다양한 정보이론적 척도를 이용한 비트 안전성 추정

이동훈, 김영식, 노종선
서울대학교, 조선대학교, 서울대학교

scott814@ccl.snu.ac.kr, iamyskim@Chosun.ac.kr, jsno@snu.ac.kr

Bit security estimation using various information-theoretic measures

Lee Dong-Hoon, Kim Young-Sik, No Jong-Seon

Seoul National University, Chosun University, Seoul National University.

요 약

본 논문에서는 두 개의 확률분포간의 통계적인 특성의 차이와 두 개의 암호학적 스킴(scheme)의 안전성 레벨의 차이를 연관 지어주는 다양한 정량적인 정보이론적 안전성 환원(security reduction)이 제안되어진다. 안전성은 암호학적 프리미티브들(primitives)을 논함에 있어서 그 무엇보다 필수적인 전제조건이다. 일반적으로 안전성에서는 크게 두 가지 갈래의 안전성이 존재한다; 하나는 계산이론적 안전성이고 다른 하나는 정보이론적 안전성이다. 우리는 본 논문에서 후자인 정보이론적 안전성에 대해 다루고자 한다. 특히, 본 논문에서 우리는 정량적인 안전성 레벨을 나타내어주는 편리한 척도로서 널리 이용되는 비트 안전성의 관점에서 암호학적 프리미티브들의 정보이론적 안전성을 고찰하는 것에 주안점을 둘 것이다. 우리는 본 논문에서 선행연구 [1,2]에서 제안되었던 정보이론적 안전성 환원들보다 보다 타이트하고 일반화된 버전의 안전성 환원들을 제안한다. 즉, 우리는 선행연구 [2]에서 제안된 안전성 환원보다 약 2.5-비트 더 타이트한 안전성 환원을 유도하였고, 뿐만 아니라 λ-효율적(λ-efficient)인 성질을 만족시키는 정보이론적 척도의 상한 값에 가해져 있던 제약을 완화시킴으로써 선행연구 [1]에서 제안되었던 안전성 환원을 보다 범용적인 경우에까지 적용될 수 있도록 일반화한 버전을 고안하였다. 이 연구성과를 통해 우리는 κ-비트 안전성을 가지는 본래의 스킴을 p-비트 정확성을 가지는 시스템 상에서 구현한다면 과연 그 안전성 레벨에는 어떠한 영향이 미쳐지게 될지에 관해 추정해볼 수 있는 이론적인 방법론을 제안할 수 있게 되었다. (여기서 정확성 p는 특정 조건을 만족하기만 하면 우리가 원하는 임의의 값으로 설정해줄 수 있다.) 기존의 선행연구 [1]에서는 p가 $\frac{\kappa}{2}$로서 고정되어 있었지만 우리의 결과는 안전성 레벨 κ와 정확성 p를 상호간에 독립적으로 변화시키면서 관찰하는 것을 가능하게 하도록 일반화시켰다. 더욱이 우리는 다섯 가지 정보이론적 척도에 대해 다양한 안전성 환원을 제안하였다. 우리는 우리의 결과가 랜덤 값을 추출하는 확률분포만 다르고 그 이외의 사항은 모두 같은 동일한 암호학적 스킴에 있어서 과연 그 랜덤 값을 추출하는 확률분포의 통계적 특성 차이가 안전성 레벨에 얼마만큼의 영향을 미치는지에 관해 알려주는 정보이론적 지침으로서의 역할을 할 수 있기를 기대한다. 특히, 우리의 결과는 이상적인 확률분포와 실제적인 확률분포간의 통계적인 특성 차이가 안전성 레벨에 얼마만큼의 영향을 미치는지에 관해 정량적인 추정을 얻는데 유용하게 활용될 수 있을 것이다.

Ⅰ. 서 론

오늘날 존재하는 거의 모든 암호학적 프리미티브들은 특정 확률분포로부터 추출해내는 어떠한 랜덤 값에 그 자신의 안전성을 의존하고 있다. (예를 들어, LWE 문제 기반 격자기반암호 스킴에서 랜덤 값인 에러를 이산 가우시안 분포로부터 추출하는 경우를 생각할 수 있다.) 달리 표현하면 암호 스킴에 있어 랜덤 값을 추출해내는 확률분포는 그것의 안전성에 매우 큰 영향을 미칠 수 있다. 이러한 관점에서 암호 스킴의 랜덤 값을 추출하는 확률분포가 다른 확률분포로 대체되었을 경우 안전성 레벨이 어떻게 변화하는지에 대해 분석하는 연구가 많이 진행되어왔다. 전통적으로 확률 보존 성질 (probability preservation property)라는 원리가 두 확률분포간의 통계적인 특성차이와 공격자의 공격성공확률을 연관 지어주는 안전성 환원으로서 널리 이용되어왔다. 이러한 종류의 안전성 환원은 암호 스킴간의 상대적인 안전성 레벨의 비교는 가능하게 해주었지만 확률 보존 성질만 가지고는 우리는 안전성 레벨에 대한 어떠한 구체적이고 정량적인 정보를 얻어낼 수는 없었다. 이러한 동기에 의해 정량적인 안전성 분석을 가능하게 하기위한 몇몇 연구들이 진행되어왔다. Micciancio 와 Walter [1,2]는 이 분야에 있어 선구자라고 여겨진다. 그들은 정보이론적 척도를 이용하여 다양한 정량적 안전성 환원을 제안했고 그러한 안전성 환원들을 비트 안전성의 관점에서 표현하였다. 그러나 우리는 그들의 안전성 환원이 더욱 개선될 여지가 남아있으며 더욱이 그들의 결과는 오직 제한된 경우에 대해서만 사용되어질 수 있다는 사실을 알게 되었다.

본 논문에서 우리의 기여는 다음과 같다. 첫째, 우리는 Micciancio 와 Walter 의 안전성 환원의 경계 값보다 더욱 타이트한 경계 값을 유도해내었다. 둘째, λ-효율적인 성질을 만족시키는 정보이론적 척도의 상한 값에 가해져 있던 제약을 완화시킴으로써 Micciancio 와 Walter 가 제안한 안전성 환원을 보다 범용적인 경우에까지 적용될 수 있도록 일반화한 버전을 고안하였다. 이 연구성과를 통해 우리는 κ-비트 안전성을 가지는 본래의 스킴을 p-비트 정확성을 가지는 시스템 상에서 구현한다면 과연 그 안전성 레벨에는 어떠한 영향이 미쳐지게 될지에 관해 추정해볼 수 있는 이론적인 방법론을 제안할 수 있게 되었다. (여기서 p 는 특정 조건만 만족한다면 우리가 원하는 임의의 값으로 설정해줄 수 있다.) 셋째, 우리는 다음과 같은 다섯 가지 종류의 정보이론적 척도를 사용하여 다양한 종류의 안전성 환원을 제안하였다; statistical distance, Renyi divergence, Kullback-Leibler divergence, max-log distance, and relative error. 이러한 척도들은 모두 암호학에서 안전성 환원 분석에서 자주 사용되는 주요 척도들이다.

Ⅱ. 본론

선행연구 [1]의 보조정리 3 에서 제안한 안전성 환원을 1-비트 가량 더 타이트하게 개선시킨 안전성 환원을 다음 정리 1 에서 제안하였다.

정리 1. S^P와 S^Q를 각각 확률분포 앙상블 P_θ, Q_θ에 블랙박스 접근이 가능한 표준적인 암호 스킴이라고 가정하자. (즉, 스킴 내부가 어떻게 동작하는지에 관해서는 관심 없고 S^P, S^Q가 다른 점은 오직 랜덤 값을 추출하는 확률분포 뿐이다.) 만약 S^P가 κ-비트 안전성을 가지고 $2^{-\frac{\kappa}{2}}$-효율적인 척도 δ에 대해 $\delta(P_\theta, Q_\theta) \le 2^{-\frac{\kappa}{2}}$ 가 만족한다면 S^Q는 (κ-2.374)-비트 안전성을 가진다. ■

max-log distance 는 $\lambda \le \frac{1}{2}$을 만족하는 λ에 대해 λ−효율적인 척도라는 사실과 선행연구 [1]의 보조정리 6 을 적용하면 정리 1 로부터 다음의 두 따름정리를 어렵지 않게 유도해낼 수 있다.

따름정리 1. 만약 S^P 가 κ-비트 안전성을 가지고 $\Delta_{ML}(P_\theta, Q_\theta) \le 2^{-\frac{\kappa}{2}} (\le \frac{1}{2})$를 만족한다면, S^Q는 (κ-2.374)-비트 안전성을 가진다. ■

따름정리 2. 만약 S^P 가 κ-비트 안전성을 가지고 $\delta_{RE}(P_\theta, Q_\theta) \le 1 - e^{-2^{-\frac{\kappa}{2}}} (\le 1 - e^{-\frac{1}{2}})$를 만족한다면, S^Q는 (κ-2.374)-비트 안전성을 가진다. ■

선행연구 [2]의 따름정리 2 에서 제안한 안전성 환원을 더욱 타이트하게 개선시킨 안전성 환원을 다음 보조정리 1 에서 제안하였다.

보조정리 1. 자원 T 를 가진 임의의 공격자 A 가 S^P와 S^Q를 공격하여 공격에 성공할 확률을 각각 γ_P, γ_Q 라 하자. 만약 효율적인 척도 δ가 $\sqrt{\frac{\gamma_Q}{T}} \times 0.44$ -효율적이며 $\delta(P_\theta, Q_\theta) \le \sqrt{\frac{\gamma_Q}{T}} \times 0.44$를 만족한다면 $\gamma_Q \le 5.184 \times \gamma_P$가 성립한다. ■

보조정리 1 을 이용하여 다음 정리 2 를 유도해 낼 수 있었다. 정리 2 는 선행연구 [2]의 정리 8 에서 제안한 안전성 환원을 약 2.5-비트 더 타이트하게 개선시킨 안전성 환원을 제안한다.

정리 2. S^P와 S^Q를 각각 확률 앙상블 $(P_\theta)_\theta, (Q_\theta)_\theta$에 블랙박스 접근이 가능한 1-비트 안전성 게임이라고 가정하자. (즉, 암호화 알고리즘 같은 구별 불가능성에(indistinguishability) 그 안전성의 근간을 두고 있는 스킴에 대해 적용할 수 있는 정리이다.) 또한, δ를 $\lambda \le 0.44$를 만족하는 임의의 λ에 대해 λ-효율적인 척도라고 하자. 만약 S^P 가 κ-비트 안전성을 가지고 $\delta(P_\theta, Q_\theta) \le 2^{-\frac{\kappa}{2}}$가 만족한다면 S^Q는 (κ-5.544)-비트 안전성을 가진다. ■

정리 1 로부터 안전성 레벨 κ와 정확성 p 를 독립적으로 조절하며 안전성 레벨을 관찰하는 것을 가능하도록 일반화한 정리 3 을 유도해내었다.

정리 3. [정리 1 의 일반화] S^P와 S^Q를 각각 확률분포 앙상블 P_θ, Q_θ에 블랙박스 접근이 가능한 표준적인 암호 스킴이라고 가정하자. 만약 S^P가 κ-비트 안전성을 가지고 $2^{-\frac{f(\kappa)}{2}}$-효율적인 척도 δ에 대해 $\delta(P_\theta, Q_\theta) \le 2^{-\frac{f(\kappa)}{2}}$가 만족한다면 S^Q 는 $(2\log_2\left(\sqrt{1+2^{f(\kappa)-\kappa+2}(1-e^{-1})}-1\right) - f(\kappa) + 2\kappa - 2$)-비트 안전성을 가진다. 여기서 $f(\kappa)$는 S^P의 안전성 레벨 κ에 대해 $f(\kappa) \ge -2\log_2(1-e^{-1}-2^{-\kappa})$를 만족하여야 한다. ■

이후 등장하는 정리 4 와 정리 5 는 각각 RD_∞와 Δ_{SD}를 척도로 하는 안전성 환원을 제안한다.

정리 4. [공격자가 자원이 제한되어 있는 상황에 놓여있는 경우에 적용 가능] S^P와 S^Q를 각각 확률분포 앙상블 P_θ, Q_θ에 블랙박스 접근이 가능한 표준적인 암호 스킴이라고 가정하자. 만약 S^P 가 κ-비트 안전성을 가지고 $RD_\infty(Q_\theta || P_\theta) \le 2^{\frac{1}{\kappa^n}}$가 성립한다면 S^Q는 $(\kappa - \frac{T_A}{\kappa^n})$-비트 안전성을 가진다. 이 때, $T_A \le \kappa^{n+1}$가 성립되어야 한다. (즉, 공격자 A 의 자원이 제한 되어있는 상황에 대해 적용될 수 있다.) ■

정리 5. S^P와 S^Q를 각각 확률분포 앙상블 P_θ, Q_θ에 블랙박스 접근이 가능한 표준적인 암호 스킴이라고 가정하자. 만약 S^P 가 κ-비트 안전성을 가지고 $\Delta_{SD}(P_\theta, Q_\theta) \le 2^{-h(\kappa)}$ 가 성립한다면 S^Q 는 $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-비트 안전성을 가진다. 여기서 $h(\kappa)$는 S^P의 안전성 레벨 κ에 대해 $h(\kappa) \ge -\log_2(1-\frac{1}{2^\kappa})$를 만족하여야 한다. ■

Pinsker 의 부등식에 의해 다음 따름정리 3 을 정리 5 로부터 유도해낼 수 있다.

따름정리 3. 만약 S^P 가 κ-비트 안전성을 가지고 $\Delta_{KL}(Q_\theta, P_\theta) \le 2^{1-2h(\kappa)}$ 가 성립한다면 S^Q 는 $\log_2 \frac{1}{2^{-\kappa}+2^{-h(\kappa)}}$-비트 안전성을 가진다. 여기서 $h(\kappa)$는 S^P의 안전성 레벨 κ에 대해 $h(\kappa) \ge -\log_2(1-\frac{1}{2^\kappa})$를 만족하여야 한다. ■

Ⅲ. 결론 및 참고문헌

본 논문에서는 확률분포간의 통계적인 특성차이로부터 기인하는 정보이론적 안전성 환원들을 정보이론적 척도의 관점에서 유도해내었다.

[1] D. Micciancio, M..Walter, "Gaussian sampling over the integers: Efficient, generic, constant-tim," CRYPTO 2017.

[2] D. Micciancio, M. Walter, "On the bit security of cryptographic primitives," EUROCRYPT 2018.