Michael Forbes
mforbes@illinois.edu

2018-03-07.4 → 2018-03-12.1
cs579

cs 579 : Computational Complexity : Lecture 16 67

admin : ps 3 back ; avg 34.

today : cryptography

Q : what is cryptography ?

eg : encryption Alice $\xrightarrow[E]{Enc(m)}$ Bob
m → m

bit commitment Alice $\xrightarrow{[b]}$ Bob
b

$\xrightarrow{k}$ $b' = b$

proof of work Alice $\xrightarrow{email}$ Bob
spam?

general : computation / interaction - allows good behavior
- disallows bad behavior

Q : complexity thy vs crypto
↓
says computational task is hard

meta fact : P=NP => "no crypto"

Complexity theoretic cryptography : formalize notions of security
identify reductions between cryptographic tasks
provide evidence separating cryptographic tasks

=

encryption : want : send information Alice → Bob

adversary : Eve to eves drop

Q : how to formalize ↗ ?

obs : encryption must be randomized, hide all information

eg : Alice $\xrightarrow{Enc(q_1)}$ Bob
$\xleftarrow{Enc(b_1, 00\cdots01)}$ $b_1, b_2 \in \{0,1\}$
$\xrightarrow{Enc(q_2)}$
$\xleftarrow{Enc(b_2, 0\cdots01)}$

Enc deterministic : $b_1 = b_2$ if $Enc(b_1) = Enc(b_2)$ ← can learn via eavesdropping

construction [One-Time Pad]

$k \leftarrow \{0,1\}^n$ given to Alice, Bob

$Enc : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

$x \quad k \to x \oplus k$ # parity of each bit #

$Dec = \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
$y \quad k \quad y \oplus k$

Michael Forbes
M.forbes@illinois.edu
~~2018-03-12-2~~ → 2018-03-12-1 → 2018-07-12-3
cs 579

lem: $Dec(Enc(x,k),k) = x$

$(x \oplus k) \oplus k = x$

def: (Enc, Dec) encryption scheme is perfectly secure if for all messages $m_1, m_2 \in \{0,1\}^n$ $\{Enc(m_1,k_1)\}_{k_1} \equiv \{Enc(m_2,k_2)\}_{k_2}$

worst case assumption; as and k_2

lem: one-time pad is perfectly secure

pf: any z, $Pr_{k_1}[Enc(m_1,k_1) = z] = Pr[m_1 \oplus k_1 = z]$

$= Pr[k_1 = z \oplus m_1]$

$= 1/2^n$

$= Pr_{k_2}[Enc(m_2,k_2) = z]$

function chosen indep of key k

cor: (Enc, Dec) encryption scheme perfectly secure $\Rightarrow$ any fixed function $f: \{0,1\}^n \to \{0,1\}$ any m_1, m_2

$Pr_k[f(Enc(m_1,k)) = 1]$

$= Pr_k[f(Enc(m_2,k)) = 1]$

$= Pr_k[f(Enc(0^n,k')) = 1]$

actual messages & key; available to eavesdropper

meta-defn: "anything" the adversary "can learn" by interacting w/ honest players, the adversary "can learn" w/ no interaction

Q: what's bad here?

A: to communicate n bits, need n pre-shared bits of rand

↳ sometimes ok, often no

A: this is information thy, not complexity

≡ question

defn: X, Y random variables over $\{0,1\}^n$

- are ε-statistically indistinguishable if for all $f: \{0,1\}^n \to \{0,1\}$

$|Pr[f(X)=1] - Pr[f(Y)=1]| \le \varepsilon$

denoted $\Delta(X,Y) \le \varepsilon$

← had $\varepsilon = 0$ in above

- are (t,ε)-computationally indistinguishable if for all $f: \{0,1\}^n \to \{0,1\}$ computed by a size $\le t$ ckt write $\Delta_t(X,Y) \le \varepsilon$

Rmk: - allow non-uniform attackers. to allow m_1, m_2 as advice

- interested in "efficient" adversaries

Q: t, ε?

Michael Forbes
miforbes@illinois.edu

2018-07-12.2 → 2018-08-12.3
2018-08-12.4 ← CS579

def: a function $f: \mathbb{N} \to \mathbb{R}_{\geq 0}$ is negligible if $f(n) \leq \frac{1}{n^{\omega(1)}}$, i.e. $\forall$ polynomial $p(n)$ $\exists N$

denoted $f(n) \leq \text{negl}(n)$ $\quad \forall n \geq N \quad f(n) \leq \frac{1}{p(n)}$

$P[E] \leq \text{negl} \Rightarrow E$ "rare" happens

def: an encryption scheme is $\text{Enc}: \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$, Dec

- Enc, Dec are probabilistic polytime
- any x, k $\Pr_{k \in \{0,1\}^k}[\text{Dec}(\text{Enc}(x,k),k) = x] = 1$
- any polynomial p, $\exists n$ $\forall x_1, x_2 \in \{0,1\}^n$
  $\Delta_{p(n,k)}(\text{Enc}(x_1, K), \text{Enc}(x_2, K)) \leq \text{negl}(k)$, $K \in \{0,1\}^k$
  → any efficient attackers fail, for large enough key sizes

Q: is there such a scheme?

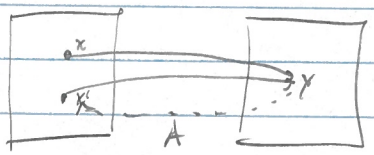
real life: yes (AES)

book: schemes $\Rightarrow P \neq NP$ ← worst case hardness

fact: $\Rightarrow$ avg case hardness

def: $f: \{0,1\}^* \to \{0,1\}^*$ is a one way function if

- easy to compute: $f \in FP$
- hard to invert: all probabilistic polytime A ← worst case hardness
  $\Pr_{x \in \{0,1\}^n, y = f(x)}[A(y) = x', f(x') = y] \leq \text{negl}(n)$ ← avg case hardness



eg: sample two random n-bit primes p, q, output $p \cdot q$

↳ use input x as randomness

Conj: ↗ is OWF ≟ hardness of factoring

Lem: $P = NP \Rightarrow$ no OWF

Pf: $L = \{(x,y) : \exists z \text{ s.t. } f(z) = y\} \in NP \Rightarrow P$

$y = f(x') \Rightarrow (x', y) \in L$

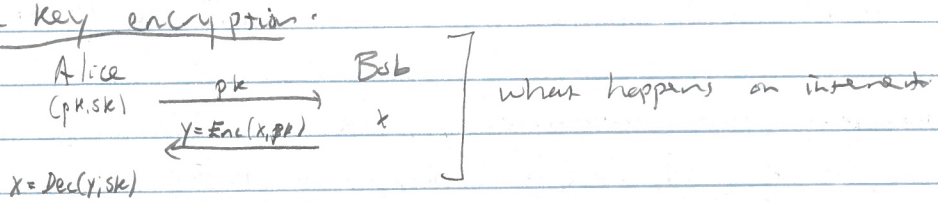
given $(x,y) \in L \Rightarrow (x0, y) \in L$ or $(x1, y) \in L$ or $f(x) = y$ ← search to decision

$\Rightarrow$ get $f(x) = y$

Michael Forbes
miforbes@illinois.edu
2018-03-12.3 ← 2018-03-15.1 → 2018-03-12.4
CS579

complexity theoretic crypto: assume OWF ⇒ encryption
bit commitment
proof of work
???

public key encryption:



when happens on internet

current worldview: OWF exist ≅ "secret key encryption"
⇏ "public key encryption"

next time: -
- zero knowledge proofs