

6번 문제 풀이

Crypto Night

July 25, 2022

1 Indifferentiability Proof

$b, c, r, n \in \mathbb{N}, b = c + r$ 이고, \mathcal{P} 를 b -bit permutation, pad 를 r 비트 블록으로 변환하는 injective padding이라고 하자. Padding된 마지막 블록은 non-zero여야 한다. (TODO: generalized sponge construction $\mathcal{S}[\mathcal{P}, \text{pad}, r]$ 정의 완성)

한편, 문제에서 설명하는 해시 함수를 $\mathcal{S}'[\mathcal{P}, \text{pad}, r_1, r_2, r_3]$ 라고 정의하면, 다음이 성립한다.

정리 1 (두 construction의 관계). 10^* -padding $\text{pad}10^*$ 과 10^*1 -padding $\text{pad}10^*1$ 을 정의할 때, 모든 $\text{bitrate } 0 \leq r_1, r_2, r_3 \leq r_{\max}$ 에 대해 함수 $I[r_1, r_2, r_{\max}], O[r_3, r_{\max}]$ 가 존재하고, 다음 관계를 만족한다.

$$\mathcal{S}'[\mathcal{P}, \text{pad}10^*1, r_1, r_2, r_3] = O[r_3, r_{\max}] \circ \mathcal{S}[\mathcal{P}, \text{pad}10^*, r_{\max}, r_3] \circ I[r_1, r_2, r_{\max}]$$

여기에서 $f \circ g$ 는 함수의 합성을 의미한다.

Proof. (TODO: 증명 완성) □

정리 2 (Indifferentiability). $\mathcal{S}'[h, \text{pad}10^*1, r_1, r_2, r_3]$ 를 *random oracle* 과 구분하는 것과 $\mathcal{S}[h, \text{pad}10^*, r_{\max}, r_3]$ 를 *random oracle* 과 구분하는 *advantage* 는 같다.

Proof. (TODO: 증명 완성) □

2 Security Model

Adversary \mathcal{A} 를 확률적 알고리즘이라고 가정하고, 우리의 해시 함수 $\mathcal{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n$ 는 permutation \mathcal{P} 에 기반한다고 가정하자. \mathcal{A} 는 q 번까지 $\mathcal{P}, \mathcal{P}^{-1}$ 에 접근하는 query가 가능하며, 같은 query를 두 번 이상 하지 않는다고 가정하자.

3 Preimage Resistance Lower Bound

우리는 여기에서 everywhere preimage resistance에 집중할 것이다.[2] Random oracle \mathcal{R} 에서 다음이 성립한다.[1]

$$\mathbf{Adv}_{\mathcal{H}}^{\text{epre}}(q) \leq \mathbf{Adv}_{\mathcal{H}}^{\text{pro}}(q) + \mathbf{Adv}_{\mathcal{R}}^{\text{epre}}(q) \quad (1)$$

여기서 $\mathbf{Adv}_{\mathcal{R}}^{\text{pro}}(q)$ 는 primitive π 를 기반으로 하는 해시함수 (\mathcal{H}, π) 를 어떤 simulator S 에 대해 random oracle (\mathcal{R}, S) 로부터 구분하는 advantage로 정의된다. $\mathbf{Adv}_{\mathcal{R}}^{\text{epre}} = q/2^n$ 이므로,
(나머지는 더 공부한다음에 완성하겠습니다...)

4 Collision Resistance Lower Bound

(1)의 식과 비슷하게, 다음이 성립한다.

$$\mathbf{Adv}_{\mathcal{H}}^{\text{coll}}(q) \leq \mathbf{Adv}_{\mathcal{H}}^{\text{pro}}(q) + \mathbf{Adv}_{\mathcal{R}}^{\text{coll}}(q)$$

(나머지는 더 공부한다음에 완성하겠습니다...)

5 Second Preimage Resistance Lower Bound

Collision resistance는 second preimage resistance를 함의함이 증명되어 있다.[2] 다르게 말하면, 다음이 성립한다.

$$\mathbf{Adv}_{\mathcal{H}}^{\text{sec}}(q) \leq \mathbf{Adv}_{\mathcal{H}}^{\text{coll}}(q)$$

References

- [1] Elena Andreeva, Bart Mennink, and Bart Preneel. “Security Reductions of the Second Round SHA-3 Candidates”. In: *Information Security*. Ed. by Mike Burmester et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 39–53. ISBN: 978-3-642-18178-8.
- [2] Phillip Rogaway and Thomas Shrimpton. “Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance”. In: *Fast Software Encryption*. Ed. by Bimal Roy and Willi Meier. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 371–388. ISBN: 978-3-540-25937-4.