Lecture 3

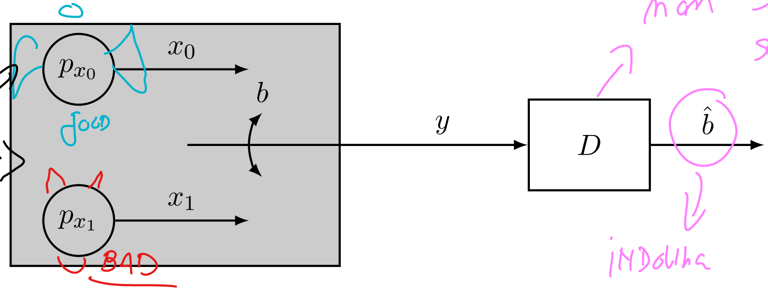
Composable Definitions of Security

Nicola Laurenti October 7, 2020

Lecture 3— Contents

Variable distinguishers (or binary hypothesis testing)

2 segnali



non sa se viene da p_{x_0} p_{x_1}

A distinguisher between two random variables x_0 and x_1 is a system D that is allowed to observe a realization of y without knowing in advance if $b = 0$ or $b = 1$ and should then guess which one holds

- x_0 and x_1 are characterized by their PMDs p_{x_0}, p_{x_1}
- D is composed of a decision function $g : \mathcal{Y} \mapsto \{0, 1\}$, i.e. $\hat{b} = g(y)$

It is a common situation in security (e.g., intrusion detection, authenticity verification, etc.)

Distinguisher performance

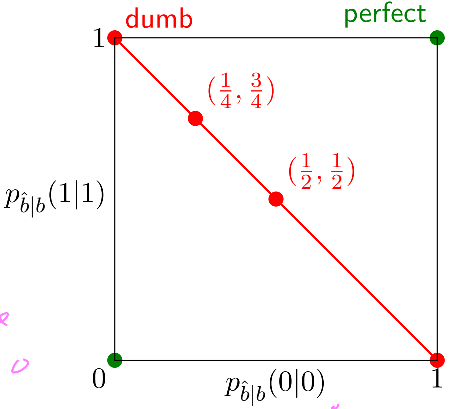
$P(\hat{b}=0|b=0)$
$P(\hat{b}=1|b=1)$

The performance of a distinguisher D is given by the pair of correct decision probabilities

$$\left(p_{\hat{b}|b}(0|0), p_{\hat{b}|b}(1|1)\right)$$

or complementarily by the pair of error probabilities

$$\left(p_{\hat{b}|b}(1|0), p_{\hat{b}|b}(0|1)\right)$$



We define the distinguishability between x_0 and x_1 with D as

$$d_D(x_0, x_1) = |p_{\hat{b}|b}(0|0) + p_{\hat{b}|b}(1|1) - 1| = |p_{\hat{b}|b}(1|0) + p_{\hat{b}|b}(0|1) - 1|$$

Note that $d_D(x_0, x_1) = 1$ for a perfect distinguisher while $d_D(x_0, x_1) = 0$ for a dumb distinguisher

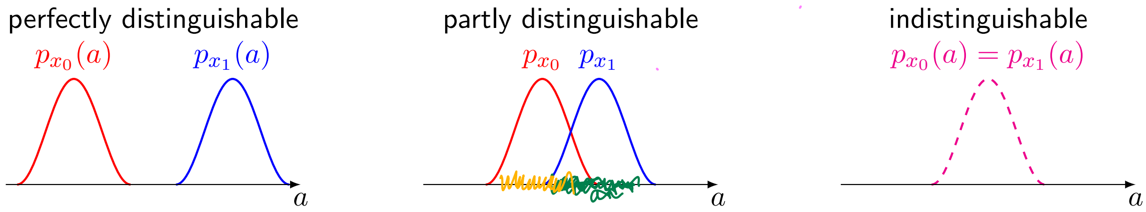
Indistinguishability and statistical distance

It is not always possible to find a perfect or even a good distinguisher

Definition (unconditional)

Two variables x_0 and x_1 are said to be ε-unconditionally indistiguishable if, for any distinguisher D, it is $d_D(x_0, x_1) \leq \varepsilon$

Unconditonal distinguishability is a measure of statistical distance between two variables



The distinguisher that maximizes $d_D(x_0, x_1)$ is the ML estimator of b from observation y

Variational statistical distance

Definition

The variational distance between two rvs x, y with alphabet $\mathcal{A}$ is defined as

every possible of message input.

$$d_{\mathsf{V}}(x,y) = \frac{1}{2} \sum_{a \in \mathcal{A}} |p_x(a) - p_y(a)|$$

It is a 1-norm distance between their PMD, and it holds

$$\text{(indistinguishable)} \quad 0 \le d_{\mathsf{V}}(x,y) \le 1 \quad \text{(perfectly distinguishable)}$$

Relationship with distinguishability

$$\sup_D d_D(x,y) = d_{\mathsf{V}}(x,y)$$

Kullback-Leibler divergence for discrete rvs

Definition

Given two discrete rvs, x, y with alphabets $\mathcal{A}_x \subset \mathcal{A}_y$ and pmds p_x, p_y, their Kullback-Leibler divergence is

$$\mathrm{D}\left(p_x \| p_y\right) = \mathrm{E}\left[\log_2 \frac{p_x(x)}{p_y(x)}\right] = \sum_{a \in \mathcal{A}_x} p_x(a) \log_2 \frac{p_x(a)}{p_y(a)}$$

Example: Binary rvs

For binary rvs, with $\mathcal{A} = \{0, 1\}$,

$$\mathrm{D}\left(p_x \| p_y\right) = p_x(0) \log_2 \frac{p_x(0)}{p_y(0)} + p_x(1) \log_2 \frac{p_x(1)}{p_y(1)}$$

The KLD definition can be extended to the case $\mathcal{A}_x \not\subset \mathcal{A}_y$ (i.e. $p_y(a) = 0$ for some $a \in \mathcal{A}_x$), by letting $\mathrm{D}\left(p_x \| p_y\right) = \infty$ in that case

Kullback-Leibler divergence (cont.)

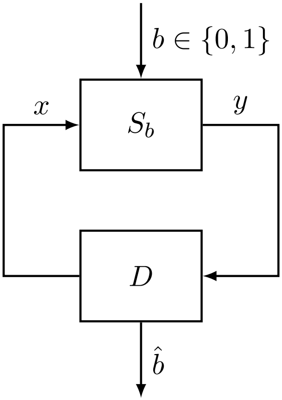
The KLD is a measure of statistical diversity between rvs. It is related to their distinguishability

Properties

1. (positivity) $\mathrm{D}\left(p_x \| p_y\right) \geq 0, \forall p_x, p_y$
   and $\mathrm{D}\left(p_x \| p_y\right) = 0$ if and only if $p_x \equiv p_y$
2. (asymmetry) $\mathrm{D}\left(p_x \| p_y\right) \neq \mathrm{D}\left(p_y \| p_x\right)$, in general
3. (Pinsker inequality) $\mathrm{D}\left(p_x \| p_y\right) \geq 2 d_{\mathsf{V}}(x, y)^2$

d_V

System distinguishers



S_0 is characterized by the conditional PMD $p_{y_0|x_0}$

S_1 is characterized by $p_{y_1|x_1}$

A distinguisher between two probabilistic systems S_0 and S_1 is a third system D that is allowed to interact with a system S_b without knowing in advance if $b = 0$ of $b = 1$ and

- can feed any input x to S_b
- can observe the corresponding output y
- should then guess whether $b = 0$ or $b = 1$

D is composed of

- an input selection strategy p_x (possibily adaptive, $p_{x|y}$) and
- a decision function $g : \mathcal{X} \times \mathcal{Y} \mapsto \{0,1\}$, i.e. $\hat{b} = g(x, y)$

Indistinguishability

It is not always possible to find a perfect or even a good distinguisher

Definition (unconditional)

Two systems S_0 and S_1 are said to be ε-unconditionally indistiguishable if $d(S_0, S_1) \leq \varepsilon$, for any distinguisher D, it is $d_D(S_0, S_1) \leq \varepsilon$

Definition (computational, concrete)

S_0 and S_1 are said to be (ε, T_0)-computationally indistiguishable if, for any distinguisher D with complexity $T_D \leq T_0$, it is $d_D(S_0, S_1) \leq \varepsilon$

Definition (computational, asymptotic)

Two sequences of systems $S_{0,n}$ and $S_{1,n}$ are said to be computationally indistiguishable in the asymptotic forumlation if, for any polynomials $p(\cdot), q(\cdot)$ and any sequence of distinguishers D_n with complexity $T_{D_n} \leq p(n)$, ther exist n_0 such that $d_{D_n}(S_{0,n}, S_{1,n}) \leq 1/q(n)$, $\forall n > n_0$

Security definitions

Definition (unconditional)

A mechanism M is said to be ε-unconditionally secure if it is ε-unconditionally indistiguishable from its ideal counterpart $M^\star$

Definition (computational, concrete)

A mechanism M is said to be (ε, T_0)-computationally secure if it is (ε, T_0)-computationally indistiguishable from its ideal counterpart $M^\star$

Definition (computational, asymptotic)

A sequence of mechanisms $\{M_n\}$, $n \in \mathbb{N}$ is said to be computationally secure in the asymptotic formulation if it is computationally indistiguishable from its ideal counterpart $\{M_n^\star\}$ in the asymptotic formulation

Example: pseudo random functions

Same same
input → output

Ideal random functions

An ideal random function $f^\star : \mathcal{X} \mapsto \mathcal{Y}$ is a random mapping such that

- for each possible input value $x \in \mathcal{X}$, $f^\star(x)$ is a random variable uniform over $\mathcal{Y}$
- the random variables corresponding to different values of x are statistically independent

Equivalently, by letting $\mathcal{X} = \{x_1, \ldots, x_N\}$, we have that $[f^\star(x_1), \ldots, f(x_N)]$ is a random vector, uniformly distributed over all possible strings of N elements from $\mathcal{Y}$

2 input k = Parameter

Pseudo random functions

A secure pseudo random function $f : \mathcal{X} \times \mathcal{K} \mapsto \mathcal{Y}$ is a system that is computationally indistinguishable from an ideal random function $f^\star$, if k is chosen uniformly over $\mathcal{K}$.

A pseudo random function is a typical model for a cryptographic hash function

Example: pseudo random permutations

Ideal random permutations

An ideal random permutation $f^\star : \mathcal{X} \times \Omega \mapsto \mathcal{Y}$ is a random mapping such that

- $[f(x_1), \ldots, f(x_N)]$ is a random vector, uniformly distributed over all possible permutations of N distinct elements from $\mathcal{Y}$

Pseudo random functions

A secure pseudo random function $f : \mathcal{X} \times K \mapsto \mathcal{Y}$ is a system that is computationally indistinguishable from an ideal random permutation $f^\star$, if k is chosen uniformly and secretly over $\mathcal{K}$.

A pseudo random permutation is a typical model for a block cipher

Relationship between security definitions

Proposition

If a mechanism M is δ-unconditionally secure and its ideal counterpart $M^\star$ offers ε-unconditional security against a class $\mathcal{A}$ of attacks, then M offers $(\varepsilon+\delta)$-unconditional security against the same class $\mathcal{A}$.

Proof.

Since $d(M, M^\star) \leq \delta$, there exist a joint conditional distribution of the outputs $p_{yy^\star|x}$ such that $\mathrm{P}\left[y \neq y^\star | x = a\right] \leq \delta$, $\forall a \in \mathcal{A}_x$.
Therefore, for all $A \in \mathcal{A}$, and by the total probabiity theorem

$$\begin{aligned}
\mathrm{P}\left[S_{\mathcal{A}}\,;\, A, M\right] &= \mathrm{P}\left[S_{\mathcal{A}}|y = y^\star\,;\, A, M\right]\mathrm{P}\left[y = y^\star\,;\, A, M\right] \\
&\quad + \mathrm{P}\left[S_{\mathcal{A}}|y \neq y^\star\,;\, A, M\right]\mathrm{P}\left[y \neq y^\star\,;\, A, M\right] \\
&\leq \mathrm{P}\left[S_{\mathcal{A}}\,;\, A, M^\star\right]\cdot 1 + 1\cdot\delta \\
&\leq \varepsilon + \delta
\end{aligned}$$

Bounded

$\square$

Relationship between security definitions

Similar relationship can be stated in the computational sense and can be proved analogously

Proposition

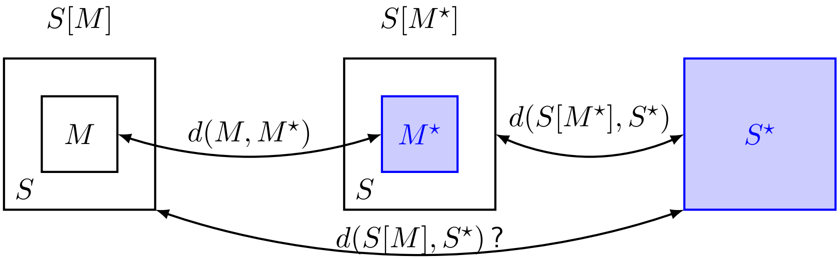
If a mechanism M *is* (δ, T_0)*-computationally secure and its ideal counterpart* $M^\star$ *offers* (ε, T_0)*-computational security against a class* $\mathcal{A}$ *of attacks, then* M *offers* $(\varepsilon + \delta, T_0)$*-computational security against the same class* $\mathcal{A}$*.*

Proposition

If a sequence of mechanisms $\{M_n\}$ *is computationally secure in the asyptotic formulation and its ideal counterparts* $\{M_n^\star\}$ *offer asymptotic computational security against a class* $\mathcal{A}$ *of attacks, then* $\{M_n\}$ *also offer asymptotic computational security against the same class* $\mathcal{A}$*.*

Composition of security mechanisms

Consider a security mechanism S that makes use of another mechanism M, and denote this occurrence by $S[M]$. Let $S[M^\star]$ denote the same mechanism S where M is replaced by its ideal counterpart $M^\star$, and $S^\star$ denote the ideal counterpart of S (which need not use M nor $M^\star$).



Is it possible to derive the security of $S[M]$ from those of M and $S[M^\star]$?

A trivial example

Consider the following mechanisms:

- S an encryption system employing a L-bit key but actually making use only of the first $L/2$ bits
- M a key generation mechanism that outputs a L-bit key where the first $L/2$ bits are deterministic and only the last $L/2$ bits are uniform

based on variational distance

$$d_{\mathsf{V}}(M, M^\star) = 2^{L/2}\left(\frac{1}{2^{L/2}} - \frac{1}{2^L}\right) + \left(2^L - 2^{L/2}\right)\frac{1}{2^L} = 2 - \frac{1}{2^{L/2-1}}$$

idem for $d_{\mathsf{V}}(S[M^\star], S^\star)$.
They are both insecure and $S[M]$ is totally insecure

The composition theorem

Theorem (unconditional)

If M *is* ε_1*-unconditionally secure and* $S[M^\star]$ *is* ε_2*-unconditionally secure, then* $S[M]$ *is* $(\varepsilon_1 + \varepsilon_2)$*-unconditionally secure*

Proof.

Follows from the triangular inequality property of distinguishability. In fact:

$$\begin{aligned} d(S[M], S^\star) &\leq d(S[M], S[M^\star]) + d(S[M^\star], S^\star) \\ &\leq d(M, M^\star) + d(S[M^\star], S^\star) \leq \varepsilon_1 + \varepsilon_2 \end{aligned}$$

□

By repeatedly applying the above result, we can generalize to N-fold uses of M in S

Corollary

If M *is* ε_1*-unconditionally secure and* $S[M^\star]$ *is* ε_2*-unconditionally secure, then* $S[M^N]$ *is* $(N\varepsilon_1 + \varepsilon_2)$*-unconditionally secure*

The composition theorem

Analogously, we can state without proof

Theorem (computational, concrete)

If M *is* (ε_1, T_0)*-computationally secure and* $S[M^\star]$ *is* (ε_2, T_0)*-computationally secure, then* $S[M]$ *is* $(\varepsilon_1 + \varepsilon_2, T_0)$*-computationally secure*

In the asymptotic form, the asymptotic security is retained even if M is used polynomially many times in S, as follows

Theorem (computational, asymptotic)

In the asymptotic formulation, if $\{M_n\}$ *is computationally secure and* $S_n[M_n^\star]$ *is computationally secure, then for any polynomial* $p(\cdot)$*,* $S_n[M_n^{p(n)}]$ *is computationally secure*

