Cryptography and Security

Lecture 3

Recalling Discrete Probability and One Time Pad

Lecture slides are adopted from slides of Dan Boneh

Discrete Probability

- Finite set $U = \{0,1\}^n$
- **Probability distribution** P over U:

  A function $P: U \longrightarrow [0,1]$ such that $\Sigma\, P(x) = 1$

  where $x \in U$.

  Examples:

  1.Uniform distribution: for all $x \in U$: $P(x) = 1/|U|$

  2.Point distribution at x_0: $P(x_0) = 1$, $\forall\, x \neq x_0$: $P(x) = 0$

- Distribution vector: (P(000), P(001), P(010), … , P(111))

Discrete Probability

- **Event**

For a set $A \subseteq U$: $Pr[A] = \Sigma P(x) \in [0,1]$ where $x \in A$ and $Pr[U]=1$.

Example: $U = \{0,1\}^8$

- $A = \{$ all x in U such that $lsb2(x)=11 \} \subseteq U$

for the uniform distribution on $\{0,1\}^8$:

$Pr[A] = 1/4$

Discrete Probability

- **Random Variable**

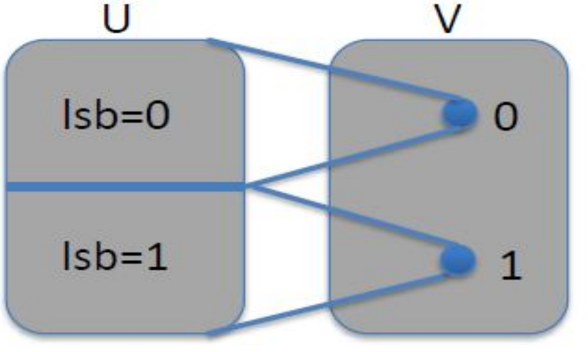
X is a function $X: U \longrightarrow V$

Example: $X: \{0,1\}^n \longrightarrow \{0,1\}$;

$X(y) = \text{lsb}(y) \in \{0,1\}$

For the uniform distribution on U:

Pr[X=0] = 1/2 , Pr[X=1] = 1/2



Discrete Probability

- **Uniform Random Variable**

  Let U be some set, e.g. $U = \{0,1\}^n$
- We write $r \longleftarrow U$ to denote a **uniform random variable** over U

  for all $a \in U$: $\Pr[\, r = a \,] = 1/|U|$

(formally, r is the identity function: $r(x)=x$ for all $x \in U$)

Discrete Probability

Let r be a uniform random variable on $\{0,1\}^2$

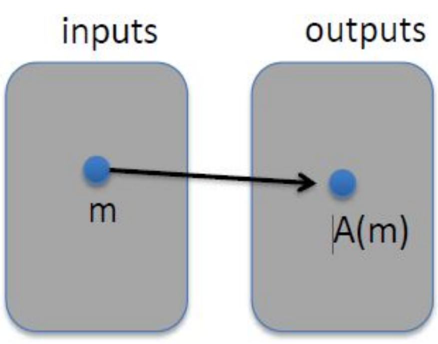
- Define the random variable X = r1 + r2

  Then Pr[X=2] = ¼

  Hint: Pr[X=2] = Pr[r=11]

Discrete Probability

- **Deterministic algorithm**: $y \longleftarrow A(m)$

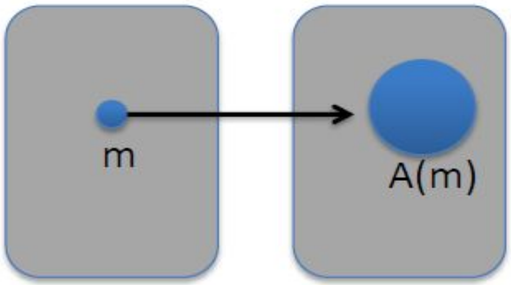


- **Randomized algorithm**

  $y \longleftarrow A(\, m \,;\, r \,)$ where $r \longleftarrow \{0,1\}^n$ R

output is a random variable $y \longleftarrow A(\, m \,)$

- Example: $A(m \,;\, k) = E(k, m)$, $y \xleftarrow{R} A(\, m \,)$ R



Discrete Probability

- **Independence**

events A and B are **independent** if

$$\textbf{Pr[A and B] = Pr[A] \cdot Pr[B]}$$

- random variables X,Y taking values in V are **independent** if

$\forall$ **a,b** $\in$ **V: Pr[X=a and Y=b] = Pr[X=a] · Pr[Y=b]**

- **Example**: $U = \{0,1\}^2 = \{00, 01, 10, 11\}$ and $r \xleftarrow{R} U$

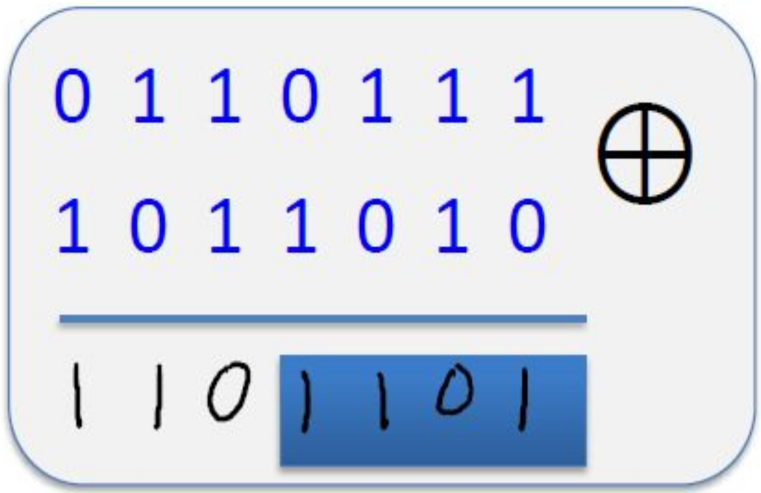
Define r.v. X and Y as: X = lsb(r) , Y = msb(r)

Pr[X=0 and Y=0] = Pr[r=00] = ¼ = Pr[X=0] · Pr[Y=0]

Review: XOR

- XOR of two strings in $\{0,1\}^n$ is their bit-wise addition mod 2

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0



An important property of XOR

- **Thm**: Y a rand. var. over $\{0,1\}^n$, X an indep. uniform var. on $\{0,1\}^n$, then Z := Y$\oplus$X is uniform var. on $\{0,1\}^n$

Proof: (for n=1)

$$\Pr[\,Z=0\,] = \Pr\big[(x,y)=(0,0) \text{ or } (x,y)=(1,1)\big] =$$

$$= \Pr\big[(x,y)=(0,0)\big] + \Pr\big[(x,y)=(1,1)\big] =$$

$$= \frac{p_0}{2} + \frac{p_1}{2} = \frac{1}{2}$$

Y	Pr
0	p_0
1	p_1

X	Pr
0	1/2
1	1/2

X	Y	Pr
0	0	$p_0/2$ ⇐
0	1	$p_1/2$
1	0	$p_0/2$
1	1	$p_1/2$ ⇐

The Birthday Paradox

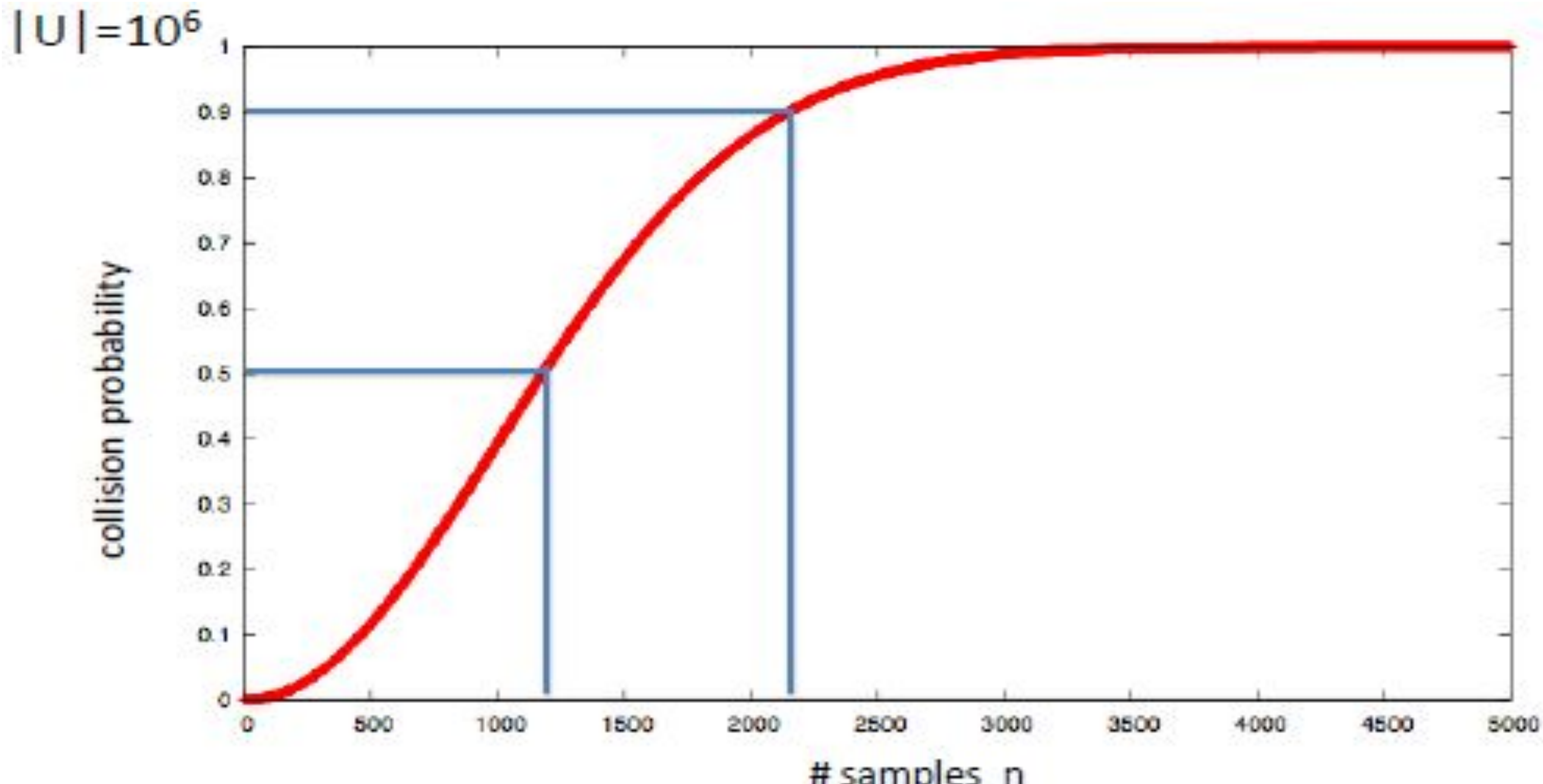
- Let $r_1, \ldots, r_n \in U$ be indep. identically distributed random vars.
- **Thm**:

  when **n**= $1.2 \times |\mathbf{U}|^{\mathbf{1/2}}$ then $\Pr[\ \exists\, i \neq j: r_i = r_j\ ] \geq ½$

  Example: Let $U = \{0,1\}^{128}$

  After sampling about 2^{64} random messages from U, some two sampled messages will likely be the same

The Birthday Paradox



Recalling Symmetric Cipher

A **cipher** defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

is a pair of "efficient" algs (***E***, ***D***) where

$$E: \mathcal{K} \times \mathcal{M} \to \mathcal{C} \quad , \qquad D: \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

$$\text{s.t.} \quad \forall m \in \mathcal{M}, k \in \mathcal{K}: \quad D(k, E(k, m)) = m$$

Where,

E is often randomized.

D is always deterministic.

One Time Pad

First example of a “secure” cipher where

$$\mathcal{M} = \mathcal{C} = \{0,1\}^n \quad , \qquad \mathcal{K} = \{0,1\}^n$$

key = (random bit string as long the message)

$$c := E(k, m) = k \oplus m$$

$$D(k, c) = k \oplus c$$

$$D(k, E(k,m)) = D(k, k \oplus m) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$$

given a message (*m*) and its OTP encryption (*c*), it is possible to compute the OTP key from *m* and *c* ?

One Time Pad

- Good point: very fast encryption and decryption.
- Bad news: long key (as long as plaintext)

Information Theoretic Security (Shannon 1949)

- CT should reveal no "info" about PT
- A cipher ***(E,D)*** over (K,M,C) has **perfect secrecy** if $\forall m_0, m_1 \in M$ ($|m_0| = |m_1|$) and $\forall c \in C$

$$\Pr[\, E(k,m_0)=c \,] = \Pr[\, E(k,m_1)=c \,] \quad \text{where } k \xleftarrow{R} K$$

$\Rightarrow$ Given CT can't tell if msg is m_0 or m_1 (for all m_0, m_1)

$\Rightarrow$ most powerful adv. learns nothing about PT from CT

$\Rightarrow$ no CT only attack!! (but other attacks possible)

One Time Pad (OTP)

- Lemma: OTP has perfect secrecy

Proof:

$\forall m, c$: $\quad \Pr_{k}\left[E(k,m)=c\right] = \dfrac{\#\text{keys } k \in \mathcal{K} \text{ s.t. } E(k,m)=c}{|\mathcal{K}|}$

e: if $\forall m, c$: $\quad \#\{k \in \mathcal{K} : E(k,m)=c\} = \text{const.}$

$\Longrightarrow$ cipher has perfect secrecy

One Time Pad (OTP)

Let $m \in \mathcal{M}$ and $c \in \mathcal{C}$.

How many OTP keys map $\boldsymbol{m}$ to $\boldsymbol{c}$?

None

1

2

Depends on $\boldsymbol{m}$

One Time Pad (OTP)

- Lemma: OTP has perfect secrecy

For OTP: $\forall m, c$: if $E(k,m) = c$

$\Longrightarrow k \oplus m = c \Longrightarrow k = m \oplus c$

$\Longrightarrow \boxed{\#\{k \in \mathcal{K} : E(k,m) = c\} = 1}$

$\Longrightarrow$ OTP has perfect secrecy ∎

OTP: no CT only attack (but other attacks are possible)

One Time Pad (OTP)

- Thm: Perfect secrecy $\Rightarrow \quad |\mathcal{K}| \geq |\mathcal{M}|$
- Implies that ***key length*** >= ***message length***
- Hard to use in practice.

https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/