{pk}}(m; r)$ 으로 표현할 수도 있다.
- $\mathcal{D}_{\text{sk}}(c)$: 결정론적 복호화 알고리즘으로, sk 와 $c \in \mathcal{C}$ 를 입력 받아 $m \in \mathcal{M}$ 를 출력한다.

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

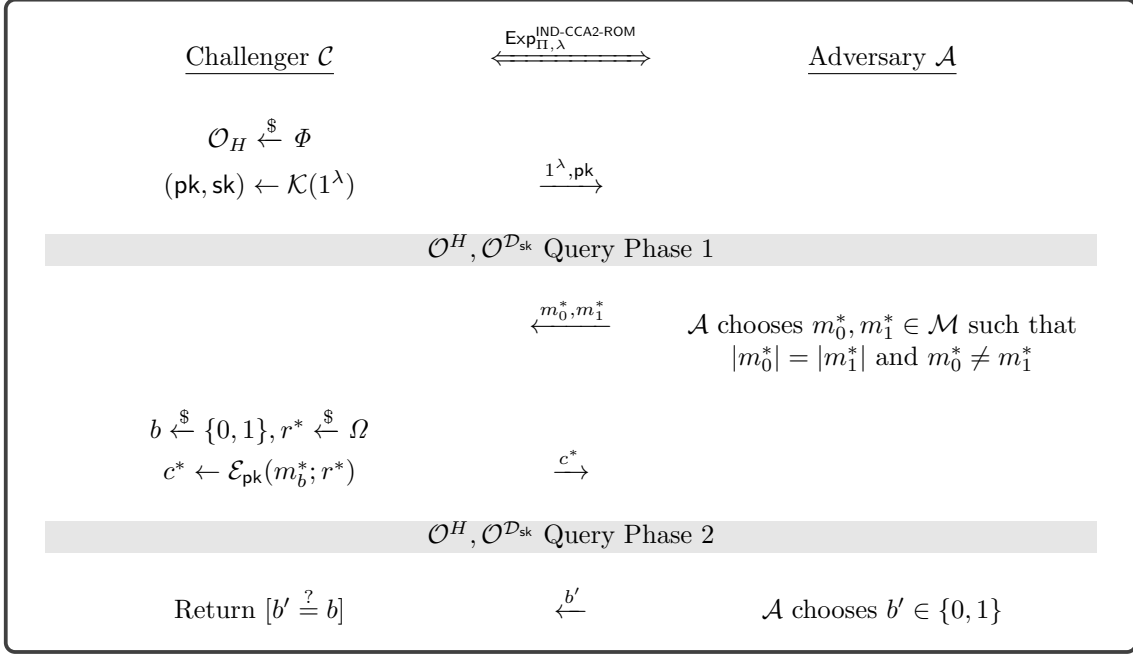


공격자 \mathcal{A} 의 능력치 $\text{Adv}_{\Pi, \lambda}^{\text{IND-CCA2}}(\mathcal{A}; \tau, q)$ 를 다음과 같이 정의한다.

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

2.5 IND security against CCA2 in ROM

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



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

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

3 RSA-OAEP

다음과 같은 트랩도어 치환 \mathcal{F} 를 고려한다.

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

그리고 두 해시 함수 H, G 를 다음과 같이 준비한다.

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

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

- $\mathcal{K}(1^\lambda)$: (pk, sk) 를 생성한다. pk 는 이후 트랩도어 치환 \mathcal{F} 에서 사용하며, sk 는 \mathcal{I} 에서 사용한다.
- $\mathcal{E}_{\text{pk}}(m; r)$: $m \in \{0, 1\}^n$ 과 $r \xleftarrow{\$} \{0, 1\}^{\lambda_0}$ 가 주어졌을 때, s, t 를 다음과 같이 계산한다.

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

s, t 를 계산하는 과정을 도식화하면 그림 1와 같다. 이후 암호문 $c = \mathcal{F}_{\text{pk}}(s, t)$ 를 출력한다.

- $\mathcal{D}_{\text{sk}}(c)$: $(s, t) = \mathcal{I}_{\text{sk}}(c)$ 을 계산한 후, r, M 을 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.

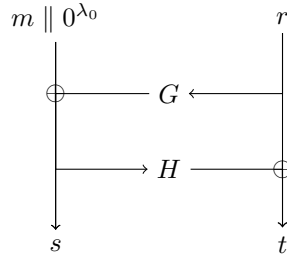


Figure 1: $\mathcal{E}_{\text{pk}}(m; r)$ 에서 s, t 를 계산하는 과정

4 증명

보조정리 1. 공격자 \mathcal{A} 를 OAEP 변환 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ 에 대해 동작시간 τ 를 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.

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

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.