Probability

Dr Emiliano De Cristofaro

(Slides partially prepared by Jens Groth)

Last updated, September 30, 2014

Why probability theory?

- Security definitions
  - What is the probability an attacker breaks a cryptographic scheme?
- Mathematical tools
  - Use mathematical reasoning about cryptographic schemes
- Probability theory in this module
  - Elementary but extensively used
  - If you don’t have much probability background, you’re expected to catch up this week!

Finite sets

- Sets $A = \{1,2\}$ $B = \{1,2,3,4\}$ $C = \{4\}$
- Empty set $\emptyset = \{\}$
- Subsets/supersets $A \subseteq B$
- Intersection $A \cap B = \{1,2\}$
- Disjoint sets $A \cap C = \emptyset$
- Union $A \cup C = \{1,2,4\}$
- Relative complement $B \setminus A = \{3,4\}$
- Cartesian product $A \times C = \{(1,4),(2,4)\}$
- Cardinality $|A| = 2$, $|\emptyset| = 0$
- Rules $|A \cup B| = |A|+|B|-|A \cap B|$

Probability mass

- Sample space $\Omega = \{a,b,\ldots,z\}$
- Probability mass function
  - $\Pr: \Omega \rightarrow [0;1]$
  - $\Pr(a) + \Pr(b) + \ldots + \Pr(z) = 1$
- Uniform distribution
  - All samples have equal probability mass $\Pr(a) = \Pr(b) = \ldots = \Pr(z)$
- Example
  - A die should have roughly 1/6 chance of landing on either side

Events

- Event $A \subseteq \Omega$
- Define $\Pr[A] = \sum_{x \in A} \Pr(x)$
- Immediate consequences
  - $\Pr[\varnothing] = 0$
  - $\Pr[\Omega] = 1$
  - $0 \leq \Pr[A] \leq 1$
- Define A and B independent events if

  $$\Pr[A \cap B] = \Pr[A] \Pr[B]$$

Various rules

- If $A \subseteq B$ then $\Pr[A] \leq \Pr[B]$
- $\Pr[A \cap B] \leq \min(\Pr[A], \Pr[B])$
- $\max(\Pr[A], \Pr[B]) \leq \Pr[A \cup B] \leq \Pr[A] + \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$
- $\Pr[A] - \Pr[B] \leq \Pr[A \setminus B] \leq \Pr[A]$

- Homework for next week:
  - Prove them

Conditional probability

- For B with $\Pr[B] > 0$ define

$$\Pr[A|B] = \Pr[A \cap B] / \Pr[B]$$

- Theorem: A and B are independent if and only if $\Pr[A|B] = \Pr[A]$

- Bayes theorem:

$$\Pr[A|B] = \Pr[B|A] \Pr[A] / \Pr[B]$$

Stochastic variables

- Random variable $X: \Omega \to R$
- Define

$$\Pr[X = y] = \Pr[X^{-1}(y)]$$

- Random variables

$$X: \Omega \to R,\ Y: \Omega \to S$$

  give the natural joint random variable

$$(X,Y): \Omega \to R \times S$$

- Independent random variables if for all x,y

$$\Pr[(X,Y)=(x,y)] = \Pr[X=x] \Pr[Y=y]$$

Dependent stochastic variables

- $X: \Omega \rightarrow R$, $Y: \Omega \rightarrow S$

- Properties
  - $\Pr[X=x|Y=y] = \Pr[(X,Y)=(x,y)] / \Pr[Y=y]$
  - $\Pr[X=x,Y=y] = \Pr[X=x|Y=y] \Pr[Y=y]$
- Useful observation
  - $\Pr[X=x|Y=y]\Pr[Y=y]+\Pr[X=x|Y\neq y]\Pr[Y\neq y] = \Pr[X=x]$
- Union bound
  - $\Pr[X=x \text{ or } Y=y] \leq \Pr[X=x] + \Pr[Y=y]$