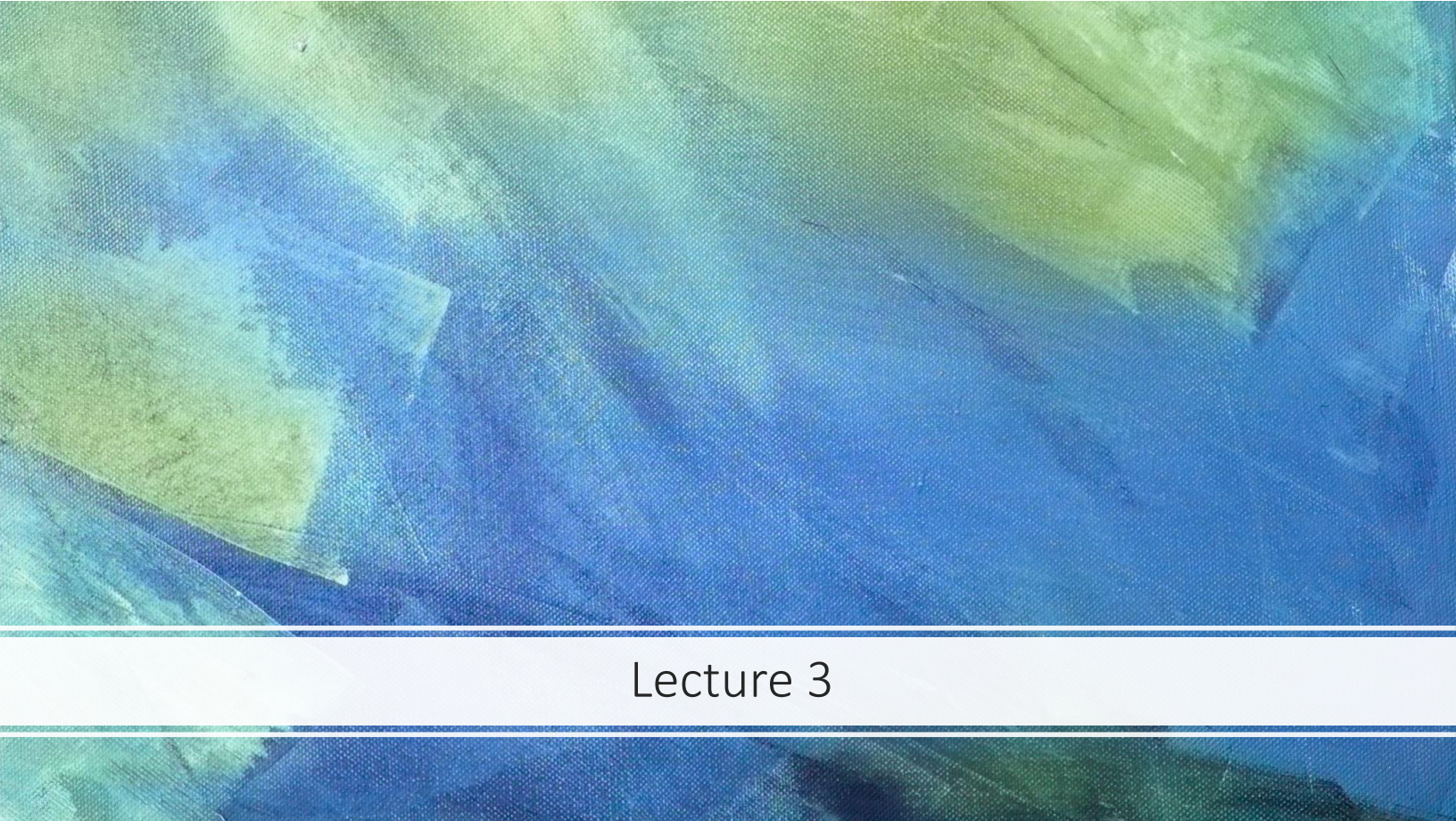
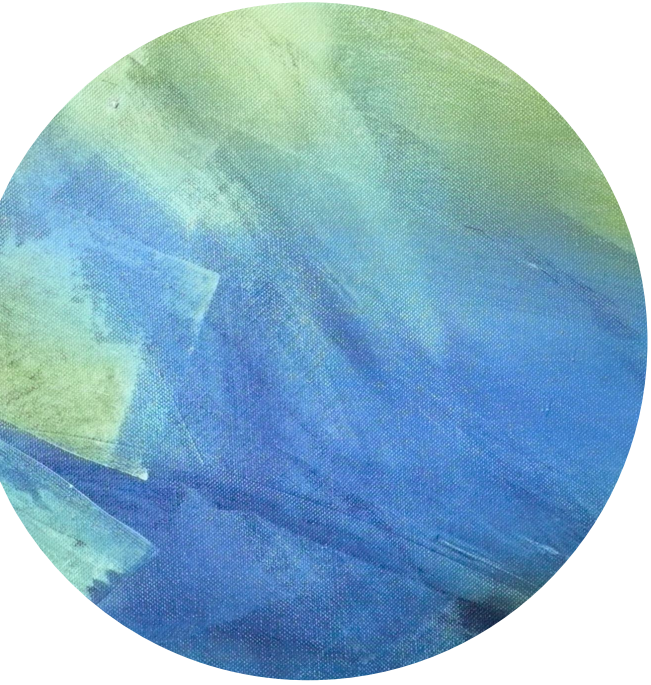


Lecture 3



Introduction

Pseudorandom Generators

Stream Ciphers

Examples and Attacks

Scribe : Alex Yuen

Administrative Details

- Course website:
  https://courses.grainger.illinois.edu/cs498ac3/fa2020/
  cs407/fa2022
- Has syllabus, instructor and TA info, office hours
- IMPORTANT: **Join Piazza!**
  piazza.com/illinois/fall2020/cscecs498ac3/home

I strongly encourage class participation.
If you don't understand something in class, please interrupt me and ask questions.
Please make abundant use of office hours.

Pseudorandomness

ONE-TIME PAD.

$$Enc(m, k) = m \oplus k : ct$$

$$Dec(ct, k) = ct \oplus k : m$$

Thm. Perfect secrecy is impossible when $|K| < |M|$

$$\left[\forall\, m_0, m_1, c \quad \Pr_{k \leftarrow K}[c = E(k, m_0)] = \Pr_{k \leftarrow K}[c = E(k, m_1)] \right]$$

To use a one-time pad, always need a key that is at least as large as the message / plaintext you're trying to encrypt.

But this is impractical, so what should we do?

- Use pseudorandomness
- Save a short "*random*" key and expand to a longer "*pseudorandom*" key
- Pseudorandom generator is a deterministic function G: $\{0,1\}^n \rightarrow \{0,1\}^{3n}$

CRYPTOGRAPHIC

$\forall i$, $G(i)$ is fixed, unique.

$3n$-bit long msg m.

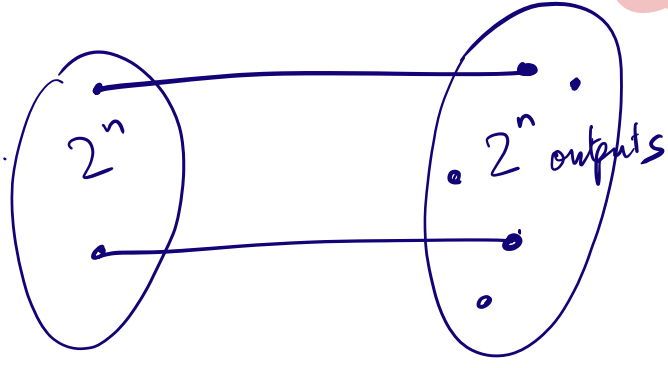
n-bit long key k.

$Enc(m, k) = G(k) \oplus m$

But this is impractical, so what should we do?

- Use pseudorandomness
- Save a short "*random*" key and expand to a longer "*pseudorandom*" key
- Pseudorandom generator is a deterministic function G: $\{0,1\}^n \rightarrow \{0,1\}^{3n}$

CRYPTOGRAPHIC



2^{3n} strings of length $3n$, outputs of G are 2^n in number

But this is impractical, so what should we do?

- Use pseudorandomness
- Save a short "*random*" key and expand to a longer "*pseudorandom*" key
- Pseudorandom generator is a deterministic function $G: \{0,1\}^n \rightarrow \{0,1\}^{3n}$

CRYPTOGRAPHIC

WORLD #1

Sample $y \leftarrow \{0,1\}^{3n}$

y →

$\Pr[y = G(x) \text{ for some } x] = \frac{2^n}{2^{3n}} = \frac{1}{2^{2n}}$

WORLD #2

Sample $x \leftarrow \{0,1\}^n$ → 256.

$y = G(x)$

y →

$\Pr[y = G(x) \text{ for some } x] = 1$

Impossible to distinguish world #1 from #2 in time poly(n).

What Properties Should a PRG Have?

- Masking with PRG should be "morally equivalent" to uniform mask
- At least need some type of unpredictability
  say $G(x_1x_2\ldots x_n) = y_1y_2\ldots.y_{3n}$

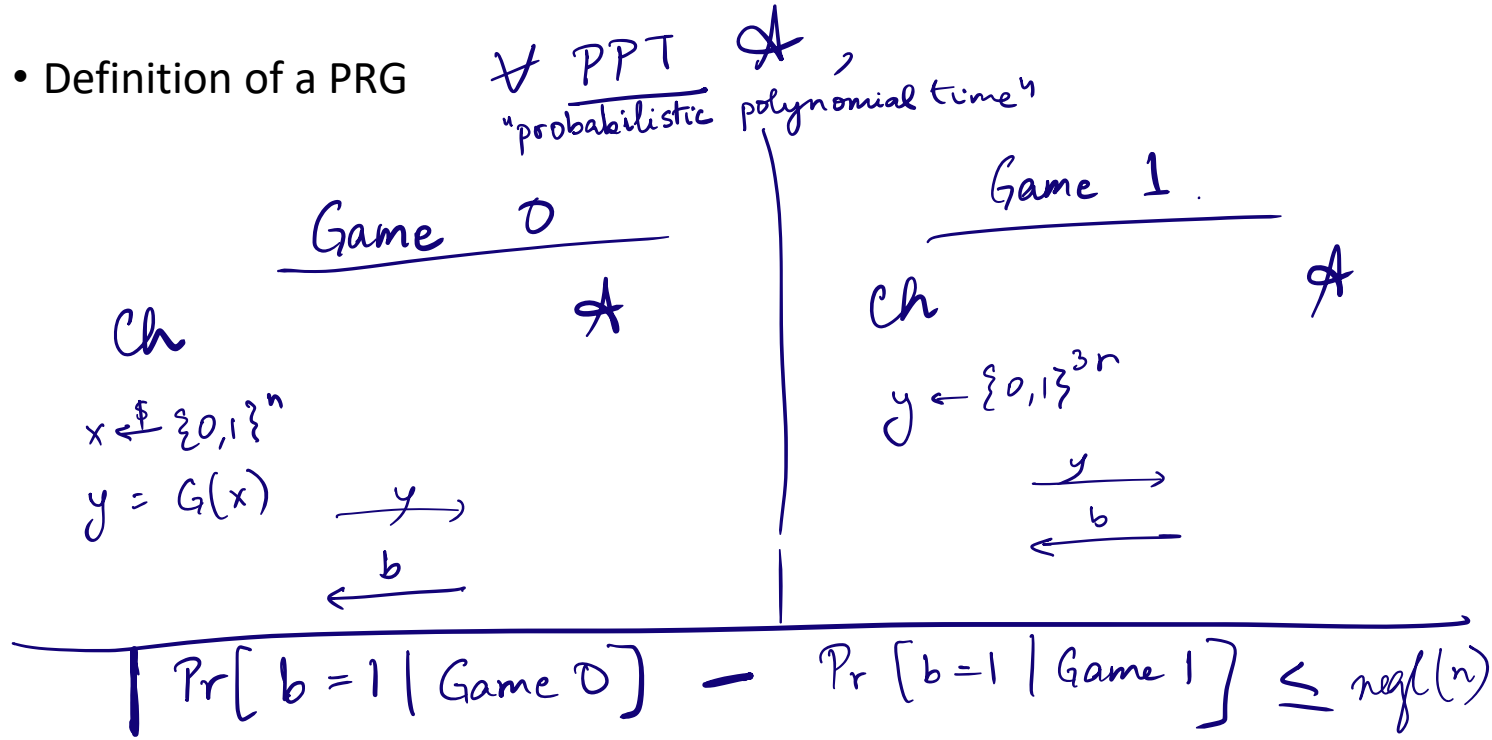
[Next-bit unpredictability] $y_1 y_2 \cdots y_{3n-1}$: Suppose easy to predict y_{3n}

[Missing bit unpredictability] $(y_1, y_2 \cdots y_{i-1})$ $(y_{i+1} \cdots y_{3n})$ $O(2^{3n})$

against adv. running in time poly(n).

What Properties Should a PRG Have?

- Definition of a PRG



What are Negligible Functions?

- In practice, **ε** is a scalar and
  - **ε** non-neg: **$\varepsilon \geq 1/2^{30}$** (likely to happen over 1GB of data)
  - **ε** negligible: **$\varepsilon \leq 1/2^{80}$** (won't happen over life of key)

- In theory, **ε** is a function **$\varepsilon: Z^{\geq 0} \longrightarrow R^{\geq 0}$** and

  $n = \lambda$ = length of key.

  - **ε** non-neg: **$\exists d: \varepsilon(\lambda) \geq 1/\lambda^d$** inf. often ($\varepsilon \geq$ 1/poly, for inf. many λ)
  - **ε** negligible: $\forall d, \exists \lambda_0$ s.t. $\forall \lambda \geq \lambda_0$: **$\varepsilon(\lambda) \leq 1/\lambda^d$** ($\varepsilon \leq$ 1/poly, for all large enough λ)

↓ Asymptotically smaller than EVERY inverse polynomial.

What are Negligible Functions?

- Are the following functions negligible?
  - $f(\lambda) = 1/2^{\lambda}$ Yes, smaller than $\frac{1}{\lambda^c}$ for all $c > 0$.
  - $f(\lambda) = 1/\lambda^{30000}$ No, $> \frac{1}{\lambda^c}$ for some c.
  - For odd λ, $f(\lambda) = 1/2^{\lambda}$, and for even λ, $f(\lambda) = 1/\lambda^{30000}$ No.

for even λ, $f(\lambda)$ is inverse poly.

- For $\lambda = 1, 2, 3 \ldots 10$, $f(\lambda) = \frac{1}{\lambda^2}$ Yes.

$\lambda = 11$ onwards, $f(\lambda) = \frac{1}{2^{\lambda}}$

Stream Ciphers

A PRG-Based Stream Cipher

- E (k, m) = $m \oplus G(k)$
- D (k, c) = $c \oplus G(k)$

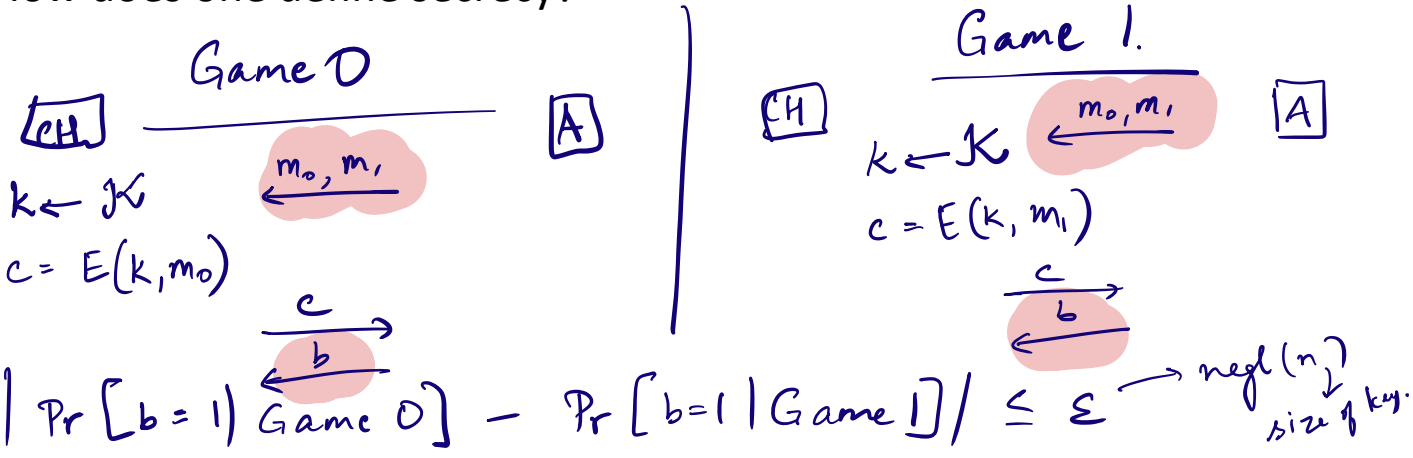
- Can this cipher have perfect secrecy?

No, key is smaller than message.

A PRG-Based Stream Cipher

- E (k, m) =
- D (k, c) =
- How does one define secrecy?

indistinguishability under CHOSEN PLAINTEXT ATTACK.



$$\left| \Pr[b = 1 \mid \text{Game } 0] - \Pr[b = 1 \mid \text{Game } 1] \right| \leq \varepsilon \rightarrow \text{negl}(n)$$

size of key.