난수생성이론

(Theory of Random Number Generation)

– 2020학년도 2학기 –

담당교수 : 강 주 성

정보보안암호수학과

과학기술대학

KMU 국민대학교 KOOKMIN UNIVERSITY

강의 계획 (2020학년도 2학기)

◈ 교과목명 : 난수생성이론
- ❍ 학수번호 139590-01

◈ 수강 대상
- ❍ 정보보안암호수학과 **3, 4 학년**

◈ 교재
- ❍ 강의노트 (가상대학에 1주일 전 배포)

◈ 평가 방법
- ❍ 중간고사 30%, 기말고사 30%
- ❍ 퀴즈 20%, 과제 10%, 출석 10%

◈ 온라인 수업 진행을 위한 주의사항
- ❍ 지정된 동영상 시청 기간을 지켜야만 출석이 인정됨.
- ❍ 과제, 퀴즈, 시험도 온라인으로 진행
  - ➢ 제출 요령을 정확히 준수해야 함.
  - ➢ 제출 마감 시간을 넘기지 말아야 함.

강의 내용 (2020년 2학기)

◈ 암호학적 난수발생기 개요 (Introduction)

◈ 난수성(randomness) 이해에 필요한 이론 (강의)

❍ **확률론(Probability)**

➢ Events and probability, Random variables, Limiting theorems…

❍ **확률과정론(Stochastic processes)**

➢ Random walks, Markov chain, Poisson process …

❍ **통계학(Statistics)**

➢ 추정(estimation), 가설검정(hypothetical tests) …

◈ 난수발생기 구현 및 안전성 평가

❍ 통계적 난수성 평가 방법 : NIST SP 800-22 문서

❍ 엔트로피 추정 방법 : NIST SP 800-90b 문서

❍ PRNG 설계 및 구현 : NIST SP 800-90a, NIST SP 800-90c 문서

❍ Linux RNG 안전성 분석

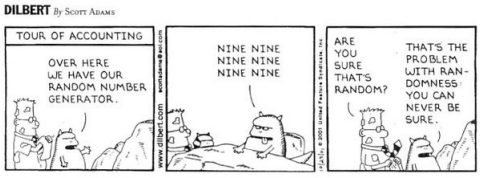
Chapter 1. Introduction

난수발생기란?

◈ 난수발생기(RBG: Random Bit Generator)의 기능
- ❍ 암호시스템에 필요한 **난수**(random number) 제공
- ❍ 암호시스템과 암호모듈의 운용에 필수적인 요소(알고리즘)

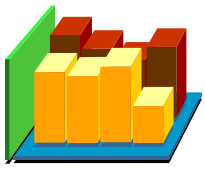
◈ 요구되는 성질: 예측불가능성, 비편향성, 비트간 독립성
- ❍ [ ]
  - ➢ 이상적으로는 "coin tossing (동전던지기)"의 결과를 기대

◈ 난수발생기의 용도
- ❍ 대칭키 암호(블록/스트림 암호)에 사용되는 **키**, ***IV*** 생성
- ❍ 공개키 암호의 각종 **파라미터** 생성 : 소수 생성, 확률적 공개키 암호 …
- ❍ 암호 프로토콜에 사용되는 각종 **파라미터** : **nonce**, **salt** …



Linear congruential generators

◈ Linear congruential generator
- ❍ [ ]
- ❍ Toy example : n=10, a=3, b=5, x_0=학번 끝자리



◈ Commonly used for simulation purposes

◈ Pass some statistical tests (Knuth, 1981)
- ❍ frequency, serial, poker, runs, autocorrelation tests, etc.

◈ Next number can be easily computed from the preceding ones
- ❍ even when x_0 , a , b , and n are not given (Plumstead, 1982)

◈ ***Predictable*** ⇒ entirely ***insecure*** for cryptographic purpose

Theoretical / Practical PRNGs

◈ PRNG vs. PRBG(Pseudorandom *Bit* Generator)

- ❍ A random bit generator can be used to generate random numbers.
- ❍ PRBG : *Theoretically-secure* under number-theoretic assumptions.
- ❍ PRNG : Practical mechanism which use block ciphers or hash functions as the underlying primitive.

◈ Theoretically-secure PRBGs

- ❍ Blum-Micali (1984), Blum-Blum-Shub (1986), RSA PRBG (1988), etc.
- ❍ Not most popular ones :

◈ Practical PRNGs

- ❍ Standardized PRNGs.
- ❍ The ANSI X9.17 PRNG, The FIPS 186 PRNG, IETF TLS-PRF…

Blum-Blum-Shub PRBG

Blum-Blum-Shub PRBG

- **Summary:** a pseudorandom bit sequence $y_1, y_2, \ldots, y_l$ of length l is generated.

1. Generate two large secret random and distinct primes p and q, each congruent to 3 modulo 4, and compute $n = pq$.
2. Select a random and secret seed $s \in [1, n-1]$ such that $\gcd(s, n) = 1$, and compute
3. For $1 \le i \le l$ do the following:
   (a) $x_i \leftarrow x_{i-1}^2 \pmod{n}$.
   (b)
4. The output sequence is $y_1, y_2, \ldots, y_l$.

- ❍ Blum-Blum-Shub (1984)
  - ➢ Intractability of quadratic residuosity problem ⇒ cryptographically strong PRBG
- ❍ Vazirani-Vazirani (1985) : proved under weaker assumption
  - ➢ Intractability of integer factorization ⇒ cryptographically strong PRBG

난수발생기 관련 용어

◈ 의사난수발생기(PRNG)

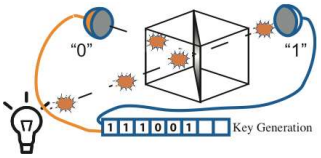
- ❍ **PRNG = Pseudo Random Number Generator**
- ❍ 일정한 알고리즘에 따라 [ ]으로부터 의사난수를 생성
- ❍ 초기값을 확장하는 방식 ➔ 알고리즘과 초기값이 모든 출력을 결정
  - ➢ Deterministic algorithm

◈ 진난수생성기(TRNG)

- ❍ **TRNG = True Random Number Generator**
- ❍ 물리적 잡음을 기반으로 진난수를 생성하는 장치

◈ 기타 용어

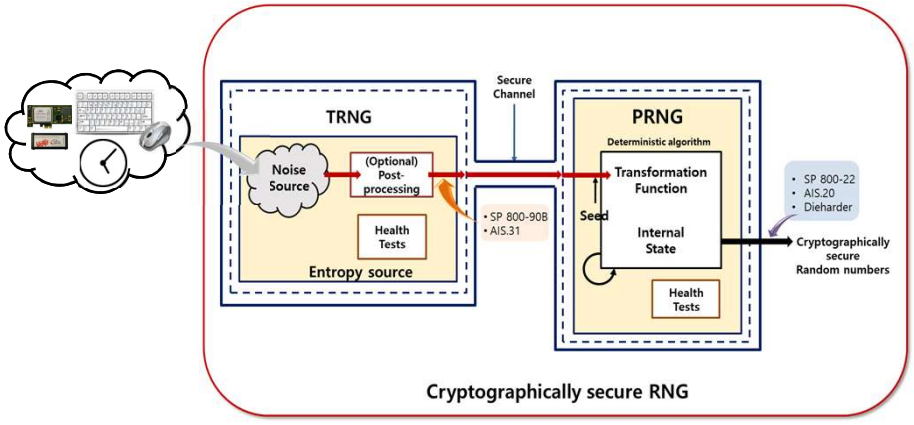
- ❍ DRNG : Deterministic RNG
- ❍ DRBG : Deterministic Random Bit Generator
- ❍ QRNG : Quantum RNG (양자난수생성기)



암호학적으로 안전한 난수발생기 구조

◈ 암호학적 난수발생기

- ❍ 암호학적 난수발생기 = [ ]
- ❍ TRNG의 출력을 PRNG의 초기값(Seed)으로 사용하여 난수를 생성



난수성 평가 – 엔트로피 소스 (TRNG)

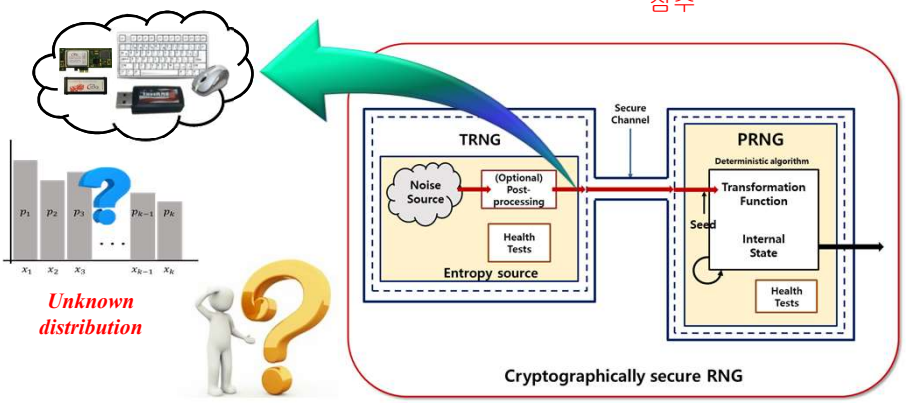
◈ NIST SP 800-90B

❍ Recommendation for the Entropy Sources Used for Random Bit Generation

➢ 2018년 1월, 최종 버전 발표

❍ 내용 : TRNG(엔트로피 소스)의 안전성 평가 [ ]

점수

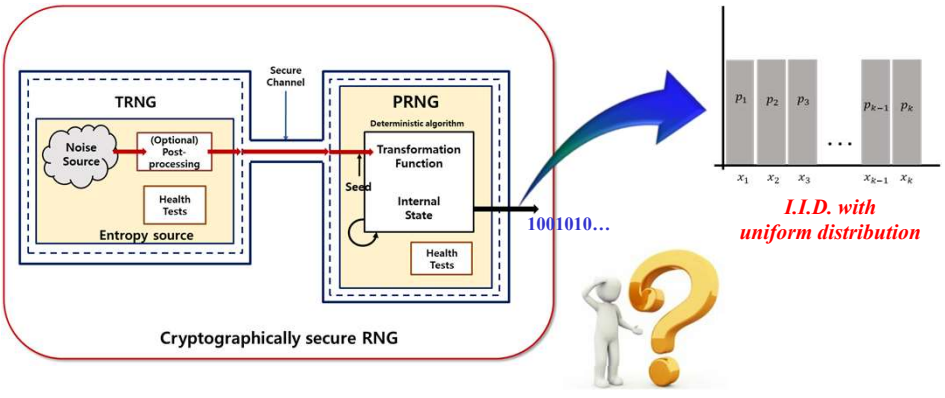


통계적 난수성 검정

◈ NIST SP 800-22

❍ A Statistical Test Suite for *Random* and *Pseudorandom* Number Generators for Cryptographic Applications

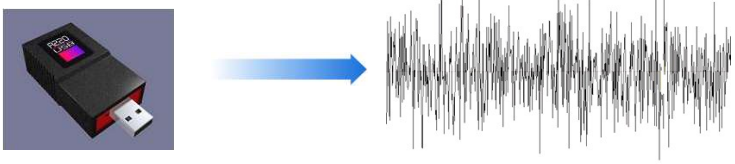
❍ 내용 : 진난수 및 의사난수의 [ ] (Pass/Fail)



난수발생기의 종류

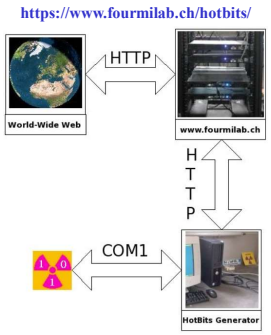
◈ 하드웨어 난수발생기
- ❍ 하드웨어 장치에서 발생되는 잡음원을 이용한 난수 생성
- ❍ 잡음원의 편향(bias)된 성질을 보정하는 과정이 필요
- ❍ 잡음원(엔트로피 소스) : 열 잡음원, 링 오실레이터, 양자 현상 등

◈ 소프트웨어 난수발생기
- ❍ 외부의 잡음원 공급을 전제로 결정론적 알고리즘을 사용
- ❍ 잡음원 : OS잡음, 사용자 입력 등



잡음원의 종류

◈ 하드웨어 잡음원
- ❍ 물리적 특성에 의존하는 잡음원
- ❍ 종류 : 열 잡음원, 링 오실레이터, 양자물리 현상, 방사성 붕괴 등

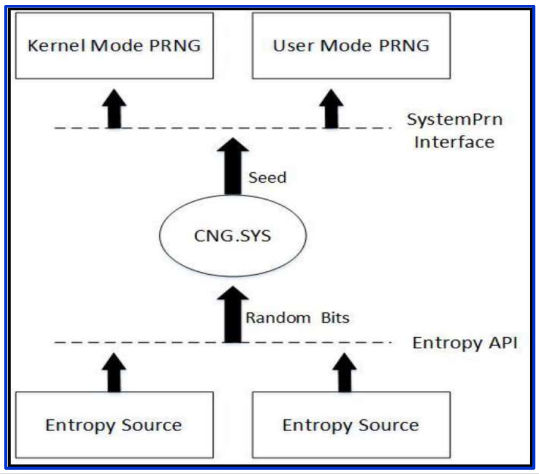


◈ 소프트웨어 잡음원
- ❍ 운영체제 또는 운영환경에 의존하는 잡음원
- ❍ 종류: Crypto API, Processor Timer 등
  - ➢ Windows OS 잡음원 : GetTickCount, GetCurrentId 등
  - ➢ Linux 잡음원 : perfstat_disk_total, perfstat_cpu_total 등
  - ➢ JRE 잡음원 : nanoTime, getProperty 등

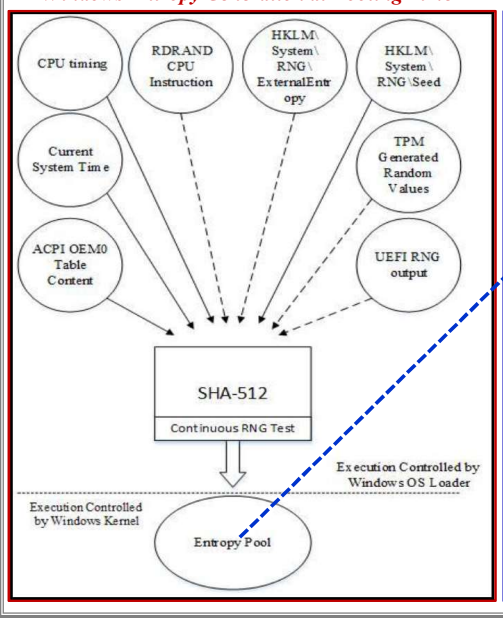
Windows RNG

◈ **CNG Cryptographic Primitive**

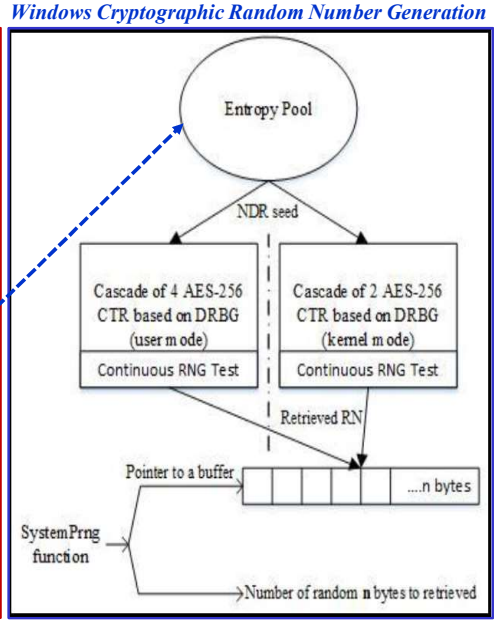
❍ *Serious vulnerabilities* found in **Windows XP** and **Windows 2000 random number generator** motivated Microsoft Windows to introduced Cryptography New Generation **(CNG)** in **Windows vista**.



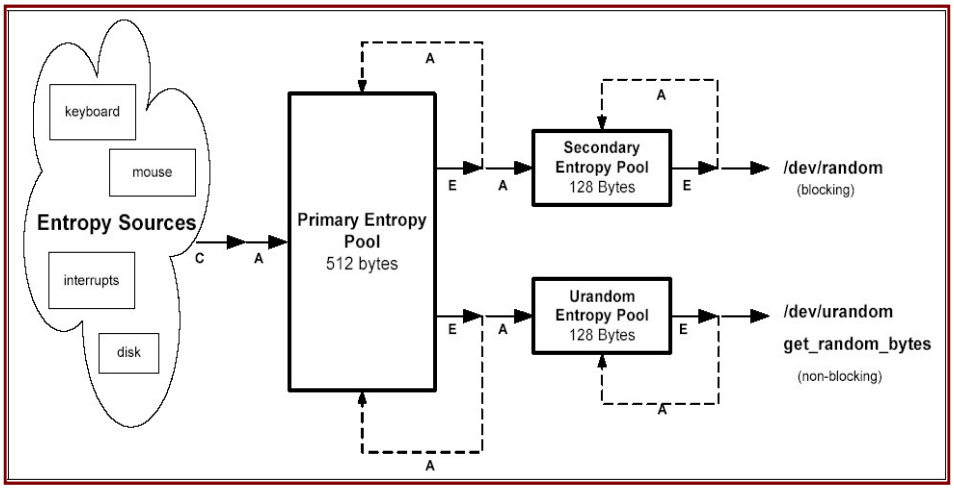
Windows Entropy Generation at Booting Time



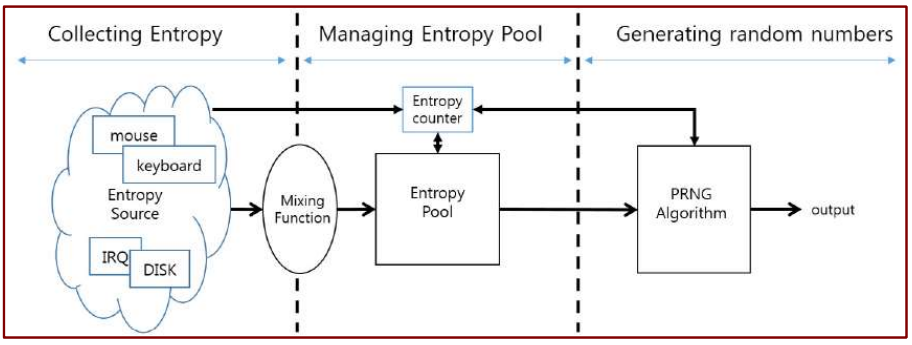
Windows Cryptographic Random Number Generation



Linux PRNG (LRNG) (1)



< General structure of LRNG >



◈ Collecting entropy

- In the entropy collecting part, LRNG collects data from various entropy sources including *interrupt information*, *disk timing* and *input devices*.
- Entropy inputs are plunged into the **entropy pool** through the mixing function.

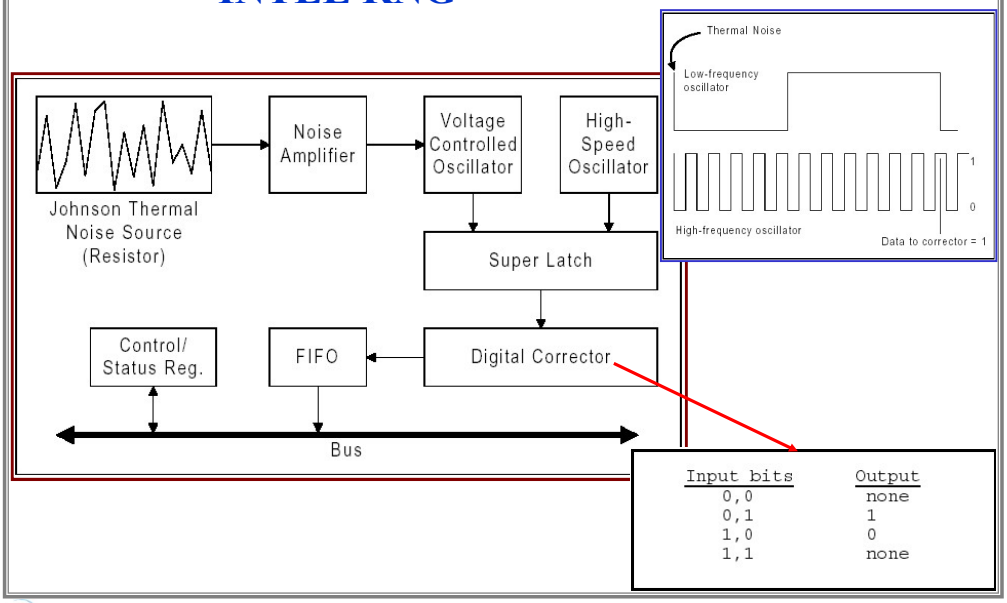
◈ Managing entropy pools

- ❍ The entropy estimator ***evaluates*** input data and determines *the amount of entropy*.
- ❍ For each input, the ***entropy counter*** is adjusted to indicate how much entropy the pool holds.

◈ Generating random numbers

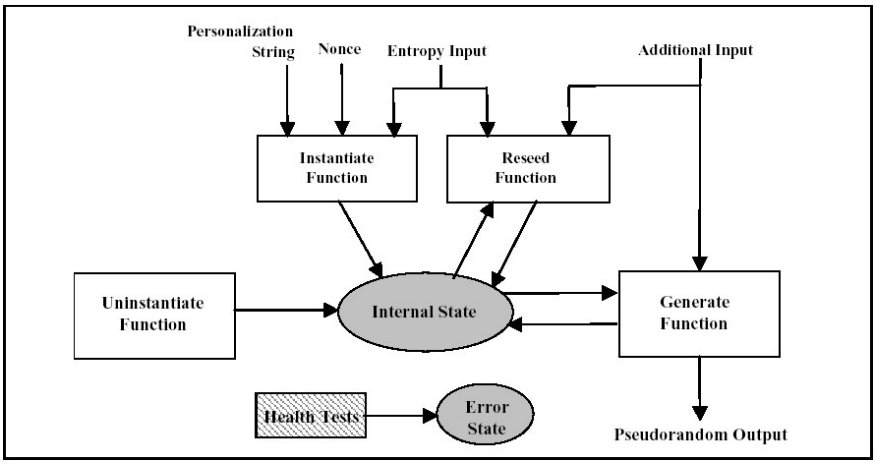
- ❍ When a user extracts data from the device **/dev/random** using the output function, the corresponding entropy counters are adjusted.
  - ➢ The output function is designed to **generate output** by *hashing* data in the output pool and simultaneously *updates* the pool by the **feedback function**.
  - ➢ If the counter needs to decrease to zero, the output request is **blocked**.
  - ➢ To produce **high quality random bits**, the output is not allowed unless the pool holds sufficient entropy.
- ❍ By contrast, **/dev/urandom** returns as many bytes as required **without blocking** regardless of the status of its entropy counter.

INTEL RNG



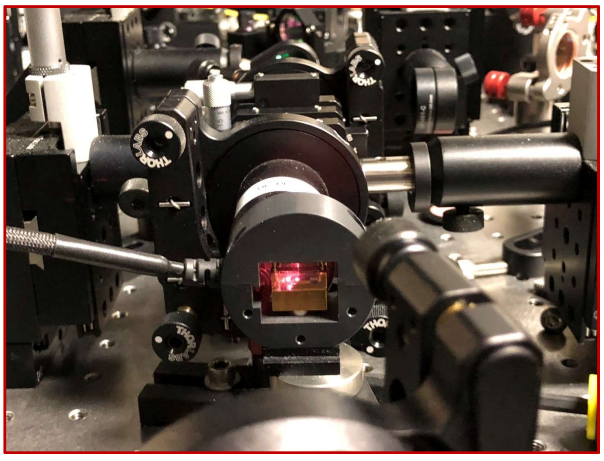
DRBG Functional Model (NIST)

◈ Deterministic RNG를 사용한 난수 발생 기법



NIST's New Quantum Method Generates *Really* Random Numbers

***Nature*. April 11, 2018**



NIST has developed a method for generating numbers guaranteed to be random by quantum mechanics. The method generates digital bits (1s and 0s) with photons, or particles of light. An intense laser hits a special crystal that converts laser light into pairs of photons that are entangled, a quantum phenomenon that links their properties. These photons are then measured to produce a string of truly random numbers.

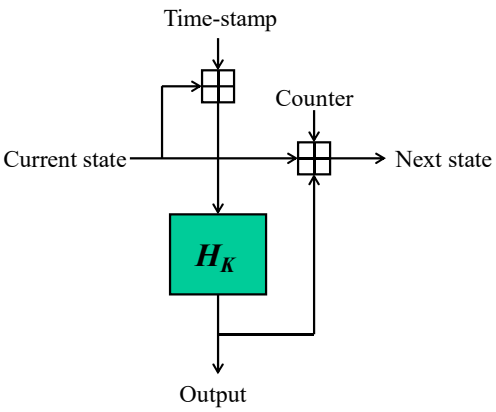
Entropy input (seed)

System Unique	Variable and Unguessable	External Random
Configuration files	Contents of screen	Cursor position with time
Drive configuration	Date and time	Keystroke timing
Environment strings	High resolution clock samples	Microphone input (with microphone connected)
	Last key pressed	Mouse click timing
	Log file blocks	Mouse movement
	Memory statistics	Video input
	Network statistics	
	Process statistics	
	Program counter for other processes or threads	

Less Entropy ⟷ More Entropy

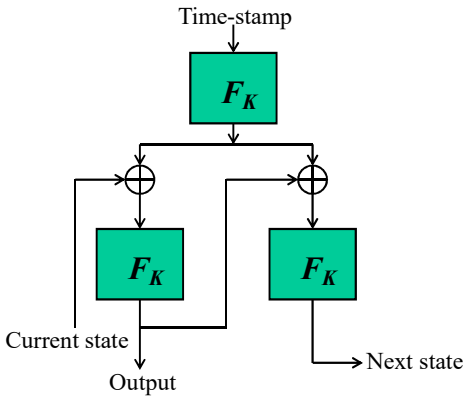
FIPS 186 PRNG

- FIPS 186 PRNG (1994)
  - Generating randomness in DSA
    - DSA private keys, DSA per-message secrets
  - H : one-way function using SHA-1
    - Also the one-way function using DES can be used
- FIPS 186-2 with Change Notice 1 (2001)



The ANSI X9.17 PRNG

- ANSI X9.17 PRNG (1986)
  - A part of a popular banking standard
  - Generating keys and IV for the use of DES
  - F_k denotes DES E-D-E two-key triple encryption under a key k



RNGVS(Validation System)

Algorithm Tested:	FIPS 186-2, FIPS 186-2 General Purpose Algorithm, ANSI X9.62, ANSI X9.31
RNG Generators Tested (applies to FIPS 186-2 and FIPS 186-2 General Purpose Algorithms)	For FIPS 186-2: x-Original, k-Original, x-Change Notice, k-Change Notice For FIPS 186-2 General Purpose Algorithm: x-Original, x-Change Notice
Curves Tested (applies to ANSI X9.62)	P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409, B-571
Core Algorithm (applies to ANSI X9.31 implementations processed after January 2005)	TDES-3Key, TDES-2Key, AES-128Key, AES-192Key, AES-256Key
G Function(s) Tested (applies to FIPS 186-2 and ANSI X9.62)	SHA-1, DES

RNG Validated Implementations

Validation No.	Vendor	Implementation	Operational Environment	Val. Date	Description/Notes
1413	RSA, The Security Division of EMC 174 Middlesex Turnpike Bedford, MA 01730 USA -Rohit Mathur TEL: +61730325220	**RSA BSAFE Crypto-C Micro Edition** Version 4.1.0.1	ARMv7 (32-bit) w/ Linaro Linux 3.10.68	1/15/2016	**FIPS 186-2 General Purpose** **[(x-Change Notice); (SHA-1)]** **"RSA BSAFE Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements."**
1412	Hewlett Packard Enterprise 153 Taylor Street Littleton, MA 01460 USA -Bob Pittman TEL: 1-978-264-5211 FAX: 1-978-264-5522	**HPE Comware** Version ComwareV7.1-R7103 (Firmware)	Freescale P2020, 1.0GHz, PowerPC; Freescale P4080, 1.5GHz, PowerPC	12/31/2015	**ANSI X9.31** **[AES-128Key]** "Comware cryptographic library is a software library that provides cryptographic functions within HP devices."
1411	OpenSSL Software Foundation, Inc. 1829 Mount Ephraim Road Adamstown, MD 27101 USA -Steve Marquess TEL: 301-874-2571	**OpenSSL FIPS Object Module** Version 2.0.12	Intel Atom E3845 (x86) without AES-NI optimizations w/ Linux 3.10 32-bit; Intel Atom E3845 (x86) with AES-NI optimizations w/ Linux 3.10 32-bit	1/22/2016	**ANSI X9.31** **[AES-128Key AES-192Key AES-256Key]** "The OpenSSL FIPS Object Module is a full featured general purpose cryptographic library that is distributed in source code form under an open source license. It can be downloaded from www.openssl.org/source/." *08/04/15: Added new tested information;* *09/04/15: Added new tested information;* *10/22/15: Added new tested information;* *10/30/15: Updated implementation information information;*

Summary

◈ 난수발생기에 요구되는 성질

- ❍ Unpredictability, Unbiasedness, Independence

◈ 암호학적으로 안전한 난수발생기의 구성 요소

- ❍ TRNG(entropy source) + PRNG

◈ 난수발생기의 안전성 평가 방법

- ❍ TRNG 출력 수열에 대한 엔트로피 추정 방법
- ❍ RNG 출력 수열에 대한 통계적 난수성 검정 방법

◈ 난수발생기의 종류

- ❍ 하드웨어/소프트웨어 난수발생기
- ❍ OS 기반 난수발생기
- ❍ 각종 표준 난수발생기