Pseudorandomness

Write Solutions

Lets' recall intuitively what a pseudorandom string is

- a pseudorandom string looks like a uniformly distributed string to polynomial time viewers

Begin hws!

We say a distribution

- D is pseudorandom over strings length ℓ means D is indistinguishable from the uniform distribution over strings of length ℓ

$s \leftarrow \{0,1\}^n$ choose random seed uniformly

then output $G(s) \in \{0,1\}^\ell$

In symbols a PRG takes a uniform string s as a seed and outputs G(s) from $\{0,1\}^\ell$

$D \rightarrow 1?$

# of s → that map to $G(s)=y$

- $\Pr_D(y) = \dfrac{|\{s \in \{0,1\}^n \mid G(s)=y\}|}{2^n}$

$D \subset \{0,1\}^n$

$s \wedge G(s) = y$

Probability of choosing an element of D

$= \dfrac{1/\text{size of } D}{2^n}$

- Generally not Uniform

Now we will be using

- Pseudorandom strings will be used to generate a large pseudorandom string from a short seed.

- But let me point out a note between the uniform distribution and our Pseudorandom distribution

Informally a distribution D is Pseudo Random if no polynomial-time distinguisher can detect if a string is sampled from D or from the uniform distribution

Pseudorandom generators

We will formalize this by:
- Every polynomial-time algorithm outputs 1 with the same probability when given a TRS, and APRS

- A pseudorandom generator is a deterministic algorithm that recieves a short truly random seed and stretches it to a long pseudorandom ones.

- Deterministic Algorithm. * ✓

Def. Let $l(\cdot)$ be a polynomial and let G be a deterministic PT algorithm s.t. for all input $s \in \{0,1\}^n$, G outputs a string of length $l(n)$.

There are two requirements

G is a pseudorandom generator if

1. $\forall n$, $l(n) > n$
2. For all PPT distinguishers D, $\exists$ a negl function s.t.

$$\left| \Pr[D(r)=1] - \Pr[D(G(s))=1] \right| \leq negl(n)$$

where r is uniformly chosen from $\{0,1\}^{l(n)}$ and s is uniformly chosen from $\{0,1\}^n$

$D(r)$

1. Randomized experiment

- D is given r and runs some algorithm to distinguish if r is a uniform string or not from $\{0,1\}^{l(n)}$
  Returns 1 if

- D is given G(s) and runs an algorithm to distinguish if G(s) is a pseudorandom string from $\{0,1\}^{l(n)}$.

In both cases return ~~true~~ 1 if uniform

2. Distinguishers have G and may feed $\{0,1\}^n$ into G. $G(\{0,1\}^n)$ is not polynomial time.

Discussion

$\boxed{\text{-PRG are not random}}$

Does this one for $U_\ell^{2\ell}$ or $G(u)$

Take away's

1. PR distributions are far from random
2. For PPT attackers PRS are indistinguishable from uniform strings

Example - Consider $\ell(n) = 2n$ -

- Uniform distribution $\{0,1\}^{2n}$ is characterized by

2^{2n} possible strings with prob 2^{-2n} 2^{-2n}

- Distribution determined by G is at most size 2^n. The prob a random string is in range of G is at most $2^n / 2^{2n} = 2^{-n}$

Brute Force is non polynomial time.

- Trivial to decide between RS, PRS given unlimited time.

$D(w) = 1 \longleftrightarrow \exists s \in \{0,1\}^n$ s.t. $G(s) = w$. $*$

- If w was generated by G then D outputs 1 with prob 1

- If w is uniformly distributed in $\{0,1\}^{2n}$ then the probability that there exists an s with $G(s) \equiv w$ is at most 2^n

2^{-n}.

so D outputs 1 with prob at most 2^{-n}

$$\boxed{\Pr[D(r)=1] - \Pr[D(G(s))=1] = 1 - 2^{-n}}$$

≈ 1 for large n's!

The Seed and it's length

- The seed is uniformly chosen and kept secret

3.4 - Constructing Secure Encryption Schemes

The encryption scheme : Psuedo - One Time pad with expansion factor l

- Let G be ~~[illegible]~~ generator ← Psuedo random generator

- Gen : input 1^n , output $K \leftarrow \{0,1\}^n$ ← uniformly chosen

- Enc : Input $K \in \{0,1\}^n$, $m \in \{0,1\}^{l(n)}$

$$c := G(k) \oplus m$$

- Dec : Input $K \in \{0,1\}^n$, $c \in \{0,1\}^{l(n)}$

$$m := G(k) \oplus c$$

Thm. If G is a RRG then the POTP is asymptotically indistinguishable.

Proof.

1. Intuition

If Π used a random string as key then Π is onetimepad.

Therefore A is unable to guess ~~setting~~ Message with prob $1/2$.

Then A must be distinguishing the output of G from a random string.

- Let A be a ppt adversary,

neglible?

$$\varepsilon(n) = Pr[\, PrivK^{cav}_{A,\Pi}(n) = 1] - 1/2$$

- Use A to construct D for PRG G, s.t D succeeds with prob $\varepsilon(n)$

- D is given a string w, it determines whether W was chosen uniformly at random or whether $w := G(k)$

- D emulates the experiment for A and observes if A succeeds or not

- If A succeeds then D guesses W is pstring.
If A fails then D guesses W is RS.

Distinguisher D

D is given as input $w \in \{0,1\}^{l(n)}$

① Run $A(1^n)$ to obtain $m_0, m_1 \in \{0,1\}^{l(n)}$

② Choose $b \leftarrow \{0,1\}$. Set $c := w \oplus m_b$

③ Give c to A and obtain output b'.

Output 1 if $b' = b$ and output 0 O/W.

Randomized experiment

1.

2

By Secrecy of the OTP

$$\Pr[\mathrm{PrivK}_{A,\tilde{\Pi}}(n) = 1] = 1/2.$$

Let $\tilde{\Pi} = (\widetilde{Gen}, \widetilde{Enc}, \widetilde{Dec})$ be the one time pad

$Gen(1^n)$

B/c A is given $c = w \oplus m_b$ where $w \in \{0,1\}^{l(n)}$ is a uniform string

Observe

① If w is chosen uniformly from $\{0,1\}^{l(n)}$ then A when run by D is distributed identically to A in experiment $\mathrm{PrivK}_{A,\tilde{\Pi}}(n)$.

② If $w = G(k)$ for $k \leftarrow \{0,1\}^n$, then the view of A when run as a subroutine of D is distributed identically to the view of A in $\mathrm{PrivK}_{A,\Pi}(n)$.

Therefore it follows when $w \leftarrow \{0,1\}^{l(n)}$ is chosen uniformly

$$\Pr[D(w)=1] = \Pr[\mathrm{PrivK}_{A,\tilde{\Pi}}(n)=1] = 1/2 \text{ by } (1.)$$

When $w = G(k)$ for $k \leftarrow \{0,1\}^n$ chosen uniformly

we have

$$\Pr[D(w)=1] = \Pr[D(G(k))=1] = \Pr[\mathrm{PrivA}_{A,\Pi}(n)]$$

$$= \frac{1}{2} + \varepsilon(n)$$

Therefore

$$\left| \Pr[D(w)=1] - \Pr[D(G(s))=1] \right| = \varepsilon(n)$$

where w, s are chosen uniformly

Then since G is PRF, $\varepsilon(n)$ is a not negligible

Conclusion

- For PPT adversary we have a secure encryption that has |key| < message length.

But what if we have multiple messages?

We will begin to explore this now and over the next few days.