Pseudo-Random Generators and Functions

Unveiling the Complexity and Elegance of Randomness

Ji Yong-Hyeon & Kim Dong-Hyeon

Department of Information Security, Cryptology, and Mathematics

hacker3740@gmail.com, eastchord0729@gmail.com

I. Introduction

현대암호학에서 블록암호가 가지는 성질 중 하나는 안전한 의사난수 순열(Pseudorandom Permutation, PRP)로 간주된다는 것이다. PRP의 안전성에 대해 논하기 전에, 먼저 의사난수 생성기(Pseudorandom Generator, PRG)의 안전성이 선행되어야 한다. 안전한 PRG라고 할지라도, 사용 방식에 따라 PRP의 안전성이 보장되지 않을 수 있다. PRP의 안전성에 대해 논하기 전에, PRG와 의사난수 함수(Pseudorandom Function, PRF)의 정의에 대한 이해가 필요하다. 본 고에서는 안전한 PRG, PRF, 그리고 PRP의 정의를 의사코드 형식으로 표현하고, 안전하지 않은 PRG와 PRF의 시각적 이해를 돕는다.

II.1 What is the PRG?

A deterministic function

$$G : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda+l}$$

with $l > 0$ is a **secure pseudorandom generator (PRG)** if $\mathcal{L}^{G}_{\text{PRG}-\text{real}} \approx \mathcal{L}^{G}_{\text{PRG}-\text{rand}}$, where:

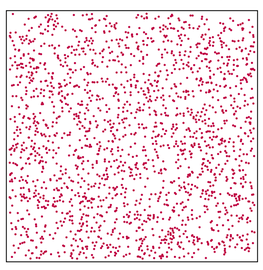
$\mathcal{L}^{G}_{\text{PRG}-\text{real}}$

Query():
$s \leftarrow \{0,1\}^{\lambda}$
return $G(s)$

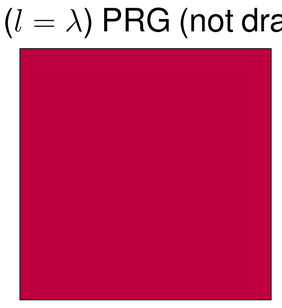
$\mathcal{L}^{G}_{\text{PRG}-\text{rand}}$

Query():
$r \leftarrow \{0,1\}^{\lambda+l}$
return r

We illustrate the distributions, for a length doubling ($l = \lambda$) PRG (not drawn to scale):



Pseudorandom dist. ($\{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$)



Uniform dist. ($\{0,1\}^{2\lambda}$)

II.2 How NOT to Build a PRG

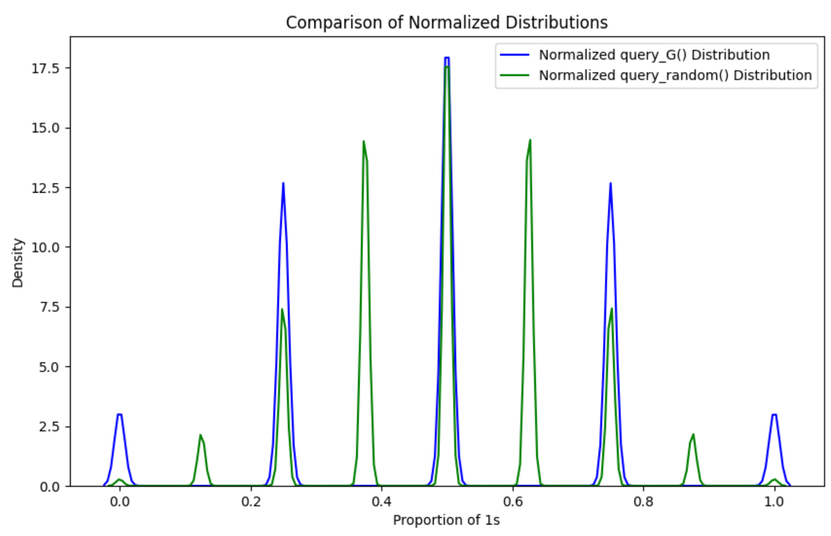
A straightforward approach for the PRG might be to duplicate its input string.

$G(s)$:
return $s \parallel s$

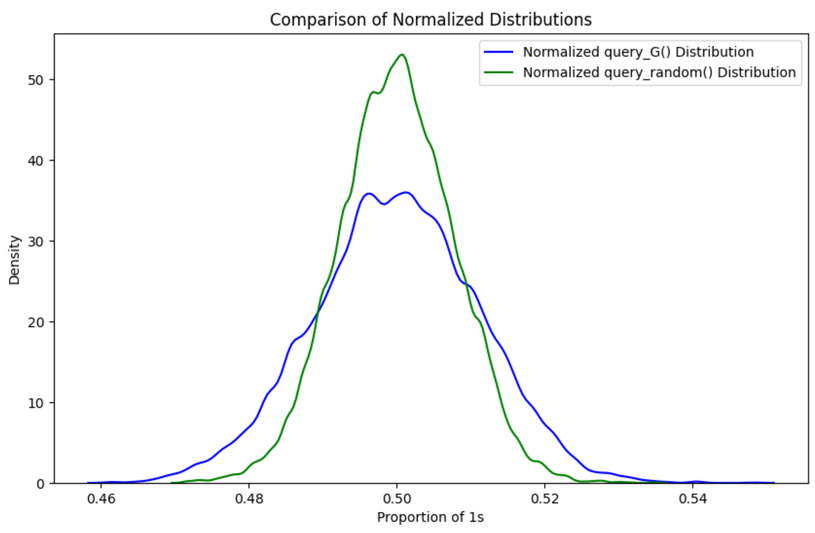
For example, the following strings look likely they were sampled uniformly from $\{0,1\}^{8}$:

$$11011101, 01110111, 01000100, \cdots$$

Comparison of Normalized Distributions:



$\lambda = 4$, i.e., $\{0,1\}^{8}$ with 1,000,000 experiments.



$\lambda = 1024$, i.e., $\{0,1\}^{2048}$ with 100,000 experiments

III.1 What is the PRF?

The following encryption scheme is information-theoretically secure.

The goal of a pseudorandom function is to "*look like*" a uniformly chosen array / lookup table.

for $x \in \{0,1\}^{\text{Idx}}$
$T[x] \leftarrow \{0,1\}^{\text{Out}}$

Lookup $(x \in \{0,1\}^{\text{Idx}})$:
return $T[x]$

Array T

Index $x_{\text{Idx}-1} \cdots x_1 x_0$	Output $T[x]$	Binary String Mapping
000	$T[000]$	1100100010 ···
001	$T[001]$	0110000101 ···
⋮	⋮	

$k \leftarrow \{0,1\}^{\lambda}$

Lookup $(x \in \{0,1\}^{\text{Idx}})$:
return $F(k,x)$

Pseudorandom Function F

Input $(x \in \{0,1\}^{\text{Idx}})$
Seed $(k \in \{0,1\}^{\lambda})$
→ Output $(\{0,1\}^{\text{Out}})$

A deterministic function

$$F : \{0,1\}^{\lambda} \times \{0,1\}^{\text{Idx}} \to \{0,1\}^{\text{Out}}$$

is a **secure pseudo-random function (PRF)** if $\mathcal{L}^{F}_{\text{PRF}-\text{real}} \approx \mathcal{L}^{F}_{\text{PRF}-\text{rand}}$, where

$\mathcal{L}^{F}_{\text{PRF}-\text{real}}$

$k \leftarrow \{0,1\}^{\lambda}$

Lookup $(x \in \{0,1\}^{\text{Idx}})$:
return $F(k,x)$

$\mathcal{L}^{F}_{\text{PRF}-\text{rand}}$

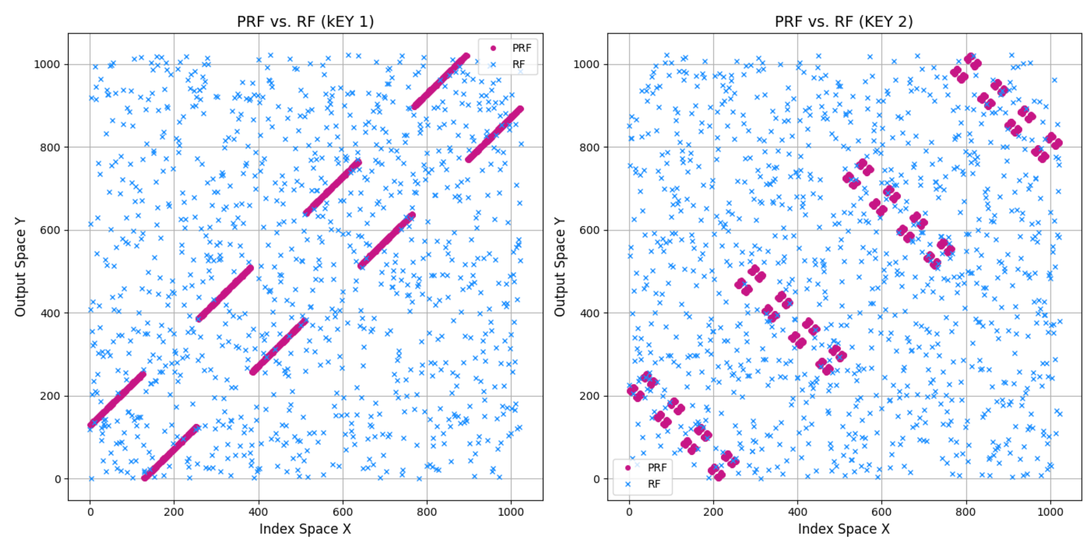
$T := \{\}$

Lookup $(x \in \{0,1\}^{\text{Idx}})$:
if $T[x]$ undefined:
$T[x] \leftarrow \{0,1\}^{\text{Out}}$
return $T[x]$

III.2 How NOT to Build a PRF

Suppose we have a length-doubling PRG $G : \{0,1\}^{\lambda} \to \{0,1\}^{2\lambda}$ and try to use it to construct a PRF F as follows:

$F(k,x)$:
return $G(k) \oplus x$



PRF vs RF

References

[1] M. Rosulek, *The Joy of Cryptography*, [Online]. Available: https://joyofcryptography.com
[2] N. P. Smart, *Cryptography Made Simple*. 1st ed. Springer International Publishing, 2016.
[3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. 2nd ed. Chapman and Hall/CRC, 2014.