6번 문제 풀이

Crypto Night

August 4, 2022

1 Padding Scheme

블록 길이 x인 패딩 함수 $\mathrm{pad}[x]$가 빈 문자열에 대응되지 않고, 다음을 만족시킬 때, pad는 sponge-complaint하다고 한다.[2]

$$\forall n \geq 0, \forall M, M' \in \mathbb{Z}_2^* : M \neq M' \Rightarrow M \| \mathrm{pad}[r](|M|) \neq M' \| \mathrm{pad}[r](|M'|) \| 0^{nr}$$

이 조건을 만족하면서 가장 간단한 패딩 방법으로 multirate padding $\mathrm{pad}10^*1$을 사용할 것이다.

정의 1. *Multirate padding* $\mathrm{pad}10^*1[x]$*는 메시지의 맨 뒤에 1을 붙이고, 패딩 결과의 길이가 블록 길이* x*의 배수가 되게 하는 최소 개수의 0과 한 개의 1을 붙인다.*

2 Indifferentiability Proof

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

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

정리 1 (두 construction의 관계)**.** *10^*-padding* $\mathrm{pad}10^*$ *과* 10^*1*-padding* $\mathrm{pad}10^*1$*을 정의할 때, 모든 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.*

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

여기에서 $f \circ g$*는 함수의 합성을 의미한다.*

Proof. (TODO: 증명 완성) □

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

Proof. (TODO: 증명 완성) □

3 Preimage Resistance Lower Bound

우리는 여기에서 everywhere preimage resistance에 집중할 것이다.[3] 문제의 해시 함수 $\mathcal{H}$와 random oracle $\mathcal{R}$에서 다음이 성립한다.[1] 여기서 q는 adversary가 $\mathcal{P}, \mathcal{P}^{-1}$에 접근하는 횟수이다.

$$\mathbf{Adv}^{\mathrm{epre}}_{\mathcal{H}}(q) \leq \mathbf{Adv}^{\mathrm{indif}}_{\mathcal{H}}(q) + \mathbf{Adv}^{\mathrm{epre}}_{\mathcal{R}}(q) \tag{1}$$

여기서 $\mathbf{Adv}^{\mathrm{indif}}_{\mathcal{R}}(q)$는 primitive π를 기반으로 하는 해시함수 $(\mathcal{H}, \pi)$를 어떤 simulator S에 대해 random oracle $(\mathcal{R}, S)$로부터 구분하는 advantage로 정의된다. $\mathbf{Adv}^{\mathrm{epre}}_{\mathcal{R}} = q/2^n, \mathbf{Adv}^{\mathrm{indif}}_{\mathcal{H}}(q) \leq \frac{q(q+1)}{2^{c+1}}$에서 다음을 얻는다.

$$\mathbf{Adv}^{\mathrm{epre}}_{\mathcal{H}}(q) \leq \frac{q}{2^n} + \frac{q(q+1)}{2^{c+1}}$$

$\mathbf{Adv}^{\mathrm{pre}}_{\mathcal{H}}(q) \leq \mathbf{Adv}^{\mathrm{epre}}_{\mathcal{H}}(q)$이므로[3], preimage attack이 최소 $\min\{2^{c/2}, 2^n\}$의 접근이 필요함을 알 수 있다.

4 Collision Resistance Lower Bound

(1)의 식과 비슷하게, 다음이 성립한다.

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

여기에서 $\mathbf{Adv}^{\mathrm{coll}}_{\mathcal{R}}(q) \leq \frac{q^2}{2^{n-1}}$ 이므로 다음을 얻는다.

$$\mathbf{Adv}^{\mathrm{coll}}_{\mathcal{H}}(q) \leq \frac{q^2}{2^{n-1}} + \frac{q(q+1)}{2^{c+1}}$$

이 결과를 이용하면 collision attack에 최소 $\min\{2^{c/2}, 2^{n/2}\}$의 접근이 필요함을 알 수 있다.

5 Second Preimage Resistance Lower Bound

Collision resistance는 second preimage reistance를 함의함이 증명되어 있다.[3] 다르게 말하면, 다음이 성립한다.

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

따라서 second preimage attack에도 최소 $\min\{2^{c/2}, 2^{n/2}\}$의 접근이 필요함을 알 수 있다.

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] Bertoni Guido et al. *Cryptographic sponge functions*. 2011.

[3] 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.