MC525: Cryptography
#0: Discrete Probability Basics
Informal Introduction for Cryptography

Sang-Hyun Yoon

Definition (Discrete Probability Space)

Let

- Ω : a finite set (e.g. $\mathcal{C}$, $\mathcal{K} \times \mathcal{M}$)
- $p : \Omega \to [0, 1]$: a function satisfying $\sum_{\omega \in \Omega} p(\omega) = 1$.

We say that

- (Ω, p) is a discrete probability space
  - Ω is the sample space (or domain)
  - p is a probability distribution (확률분포) over Ω
- Each subset $A \subseteq \Omega$ is an event
  - Each $\omega \in \Omega$ is an elementary event
- $p(A) \triangleq \sum_{\omega \in A} p(\omega)$ is the probability of an event A
- $p(\omega) = 1/|\Omega|$ (for each $\omega \in \Omega$) is the uniform distribution

Given a discrete probability space (Ω, p), it is customary to use

- $\Pr_\Omega$ instead of the probability distribution p
- $\Pr_\Omega[A]$ instead of $p(A)$
- $\Pr$ and $\Pr[A]$ when Ω is clear from the context

Discrete Probability Space: Example

Example (Rolling a Dice)

The corresponding probability space $(\Omega, \Pr_\Omega)$ is given by:

- $\Omega = \{1, 2, 3, 4, 5, 6\}$
- $\Pr_\Omega[\omega] = 1/6$ for each $\omega \in \Omega$

The following A, B are events of the probability space $(\Omega, \Pr)$:

- $A = \{2\} \ (\subseteq \Omega)$
- $B = \{\omega \in \Omega \,|\, \omega \text{ is even}\} \ (\subseteq \Omega)$

Then,

- $\Pr_\Omega[A] = 1/6$
- $\Pr_\Omega[B] = 1/2$

암호학에서는 여러개의 probability space를 동시에 고려하므로 $\Pr_{\Omega_1}, \Pr_{\Omega_2}$와 같이 sample space를 표시해줘야 헷갈리지 않음

Discrete Probability Space: Example from Cryptography

Let

- $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$: a (private-key) encryption scheme.
- $\Pr_{\mathcal{M}} \in \mathcal{P}_{\mathcal{M}}$: a probability distribution over $\mathcal{M}$
- $\Omega = \mathcal{K} \times \mathcal{M}$
- $\Pr_{\Omega}$: prob. dist. over Ω s.t. $\Pr_{\Omega}(k, x) = \Pr_{(\mathcal{K}, \mathsf{Gen}())}(k) \cdot \Pr_{\mathcal{M}}(x)$

$(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is said to be Shannon secret w.r.t. $\Pr_{\mathcal{M}}$ if

- $\forall m \in \mathcal{M}$, $\forall c \in \mathcal{C}$,

$$\Pr_{(\Omega, \Pr_{\Omega})}\left[\{(k, x) \in \Omega \,|\, x = m\} \;\middle|\; \{(k, x) \in \Omega \,|\, \mathsf{Enc}(k, x) = c\}\right]$$
$$= \Pr_{(\Omega, \Pr_{\Omega})}\left[\{(k, x) \in \Omega \,|\, x = m\}\right] \quad (= \Pr_{\mathcal{M}}(m))$$

  - i.e. two events $\{(k, x) \,|\, x = m\}$ and $\{(k, x) \,|\, \mathsf{Enc}(k, x) = c\}$ are independent

$(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is said to be Shannon secret if

- it is Shannon secret with respect to all $\Pr_{\mathcal{M}} \in \mathcal{P}_{\mathcal{M}}$

Outline

Conditional Probability & Independence of Events

Fix a probability space $(\Omega, \Pr)$ and events $A, B \subseteq \Omega$ with $\Pr[B] \neq 0$

Definition (Conditional Probability)

The conditional probability of A given B, denoted $\Pr[A|B]$, is

- $\Pr[A|B] \triangleq \dfrac{\Pr[A \cap B]}{\Pr[B]}$
  - events B가 일어난 상황하에서 A가 일어날 확률을 나타냄

Definition (Independence of Events)

A and B are said to be independent if

- $\Pr[A|B] = \Pr[A]$ (equivalently, $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$)

Example (Rolling a Dice)

Let $A = \{2\}$ and $B = \{2, 4, 6\}$. Then,

- $\Pr[A|B] = \Pr[A \cap B]/\Pr[B] = 1/3$ (A, B not independent)
- $\Pr[B|A] = \Pr[A \cap B]/\Pr[A] = 1/1 = 1$

Bayes' Theorem

Bayes' Theorem

Given pairwise disjoint events $C_1, C_2, \ldots, C_n$ and a feasure set F,

$$\Pr(C_i|F) = \frac{\Pr(F \cap C_i)}{\Pr(F)} = \frac{\Pr(F \cap C_i)}{\sum_{j=1}^{n} \Pr(F \cap C_j)}$$
$$= \frac{\Pr(F|C_i)\Pr(C_i)}{\sum_{j=1}^{n} \Pr(F|C_j)\Pr(C_j)}.$$

- of much use when
  - C_i = possible causes (e.g. diseases)
  - F = observed result (e.g. symptom)
  - cause-to-result relationship (e.g. $\Pr(F|C_i)$) is well-understood

Terms in Bayesian community:

- $\Pr(C_i)$: a prior of C_i
- $\Pr(C_i|F)$: a posterior of C_i given F

Bayesian Decision Problems

Uncertain Quantity & Prior Information

- $\theta \in \Theta$: uncertain quantity
- $\pi(\theta)$: prior information (given probabilistically)

Measurement

- $z \in \mathcal{Z}$: sample information & space
- $f(z|\theta)$: measurement model (given probabilistically)

Posterior Distribution

$$\pi(\theta|z) = \frac{\pi(\theta)f(z|\theta)}{m(z)} = \frac{\pi(\theta)f(z|\theta)}{\int_\Theta f(z|\theta)\pi(\theta)d\theta} \quad \left(\Pr(A|B) = \frac{\Pr(A)\Pr(B|A)}{\Pr(B)}\right)$$

Decision Rule: Posterior Bayesian

A function $\delta : \mathcal{Z} \to \mathcal{A}$ $\quad (\mathcal{A} = \Theta$ for estimation problems)

- $L(\theta, \delta(z))$: loss function ($L(\theta, \hat{\theta}(z))$ for estimation prob.)

$$\delta(z) \triangleq \arg\min_{a\in\mathcal{A}} \int_\Theta L(\theta, a)\pi(\theta|z)d\theta = \arg\min_{a\in\mathcal{A}} \int_\Theta L(\theta, a)\pi(\theta)f(z|\theta)d\theta$$

Outline

Random Variables

Definition (Random Variables)

Let $(\Omega, \Pr)$ be a probability space and $X : (\Omega, \Pr) \to \Omega'$. Then,

- X is called a random variable (RV) over $(\Omega, \Pr)$
- For $\omega' \in \Omega'$, $\Pr[X = \omega']$ denotes $\Pr_\Omega\left[\{\omega \in \Omega : X(\omega) = \omega'\}\right]$
- Distribution of X is func. $f_X : \Omega' \to [0, 1]$; $f_X(\omega') = \Pr[X = \omega']$

- (Ω', f_X)는 $(\Omega, \Pr_\Omega)$로부터 X를 거쳐서 만들어진 새로운 probability space로 이해하면 됨
- Ω'는 measurable space에 대해 고려하는데 대부분 $\mathbb{R}$

Definition (Independence of Random Variables)

Two RVs $X, Y : \Omega \to \Omega'$ are said to be independent if

- for each $\omega'_1, \omega'_2 \in \Omega'$, the events $X^{-1}(\omega'_1)$ and $Y^{-1}(\omega'_2)$ are independent (i.e. $\Pr[X = \omega'_1, Y = \omega'_2] = \Pr[X = \omega'_1] \cdot \Pr[Y = \omega'_2]$)

Expectation & Variance

Definition (Expectation/Variance of a Random Variable)

Let $X : \Omega \to \mathbb{R}$ be a random variable over $(\Omega, \Pr_\Omega)$. We say that:

- $\mathbb{E}[X] \triangleq \sum_{\omega\in\Omega} X(\omega)\Pr_\Omega[\omega] = \sum_{a\in\mathbb{R}} a \cdot \Pr[X=a]$ is the expectation of X
- $\mathrm{Var}[X] \triangleq \mathbb{E}\left[(X-\mathbb{E}[X])^2\right] = \sum_{\omega\in\Omega} \Pr_\Omega[\omega]\left(X(\omega)-\mathbb{E}[X]\right)^2$ is the variance of X

Useful properties:

- $\mathbb{E}[X_1 + \cdots + X_n] = \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_n]$ (linearity of exp.)
  - $X_1, \cdots, X_n$이 independent하지 않아도 성립됨에 유의
- $\Pr[X \geq \lambda] \leq \mathbb{E}[X]/\lambda$ for each $\lambda > 0$ (Markov inequality)
- $\Pr\left[|X-\mathbb{E}[X]| \geq \lambda\right] \leq \mathrm{Var}[X]/\lambda^2$ (Chebyshev inequality)
- $\Pr[|(\sum X_i - \mathbb{E}[X_i])/n| > \lambda] < 2^{-\lambda^2 n/4}$ (Chernoff inequality)

이번 학기 수업에서는 별로 사용되지 않음

Notational Conventions for Cryptography (매우 중요!!)

Given a finite sample space Ω,

- $\mathcal{P}_\Omega \triangleq \{p : \Omega \to [0,1] \mid \sum_{\omega\in\Omega} p(\omega) = 1\}$
  - i.e. the set of all probability distributions over Ω
- $U_\Omega \triangleq$ the uniform probability distribution over Ω
  - i.e. $U_\Omega(\omega) = 1/|\Omega|$ for all $\omega \in \Omega$

Enc는 probabilistic poly-time 알고리즘이므로 이것의 randomness도 probability space에 반영해줘야 하는데..

- 예를 들어, $\Pr_{\mathcal{K},\mathsf{Gen}(1^n)}\left[\{k \in \mathcal{K} \mid \mathsf{Enc}(k,m)...\}\right]$에서 sample space는 $\mathcal{K}$만 표시되어 있는데, Enc에서 사용되는 random number들의 sample space도 implicitly 포함된 것
- 즉, 위 표시는 다음을 줄여서 표현한 것으로 이해해야 함:
  $\Pr_{\mathcal{K}\times\mathcal{R},\cdots}\left[\{(k,r) \in \mathcal{K}\times\mathcal{R} \mid \mathsf{Enc}(r,k,m)...\}\right]$
- Enc의 randomness는 무조건 포함되므로 앞으로 Enc가 연루된 모든 확률 표현은 위와 같이 해석하도록