

RSA-OAEP IND-CCA2 증명

김동현(wlswudpdlf31@kookmin.ac.kr)

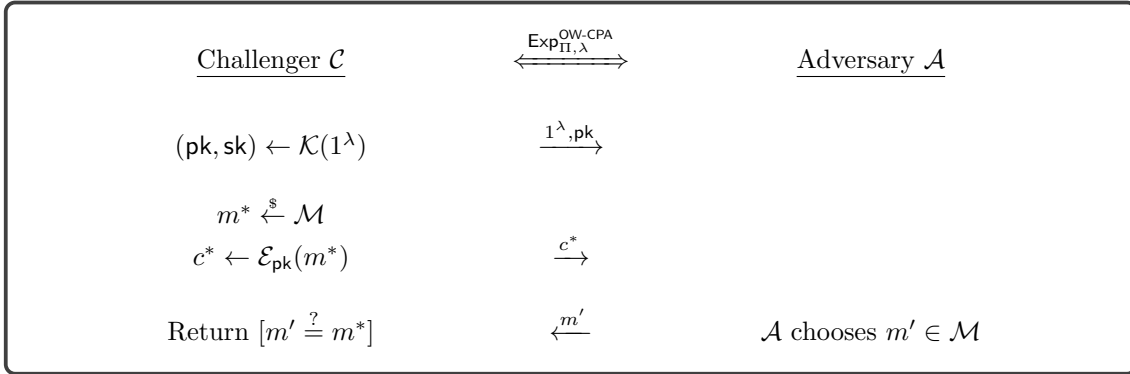
March 11, 2025

1 기호

- λ 보안 매개변수
- pk 공개키
- sk 비밀키
- $(pk, sk) \leftarrow \mathcal{K}(1^\lambda)$ 키 생성 알고리즘, 확률론적
- m 메시지
- c 암호문
- $c \leftarrow \mathcal{E}(m, pk)$ 암호화 함수, 확률론적
- $m \leftarrow \mathcal{D}(c, sk)$ 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

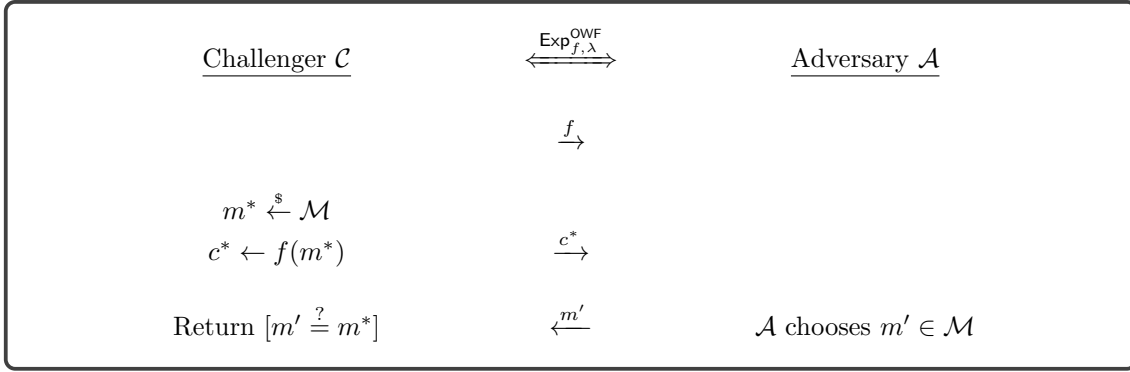
2 보안 개념

2.1 OW-CPA



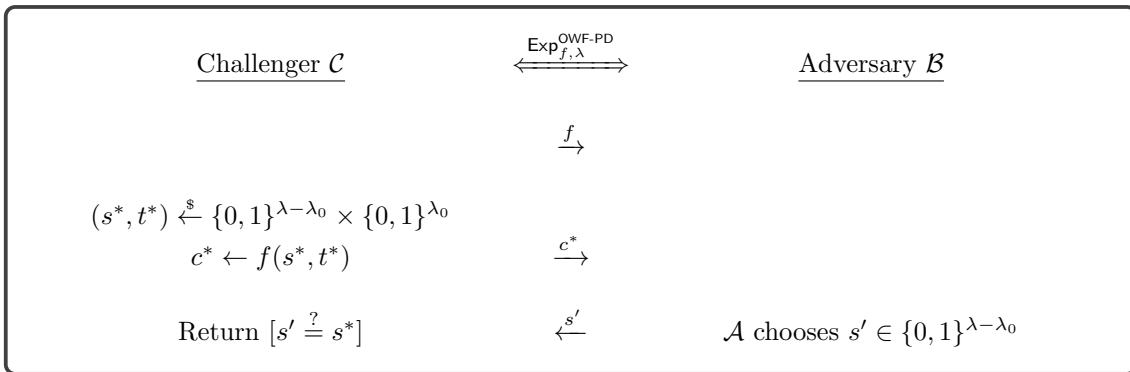
2.2 OWF

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



2.3 OWF-PD

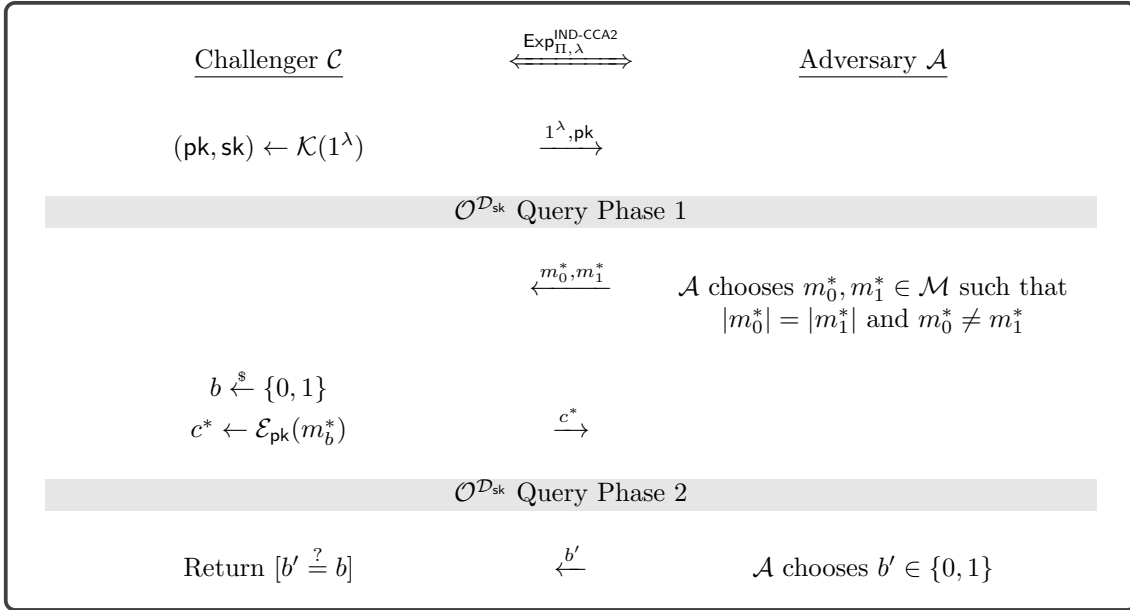
$f : \{0, 1\}^{\lambda-\lambda_0} \times \{0, 1\}^{\lambda_0} \rightarrow \{0, 1\}^{\lambda-\lambda_0} \times \{0, 1\}^{\lambda_0}$ is a trapdoor one-way permutation.



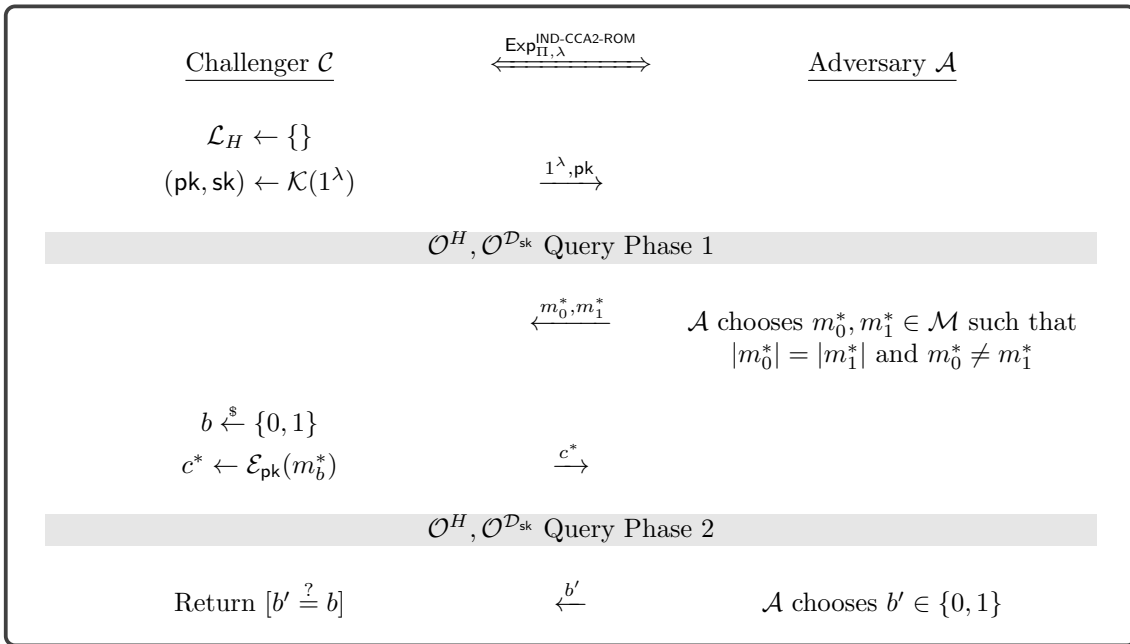
2.4 OWF-PD-S

??

2.5 IND-CCA2



2.6 IND-CCA2-ROM



3 RSA-OAEP

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

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

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

함수 f 와 그 역함수 g 로부터 얻은 OAEP 암호 $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ 를 나타내기 위해, 다음과 같은 두 해시 함수 H, G 가 필요하다.

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

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

- $\mathcal{K}(1^\lambda)$: 함수 f 의 인스턴스 pk , 함수 g 의 인스턴스 sk 를 생성한다.
- $\mathcal{E}_{\text{pk}}(m, r)$: $m \in \{0, 1\}^n$ 과 $r \xleftarrow{\$} \{0, 1\}^{\lambda_0}$ 가 주어졌을 때, 다음을 계산한다.

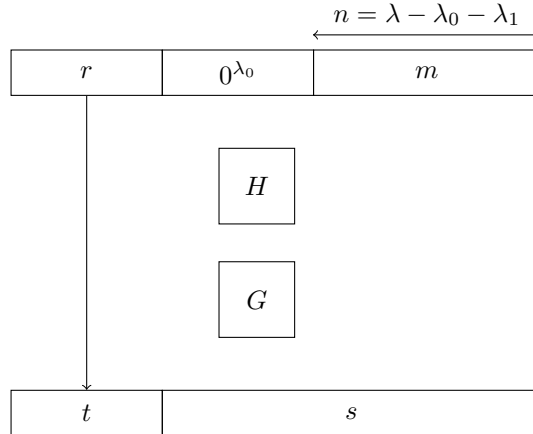
$$s = (m \parallel 0^{\lambda_1}) \oplus G(r) \quad t = r \oplus H(s).$$

이후 암호문 $c = f(s, t)$ 를 출력한다.

- $\mathcal{D}_{\text{sk}}(c)$: sk 를 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 M 의 하위 λ_1 비트를, $[M]_n$ 은 M 의 상위 n 비트를 의미한다.



4 OAEP IND-CCA2 증명

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

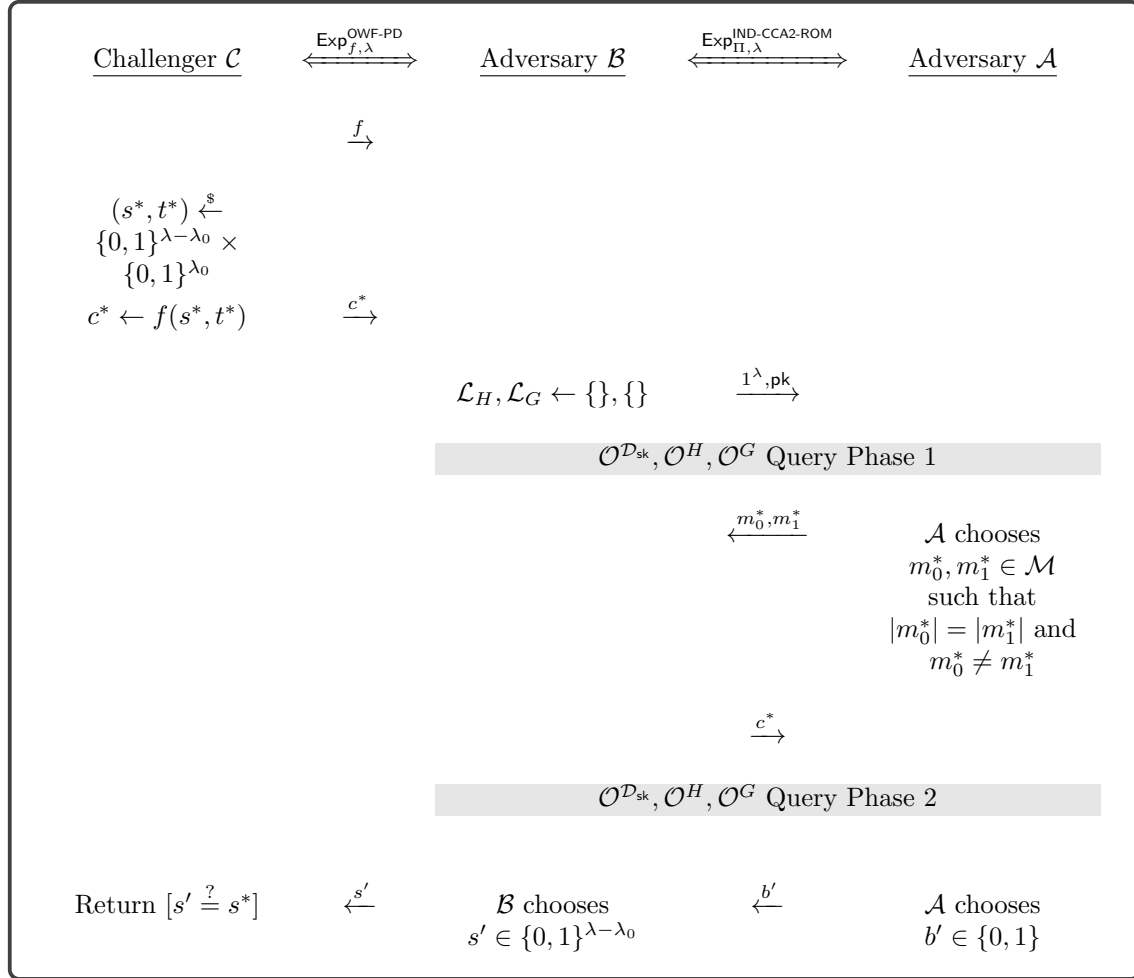
$$S \geq \frac{1}{q_H} \left(\frac{\varepsilon}{2} - \frac{2q_D q_G + q_D + q_G}{2^{\lambda_0}} - \frac{2q_D}{2^{\lambda_1}} \right).$$

이 때, $t' \leq t \cdot q_H \cdot q_G \cdot (T_f + O(1))$ 이고, T_f 는 함수 f 의 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) f 를 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_D 개의 질의를 하고, 무작위 오라클 H, G 에 대해 각각 q_H, q_G 개의 질의를 수행하며, 특정 확률 ε 보다 높은 능력치로 올바른 평문을 구별해낸다. 이제 환원 \mathcal{B} 을 설명한다.



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

- If $\gamma \in \mathcal{L}_G$, then response G_γ and $\mathcal{L}_G \leftarrow \mathcal{L}_G \cup (\gamma, G_\gamma)$.
- 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 $\mathcal{L}_G \leftarrow \mathcal{L}_G \cup (\gamma, G_\gamma)$.

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 $\mathcal{L}_H \leftarrow \mathcal{L}_H \cup (\delta, H_\delta)$.

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

- 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.