Lecture Let 5

Sept 13, 2020

Last time

- Attack on Vigenère cipher
- Modern crypto — security goal, threat model; precise assumptions; formal proofs

Bayes Theorem

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

- $\mathcal{U}$ = {four coin tosses} — 16 ($2\times2\times2\times2$)

B = "atleast 3 H" A = "first toss is T"

$P(A) = \frac{1}{2} = \frac{8}{16}$

$P(B) = {}^4C_3 \left(\frac{1}{2}\right)^4 + \left(\frac{1}{2}\right)^4$ (3 H's, 4 H's)

$= \frac{4}{16} + \frac{1}{16} = \frac{5}{16}$

$P(B|A) = \left(\frac{1}{2}\right)^3 = \frac{2}{16}$ (why?)

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} = \frac{\frac{2}{16}\cdot\frac{8}{16}}{\frac{5}{16}} = \frac{\frac{1}{16}}{\frac{5}{16}} = \frac{1}{5}$$

$\mathcal{K}$: space of keys ($\mathcal{K} = \{0 \ldots 25\}$)

$\mathcal{M}$: space of plaintexts ($\mathcal{M}$ = "english sentences")

$\mathcal{C}$: space of ciphertexts

- distribution over $\mathcal{K}$ (defined by Gen) — 1/26
- distribution over $\mathcal{M}$ (defined by context)
- distribution over $\mathcal{C}$

$C = Enc_K(m)$ — defined by these dist.

Random variables

M, K, C

specific values

m, k, c

Ex:

$\mathcal{M} = \{kim, ann, boo\}$

$\mathcal{K} = \{0 \dots 25\}$

shift cipher.

$Pr[M = kim] = 0.5$

Prior

$Pr[M = ann] = 0.2$ $\quad Pr[M = boo] = 0.3$

$C = DQQ$

$$Pr[M = ann \mid C = DQQ] = \frac{Pr[C = DQQ \mid M = ann]\, Pr[M = ann]}{Pr[C = DQQ]}$$

($K = 3$, $Pr = 1/26$; $M = ann$, $Pr = 0.2$)

$$= \frac{1/26 \cdot 0.2}{1/52} = 0.4$$

$Pr[C = DQQ] = 1/52 \left[+ \; 0.2 \times 1/26 \;(K=3,\ M=ann) \;+\; 0.3 \times 1/26 \;(K=2,\ M=boo) \right] = 11/52$

counterexample (shift cipher is not perfectly secret)

$Pr[M = boo \mid C = DQQ] = 0.6$

$Pr[M = kim \mid C = DQQ] = 0$

Ideally should be the same

Mean it be kim #

Prior Δ

guess (*) $Pr[M = kim] = 0.5$

$Pr[M = ann] = 0.2$

$Pr[M = boo] = 0.3$

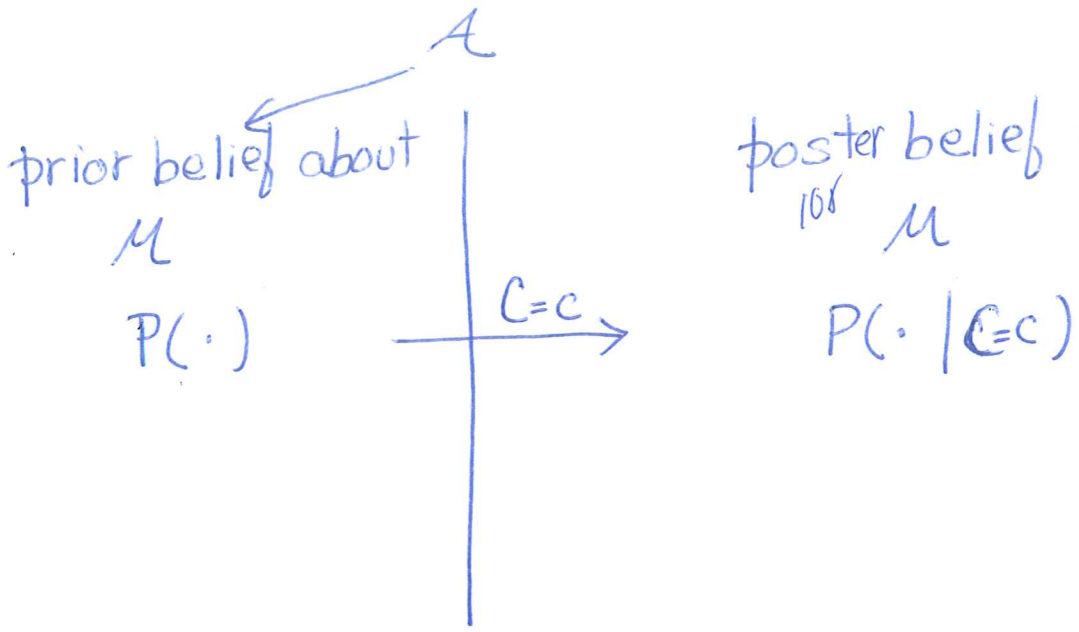
$C = DQQ$ →

Posterior Δ (*)

$Pr[M = kim \mid C = DQQ] = 0$

$Pr[M = ann \mid C = DQQ] = 0.4$

$Pr[M = boo \mid C = DQQ] = 0.6$ (*)



prior = posterior

$P(\cdot) = P(\cdot \mid C=c)$

ciphertext reveals nothing about the underlying plaintext and the adversary learns absolutely nothing about the plaintext that was encrypted.

↑ informally

Perfect secrecy

Def I ✓

Def I (preamble)

(An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret) if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and for every ciphertext $c \in \mathcal{C}$ for which $\Pr[C=c] > 0$

$$\Pr[M=m \mid C=c] = \Pr[M=m]$$

- $\Pr[M=m \mid C=c]$: posterior after seeing c (e.g. "xy..v" = 0.002)
- $\Pr[M=m]$: prior (e.g. "I love crypto" = 0.002)

technical condition: $\Pr[C=c]=0$ ↓ ciphertext can never be c

Prior distributions (for all) → all

$\Pr[M=m \mid C=c]$ ~~$= \Pr[M=m]$~~ (c) → posterior

Q: Is shift cipher perfectly secret?

Sept 16, 2020

Lecture Let 6

Last time
- Bayes thm
- Def I for Perfect secrecy

- Def II

An encryptios scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret if for every prob. distribution over $\mathcal{M}$ ~~every message $m \in \mathcal{M}$, and every~~ for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

- $\Pr[Enc_K(m) = c]$: prob. m can be encrypted to c
- $\Pr[Enc_K(m') = c]$: prob. m' can be encrypted to c

preamble

K: random key

$\Pr[C = c \mid M = m]$

equivalent

Def I $\Leftrightarrow$ Def II

- Def I $\Rightarrow$ Def II (Exercise)
- Def II $\Rightarrow$ Def I

Def II implies Def I

- Fix dist. over $\mathcal{M}$
- $m \in \mathcal{M}$, $c \in \mathcal{C}$, s.t $\Pr[C = c] > 0$ ← technical condition in Def I

To show: $\Pr[M = m \mid C = c] = \Pr[M = m]$ (Def I)

- $\Pr[M = m] = 0$

  $\Pr[M = m \mid C = c] = 0 = \Pr[M = m]$ ✓
- $\Pr[M = m] > 0$

$p_c = \Pr[Enc_K(m) = c]$ ↓ no dependence $\rightsquigarrow \Pr[Enc_K(m') = c]$ (Def II)

$$\Pr[M=m \mid C=c] = \frac{\Pr[C=c \mid M=m] \cdot \Pr[M=m]}{\Pr[C=c]} \quad \text{(Bayes)}$$

$$= \frac{\Pr[C=c \mid M=m] \cdot \Pr[M=m]}{\sum_{m' \in \mathcal{M}} \Pr[C=c \mid M=m'] \cdot \Pr[M=m']}$$

p_c = p_c (Def II)

m_1, m_2, m_3, m_4

$$= \frac{p_c \cdot \Pr[M=m]}{\sum_{m' \in \mathcal{M}} p_c \cdot \Pr[M=m']}$$

to prove.

$\Pr[M=m \mid C=c] = \Pr[M=m]$

$$= \frac{\Pr[M=m]}{\sum_{m' \in \mathcal{M}} \Pr[M=m']} \quad \text{distribution}$$

$$\sum_{m' \in \mathcal{M}} \Pr[M=m'] = 1$$

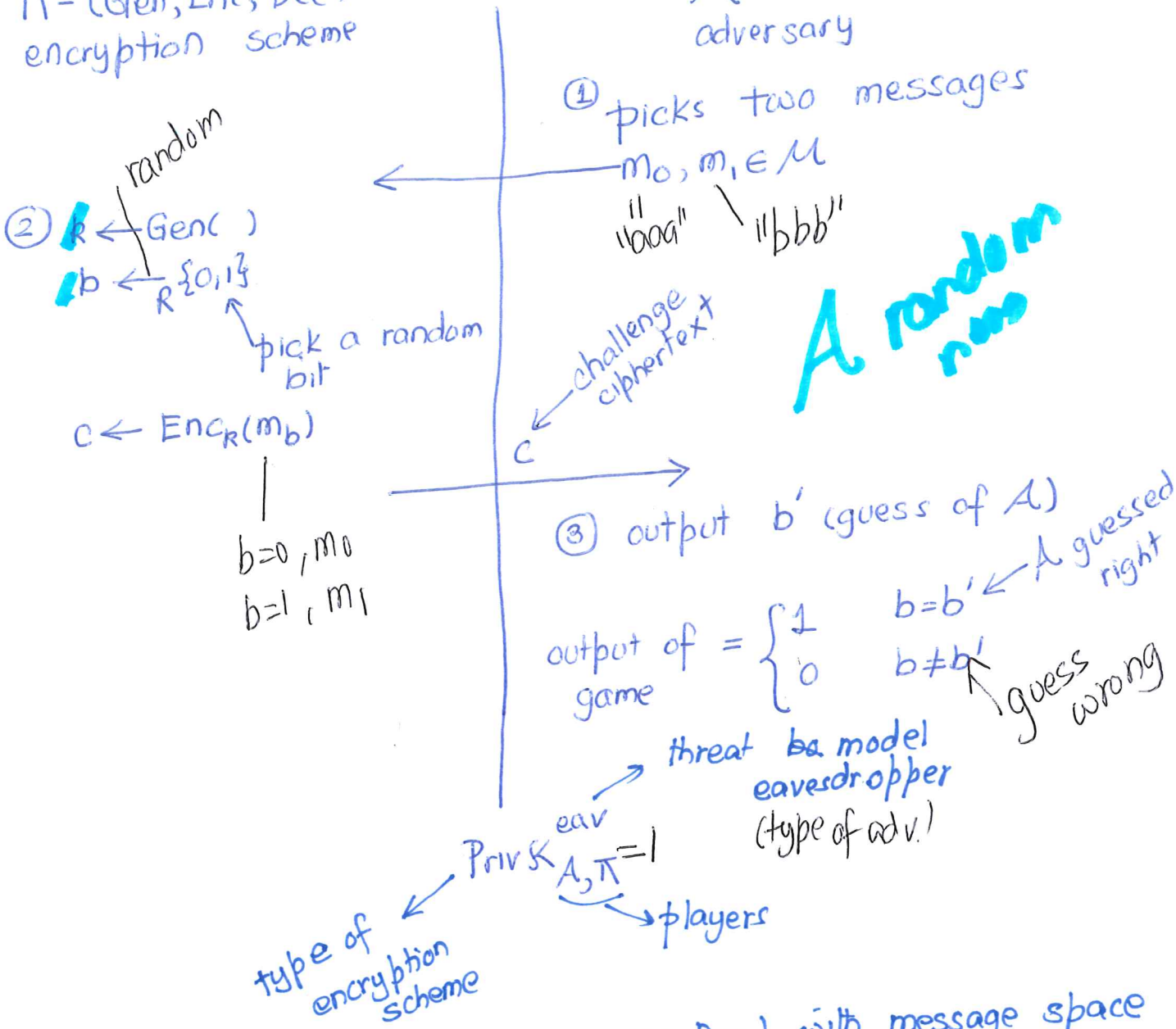
$$= \Pr[M=m]$$

Def III

Indistinguishability experiment

$\Pi = (Gen, Enc, Dec)$ encryption scheme

$\mathcal{A}$ adversary



Def III Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$ is perfectly indistinguishable if for every $\mathcal{A}$ it holds that

$$Pr[PrivK^{eav}_{\mathcal{A},\Pi} = 1] = 1/2$$

$\mathcal{A}$ winning game

perfectly secret

Some adversaries

- $\mathcal{A}$ always predicts 0

  $\Pr(b=0) = 1/2$

  ↑ picked by Π

- $\mathcal{A}$ always predicts 1

  $\Pr(b=1) = 1/2$

- $\mathcal{A}$ randomly guesses $b' \leftarrow \{0,1\}$

  $\Pr(b=b') = 1/2$

Perfect secrecy says no strategy can do better than

Hw:

$\mathcal{A}$ computes $\Pr[Enc_K(\cdot) = m_0] = p_0$; $\Pr[Enc_K(\cdot) = m_1] = p_1$ — argue $\mathcal{A}$ can compute these

c: challenge

$p_0 \geq p_1$ guess $b'=0$

$p_0 < p_1$ guess $b'=1$

analyze this!

Sept 18 2020

Lecture Let 7

Last time
- Def II
- Def III

→ indistinguishability game

One-time pad (OTP)

$\oplus$: xor

xor truth table $\oplus$

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

different bits are

$x \oplus x = 0$

$x \oplus 0 = x$

Ex:

$$\begin{array}{r} 11001 \\ \oplus\ 01100 \\ \hline 10101 \end{array}$$

Extending to bit string

$$\begin{array}{rccc} & x_1 & \cdots & x_k \\ \oplus & y_1 & \cdots & y_k \\ \hline & x_1 \oplus y_1 & \cdots & x_k \oplus y_k \end{array}$$

bitwise $\oplus$

OTP

$\ell = 1000$

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^{\ell}$$

ℓ-bit strings.

$$\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c]$$

— Def II of perfect secrecy.

(Gen, Enc, Dec)

Gen:

$k \leftarrow Gen$ (randomly generate)

↑ random ℓ-bit string

Enc:

$m = m_1 \dots m_\ell$

$k = k_1 \dots k_\ell$ (⊕ key with msg.)

$c = c_1 \dots c_\ell$

$c_i = m_i \oplus k_i$, $1 \le i \le \ell$

Dec:

$c = c_1 \dots c_\ell$

$k = k_1 \dots k_\ell$ (⊕ key with cipher text)

$m_1 \dots m_\ell$

$m_i = c_i \oplus k_i$, $1 \le i \le \ell$

Sanity check

$Dec_k(Enc_k(m)) = m$

small example.

$c_i = m_i \oplus k_i$

$1 \le i \le \ell$

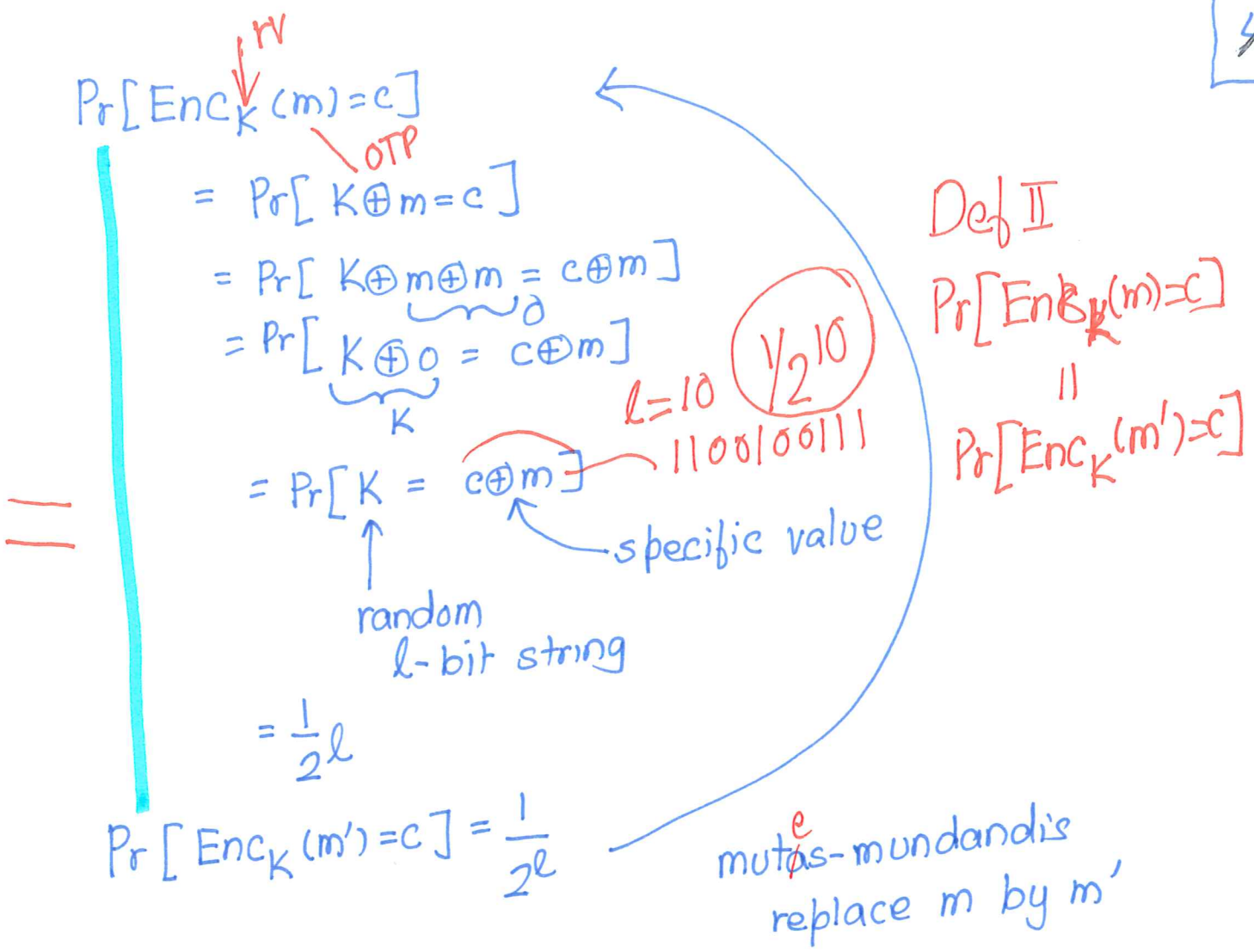
$(c_i \oplus k_i) = (m_i \oplus k_i) \oplus k_i$

$= m_i \oplus 0$

$= m_i$

OTP is perfectly secret

Use Def II



Bad news thm

:(

If $\Pi = (Gen, Enc, Dec)$ is a perfectly secret encryption scheme with msg space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$

contrapositive (implication)

perfect-secrecy $\Rightarrow$ $|\mathcal{K}| \geq |\mathcal{M}|$

$\neg(|\mathcal{K}| \geq |\mathcal{M}|) \Rightarrow \neg$perfect-secrecy

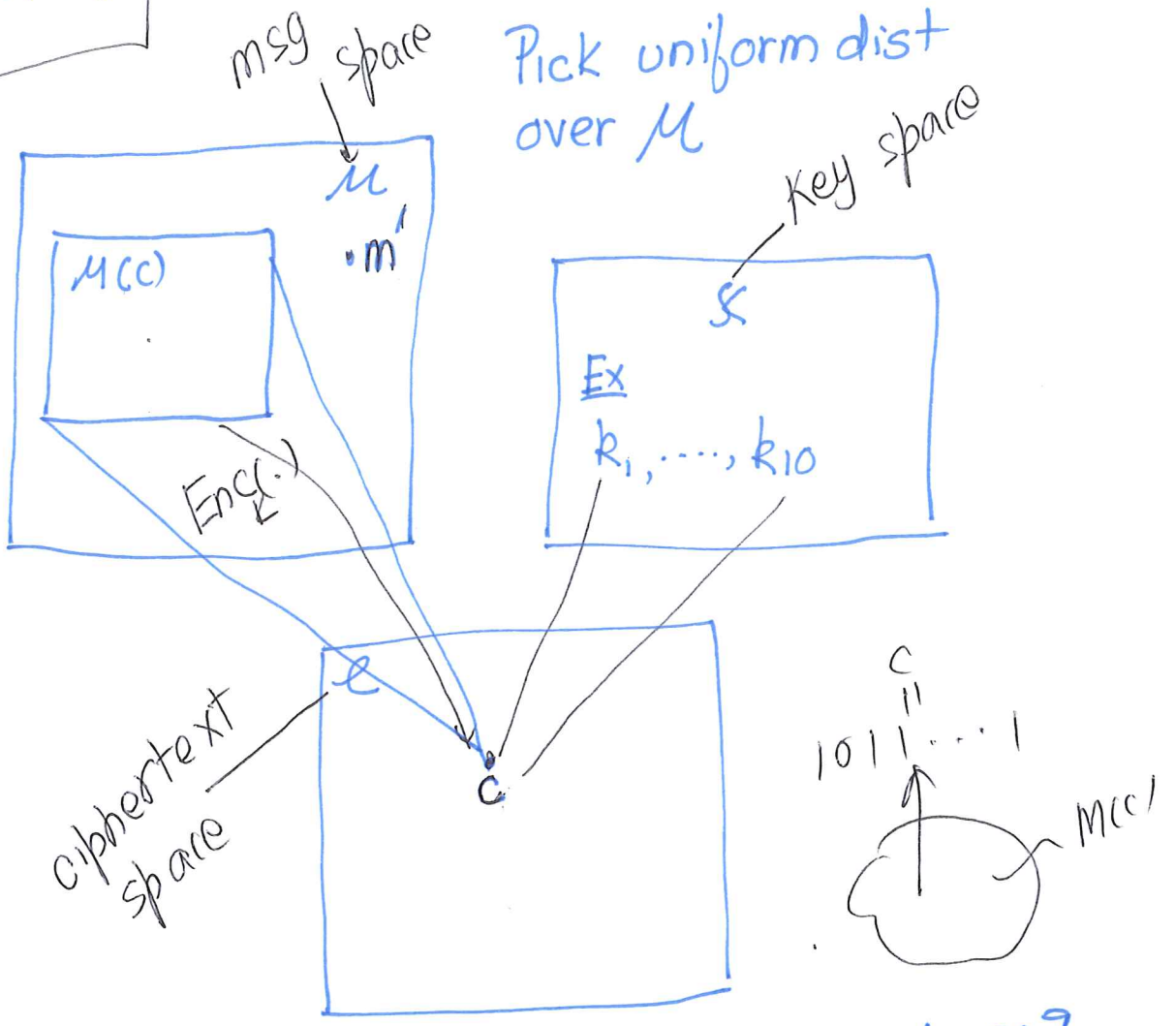
$|\mathcal{K}| < |\mathcal{M}| \Rightarrow \neg$perfect-secrecy

$a \Rightarrow b$
$\neg b \Rightarrow \neg a$

#

Assume $|K| < |M|$

$|K| \leq |M| \Rightarrow$ not perfectly-secret ✓



$M(c) = \{ m \mid m = Dec_k(c) \text{ for some } k \in K \}$

$Dec_k(Enc_k(m)) = c$

$|M(c)| \leq |K| < |M|$

$m' \notin M(c)$

$Pr[M = m'] > 0$

$Pr[M = m' \mid C = c] = 0$ ≠

How we chose m'?

Violates Def I

400MB ≅ m

400MB = K

Last time
- OTP
- Bad news Thm

Lecture Let 8

Sept 22, 2020

n (security parameter)
99% key size in bits
n=1000 (Key size is 1000 bits)

What we want?

n=1000 (key size)
should be able to encrypt messages of very large size (1G-bits)

Not possible with perfect secrecy (Why?)

Bad news Thm ($|K| \geq |M|$)

Need to weaken the definition

- Limit adversaries
  - probabilistic polynomial time (PPT)
    (e.g runs in time $n \log n$)
    - adv can use randomness
    - key size
    - sorting

Rules out exponential adversaries (2^n, $2^{\sqrt{n}}$, ...)
- 2^{1000}

- Adversary can potentially succeed with very small probability
  - breaking the scheme
  - will formalize later.

$\frac{1}{2^n}, \frac{1}{2^{\sqrt{n}}}, \ldots$

n=1000, $\frac{1}{2^{\sqrt{n}}}, \ldots$ $\frac{1}{2^{\sqrt{1000}}}$

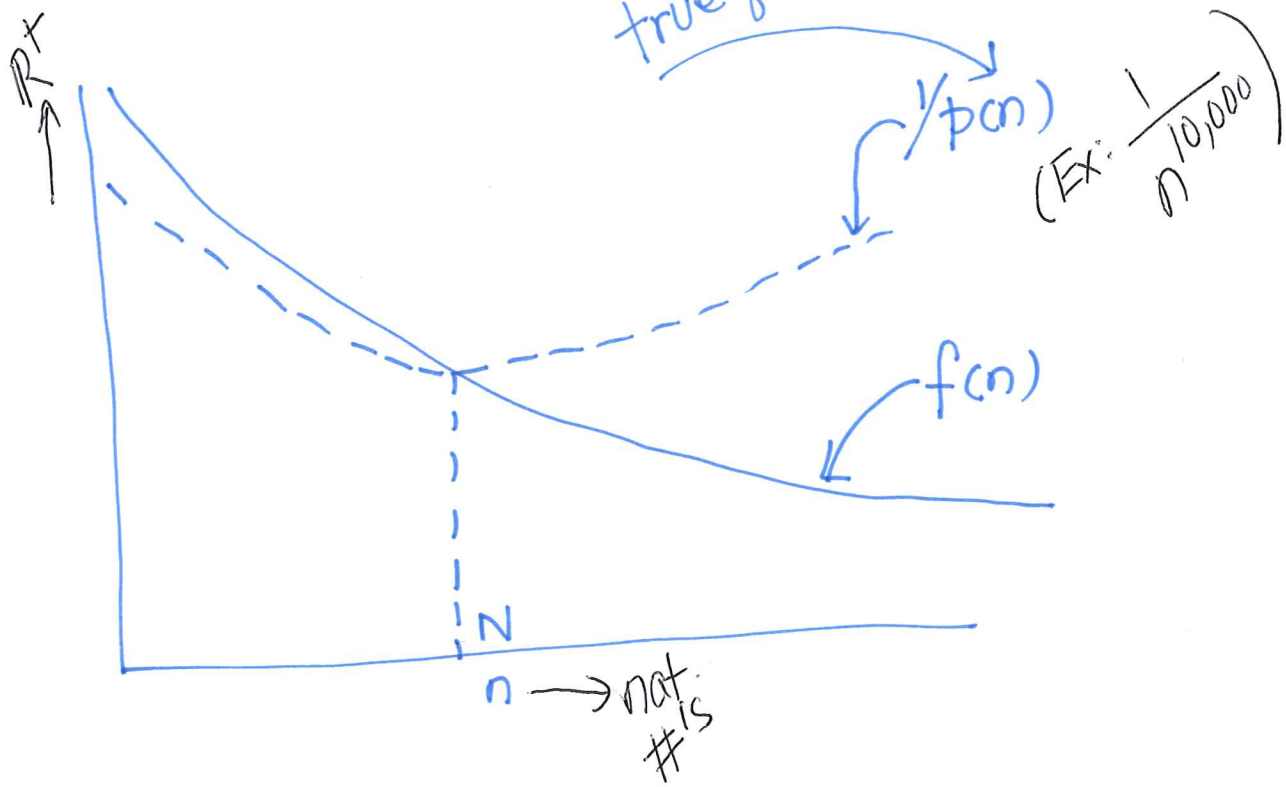
A scheme is secure if any PPT (probabilistic poly time) adversary succeeds in breaking the scheme with at most negligible probability.
(formalizes "very small")

Negligible functions

A function f from natural numbers to the non-negative real numbers is negligible if for every positive polynomial p there is an N s.t. for all $n > N$ it holds that

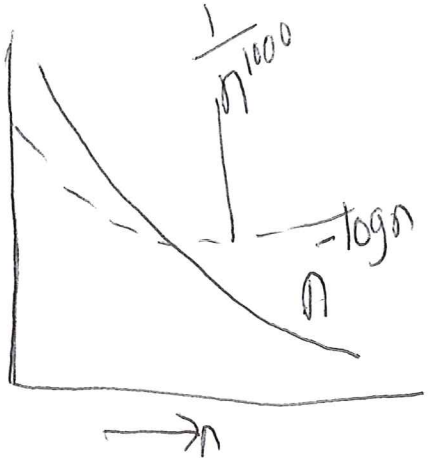
$$f(n) < \frac{1}{p(n)}$$

(true for every polynomial).



~~Darpa engagement~~

$2^{-n}, 2^{-\sqrt{n}}, n^{-\log n}$ } negligible



② $\frac{1}{n^2+n} > \frac{1}{3n^3}$ (not negligible, why?)

~~f+g~~

f, g negligible functions

p (positive polynomial)

closure properties

(I) $f(n)+g(n)=z(n)$ is negligible*

Ex: $2^{-n} + n^{-\log n}$ is negligible

(II) Ex: $p(n) = n^3+n^2+n$

• $\frac{n^3+n^2+n}{2^n}$ is negligible $\frac{1}{2^n}$

$p(n)f(n)$ is negligible*

Proof:

definition

$f(n), g(n)$ negl. — Assume

To prove: $f(n)+g(n)$ is negl ← negligible 2^{-n}

Let $p(n)$ be an arbitrary positive polynomial

~~There exists N s.t~~

To prove that there exists N s.t for all $n>N$

$f(n)+g(n) < \frac{1}{p(n)}$

there exists N_1 s.t for all $n > N_1$

$$f(n) < \frac{1}{2p(n)}$$

there exists N_2 s.t for all $n > N_2$

$$g(n) < \frac{1}{2p(n)}$$

$\frac{1}{2p(n)}$ → polynomial

$f(n), g(n)$ are negl. / why?

max

for all $n > N = \max(N_1, N_2)$

$$f(n) + g(n) < \frac{1}{2p(n)} + \frac{1}{2p(n)} \quad \text{(previous step)}$$

$$= \frac{1}{p(n)}$$

✓

(II) will be on HW!

Lecture Let 9

Sep 24, 2020

Last time
- Limiting the adv.
- negl. functions

- Relaxations are necessary

① n = "key size in bits" (sec. parameter)

A

$c_1, \ldots, c_\ell$ ← ciphertexts
$m_1, \ldots, m_\ell$ ← known-plaintext attack
msgs ci

Review this!

exhaustive attack

for k in $0..2^n-1$
  $\hat{m}_i = Dec_k(c_i)$
  $1 \le i \le \ell$
  stop when $(m_1 = \hat{m}_1, \ldots, m_\ell = \hat{m}_\ell)$

$0, \ldots, 2^n-1$
Ex: $0, \ldots 2^5-1$

k is the right key with very high prob.

$m = Dec_k(c)$ ← new ciphertext

$\neq$ → $O(2^n)$

Limiting A to PPT is necessary

② Random

$k \leftarrow 0 \ldots 2^n-1$
check $m_i = Dec_k(c_i)$?
$1 \le i \le \ell$

will guess right with prob. $1/2^n$

negl. fun

Allowing A to succeed by negl. probability is necessary

Private-key Encryption Scheme

(Gen, Enc, Dec)

Gen:

$k \leftarrow Gen(1^n)$ — sec. parameter (usually the key size)

$n = 100$

$1^{100} = \underbrace{11\ldots1}_{100 \text{ times}}$

$|k| \geq n$ — size of the key in bits

Enc

$c \leftarrow Enc_k(m)$ — m: message; c: ciphertext; k: key

$m \in \{0,1\}^*$ (arbitrary size) → bit string arbit len

$m \in \{0,1\}^{l(n)}$ (fixed size)

Ex: $l(n) = n^3$

$n = 100$

$(100)^3$

Dec

$m := Dec_k(c)$

$\leftarrow$ (randomness)

$:=$ (assign)

Sanity check: $Dec_k(Enc_k(m)) = m$

$\Pi = (Gen, Enc, Dec)$ $\quad 1^n$ $\quad \mathcal{A}$ (adv)

same

$k \leftarrow Gen(1^n)$

$b' \in_R \{0,1\}$, $b' \leftarrow \{0,1\}$

$c \leftarrow Enc_k(m_{b'})$ (challenge ciphertext)

① outputs m_0, m_1 — size of m_1 in bits

$|m_0| = |m_1|$

Indistinguishability game

② c

$\mathcal{A}$ outputs $b \in \{0,1\}$

$$output = \begin{cases} 1 & b = b' \text{ (guess right)} \\ 0 & b' \neq b \text{ (wrong)} \end{cases}$$

$PrivK^{eav}_{\mathcal{A},\Pi}(n)$

$\Pi = (Gen, Enc, Dec)$ is EAV-secure if for all PPT adversaries $\mathcal{A}$ there is a negligible function negl

has indistinguishable encryptions

$$Pr[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$

$\mathcal{A}$ winning

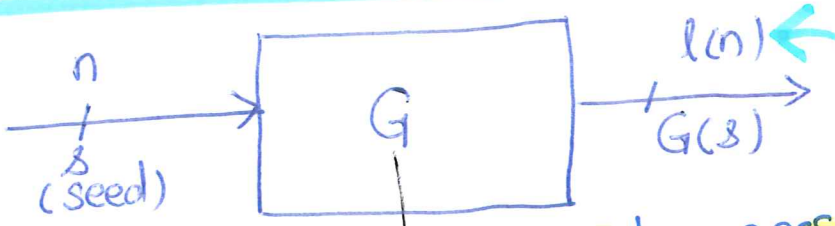
Limitation 1

Limitation 2

Psuedo-Random Generators (PRG)

Lecture Let 10 | 4

Sept 26, 2020



Expands randomness

expansion factor

- deterministic
- efficient

-Expansion

- expansion factor $\leftarrow l(n) > n$

D: distinguisher (PPT)
Neo

randomness

world 0

$s \leftarrow \{0,1\}^n$

G(s) given to D

l(n) bits

world 1

$r \leftarrow \{0,1\}^{l(n)}$

r given to D

D outputs 1 if Neo believes he is in world 0

D outputs 0

$|Pr[D(G(s))=1] - Pr[D(r)=1]| < negl(n)$

- for all PPT distinguishers D

Ex

concatenation

$G(s) = s \circ \bigoplus_{i=1}^{n} s_i$

$\bigoplus$ → ⊕ of all bits of s

xor

n-bit seed

$s_1 \dots s_n$

$\ell(n) = n+1 > n$: Expansion ✓

world 0

$s \leftarrow \{0,1\}^n$

G(s) given to D

world 1

$r \leftarrow \{0,1\}^{\ell(n)}$, $\ell(n) = n+1$

r given to D

PRG world

Random world

runs in PPT time

linear

$$D(r) = \begin{cases} 1 & r_{n+1} = \bigoplus_{i=1}^{n} r_i \\ 0 & \text{otherwise} \end{cases}$$

$D(r)$: $n+1$ bits

$\Pr[D(G(s))=1] = 1$

$\Pr[D(r)=1] = 1/2$

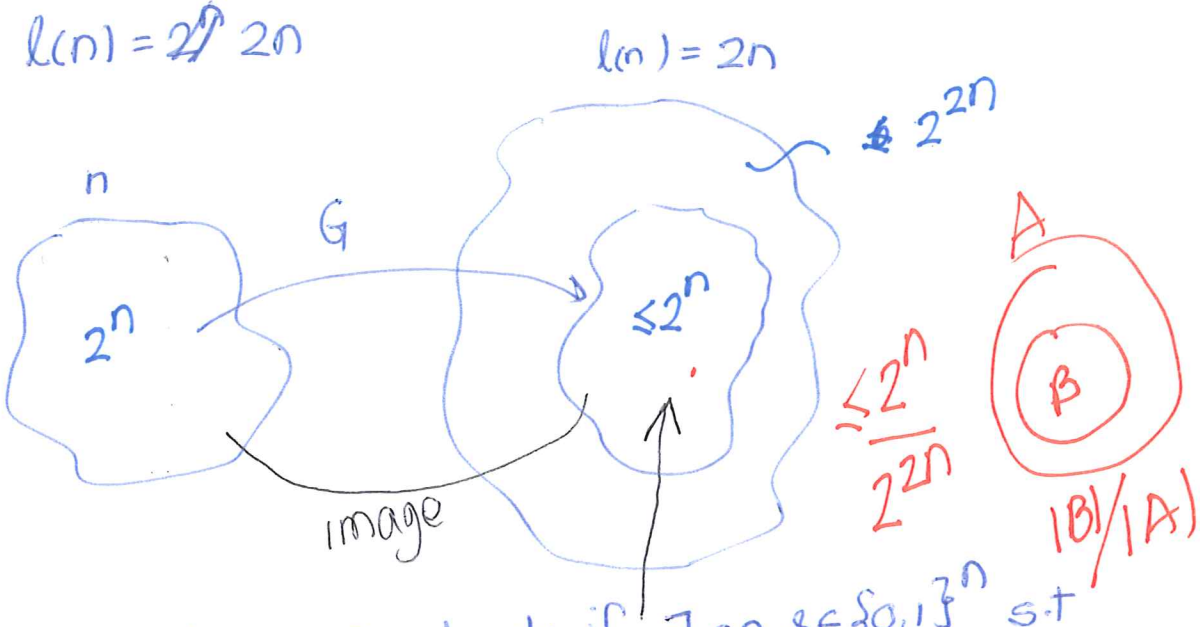
$r_1 \dots r_n \; r_{n+1}$

$\Pr = \bigoplus_{i=1}^{n} r_i$

$1 - 1/2 = 1/2$

not negligible

Is restriction of $\mathcal{D}$ to PPT necessary?



$\mathcal{D}(\omega) = \begin{cases} 1 \\ 0 \end{cases}$ ← $2n$-bits

if and only if $\exists$ an $s \in \{0,1\}^n$ s.t
$G(s) = \omega$
otherwise

runs in time 2^n | w exhaustive.

$s = 0, \cdots, 2^n - 1$
check $G(s) = \omega$

world 0 (PRG)
$s \leftarrow \{0,1\}^n$
$\mathcal{D}$ given $G(s)$

$\Pr[\mathcal{D}(G(s)) = 1] = 1$

world 1
$r \leftarrow \{0,1\}^{2n}$
$\mathcal{D}$ given r

$\Pr[\mathcal{D}(r) = 1] \leq \frac{2^n}{2^{2n}} = 2^{-n}$

$|\Pr[\mathcal{D}(G(s)) = 1] - \Pr[\mathcal{D}(r) = 1]| \leq 1 - 2^{-n} \neq \text{negl}.$

1 $\quad$ 2^{-n}

G be a PRG with expansion factor $\ell(\cdot)$

- Gen: $k \leftarrow Gen(1^n)$ ↑ random key of size n-bits

$k \in \{0,1\}^n \neq m \in \{0,1\}^{\ell(n)}$

- Enc: $c := G(k) \oplus m$ ($\ell(n)$, $\ell(n)$, $\ell(n)$)

OTP $|K| = |M|$

- Dec: $m := G(k) \oplus c$ $\quad Dec_k(m)$

Sanity check: $G(k) \oplus (G(k) \oplus m)$ $\quad Enc_k(m)$

$= m \oplus 0$

$= m$

Is it perfectly secret?

NO

Bad news Thm

$(\ell(n) > n)$ ← size of the key

↑ size of the msg