Attack Bound 계산

Crypto Night

August 23, 2022

1 Padding Scheme

x 비트 패딩 함수 pad$[x]$가 빈 문자열에 대응되지 않고, 다음을 만족시킬 때, pad$[x]$는 sponge-complaint하다고 한다.[3]

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

이 조건을 만족하면서 가장 간단한 패딩 방법으로 multirate padding pad10*1을 사용할 것이다.

정의 **1**. *Multirate padding* pad10*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.*

또한, 우리의 해시 함수에서는 직접적으로 사용되지는 않지만 이후의 증명에서 사용할 10*-padding pad10*$[x]$를 다음과 같이 정의한다.

정의 **2**. 10*-*padding* pad10*$[x]$ *는 메시지의 맨 뒤에 1을 붙이고, 패딩 결과가 블록 길이* x *의 배수가 되게 하는 최소 개수의 0을 덧붙인다.*

2 Indifferentiability Proof

$b, c, r, n \in \mathbb{N}, b = c + r$ 이고, $\mathcal{P}$를 b-bit cryptographic permutation, pad를 r 비트 블록으로 변환하는 injective padding이라고 하자. Padding된 마지막 블록은 non-zero여야 한다. Sponge construction의 absorbing phase와 squeezing phase에서의 birate가 모두 r로 같고 패딩 함수가 pad, 해시 함수가 기반하는 permutation이 $\mathcal{P}$일 때 이러한 해시 함수를 $\mathcal{S}[\mathcal{P}, \mathrm{pad}, r]$으로 정의한다.

한편, 문제에서 설명하는 해시 함수를 $\mathcal{S}'[\mathcal{P}, \mathrm{pad}, r_1, r_2, r_3]$라고 정의하면,[1] 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.[2]

$$\mathcal{S}'[\mathcal{P}, \mathrm{pad10^*1}, r_1, r_2, r_3] = O[r_3, r_{\max}] \circ \mathcal{S}[\mathcal{P}, \mathrm{pad10^*}, r_{\max}, r_3] \circ I[r_1, r_2, r_{\max}]$$

[1] $\mathcal{S}[\mathcal{P}, \mathrm{pad}, r] = \mathcal{S}'[\mathcal{P}, \mathrm{pad}, r, r, r]$이므로 $\mathcal{S}[\mathcal{P}, \mathrm{pad}, r]$를 $\mathcal{S}'[\mathcal{P}, \mathrm{pad}, r_1, r_2, r_3]$의 특수한 경우라고 할 수 있을 것이다.

[2] 여기에서 $f \circ g$는 함수의 합성을 의미한다.

이때 함수 I에 대해 $M' = I[r_1, r_2, r_{\max}](M)$이라고 할 때, I는 우선 M을 multirate padding으로 패딩하여 $M_{\text{pad}} = M \| \text{pad10}^*1[r](|M|)$을 구하고, M_{pad}를 첫 블록은 r_1, 그 뒤는 r_2 길이로 나누어 M'_{pad}을 만든 뒤, Q'의 패딩을 pad10^*에 따라 해제하여 M'을 구성한다.

함수 O는 $\mathcal{S}[\mathcal{P}, \text{pad10}^*, r_{\max}, r_3]$의 출력을 $r_{\max}$ 길이로 나눈 다음, 각 블록의 첫 r_3 비트를 취한 다음 다시 블록들을 이어 붙이는 방식으로 출력을 계산한다.

문제에 제시된 해시 함수 $\mathcal{S}'[h, \text{pad10}^*1, r_1, r_2, r_3]$를 random oracle과 구분하는 공격은 $\mathcal{S}[h, \text{pad10}^*, r_{\max}, r_3]$에 적용될 수 있고, 그 반대도 가능하기 때문에 두 해시 함수를 random oracle과 구분하는 advantage는 같다.

3 Preimage Resistance Lower Bound

우리는 여기에서 everywhere preimage resistance에 집중할 것이다.[4] 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.

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

여기서 $\mathbf{Adv}_{\mathcal{R}}^{\text{indif}}(q)$는 primitive π를 기반으로 하는 해시함수 $(\mathcal{H}, \pi)$를 어떤 simulator S에 대해 random oracle $(\mathcal{R}, S)$로부터 구분하는 advantage로 정의된다. Capacity가 c일 때, $\mathbf{Adv}_{\mathcal{H}}^{\text{indif}}(q) \leq \frac{q(q+1)}{2^{c+1}}$임이 알려져 있다.[2] $\mathbf{Adv}_{\mathcal{R}}^{\text{epre}} = q/2^n$와 앞서 증명한 사실을 종합하면 다음을 얻는다.

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

여기서 $c_{\min} = \min\{c_1, c_2, c_3\}$이고, $\mathbf{Adv}_{\mathcal{H}}^{\text{pre}}(q) \leq \mathbf{Adv}_{\mathcal{H}}^{\text{epre}}(q)$이므로[4], preimage attack이 최소 $\min\{2^{c_{\min}/2}, 2^n\}$의 접근이 필요함을 알 수 있다.

4 Collision Resistance Lower Bound

(1)의 식과 비슷하게, 다음이 성립한다.

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

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

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

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

5 Second Preimage Resistance Lower Bound

(1)의 식과 비슷하게, 다음이 성립한다.

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

한편 $\mathbf{Adv}_{\mathcal{R}}^{\mathrm{sec}}(q) \leq \mathbf{Adv}_{\mathcal{R}}^{\mathrm{coll}}(q)$ 임이 알려져 있으므로, second preimage attack 에도 최소 $\min\{2^{c_{\min}/2}, 2^{n/2}\}$ 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] Guido Bertoni et al. "On the Indifferentiability of the Sponge Construction". In: *Advances in Cryptology – EUROCRYPT 2008.* Ed. by Nigel Smart. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 181–197. ISBN: 978-3-540-78967-3.

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

[4] 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.