FRO기반 난수 발생기 설계

Feedforward Ring Oscillator – based True Random Number Generator

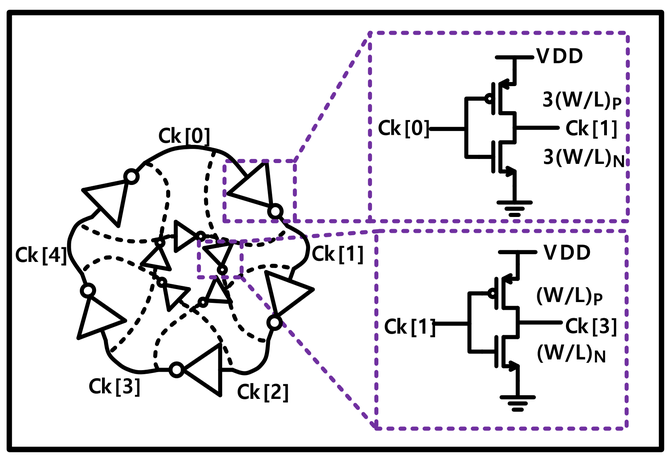
2025 전자공학과 산학박람회

Researcher 박승화 Professor 이 종 민 교수님

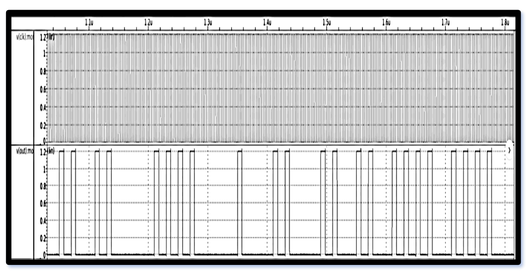
ABSTRACT

TRNG는 True Random Number Generator로써 자연계의 무작위성을 활용하여 Random number를 생성하는 모듈이다. 이러한 TRNG는 높은 보안을 필요로 하는 곳에서 핵심적인 역할을 한다.

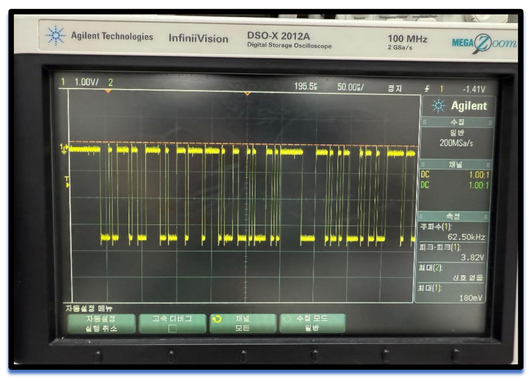
1. 암호화 모듈의 KEY 생성
2. 양자 내성 암호 알고리즘의 구동



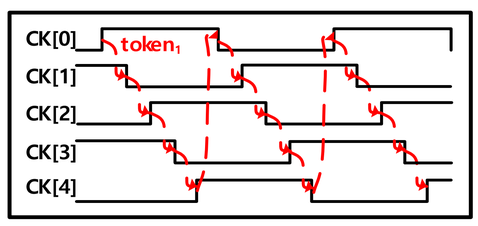
Feedforward Ring Oscillator
→ RO + Feedforward path
→ Jitter Integration Speed 증가
→ Random number Generation 주기 감소
→ Throughput 증가



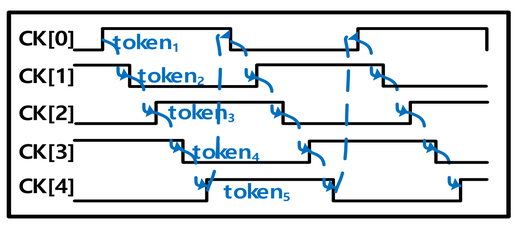
[Simulation 결과]



[측정 결과]



[5 Stage RO]



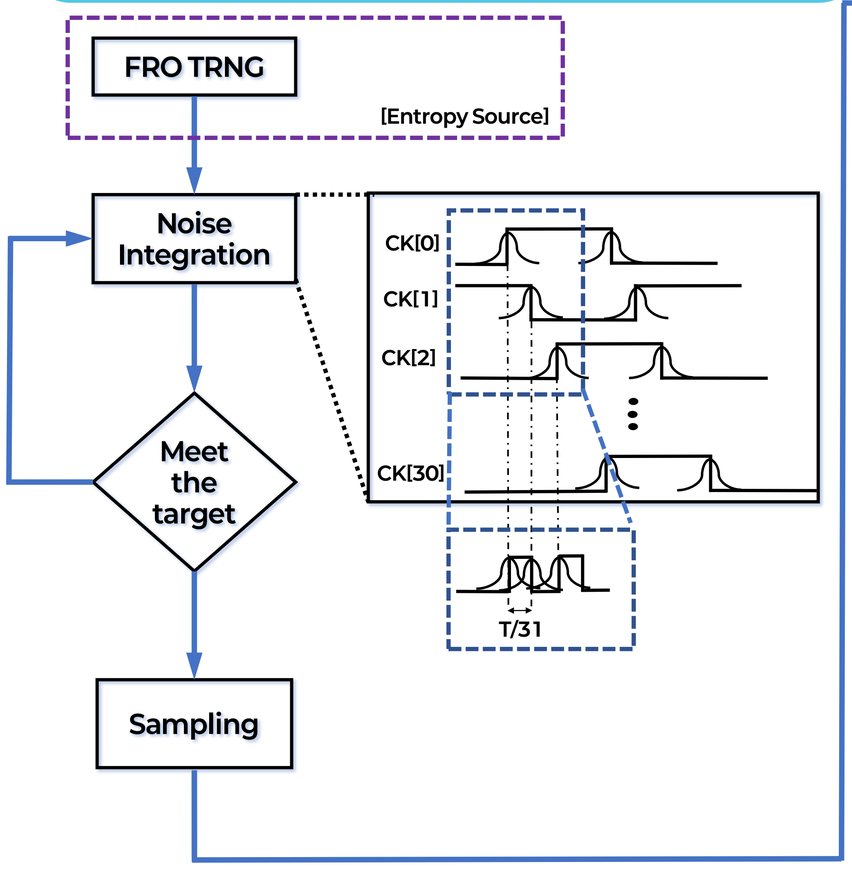
[5 Stage FRO]

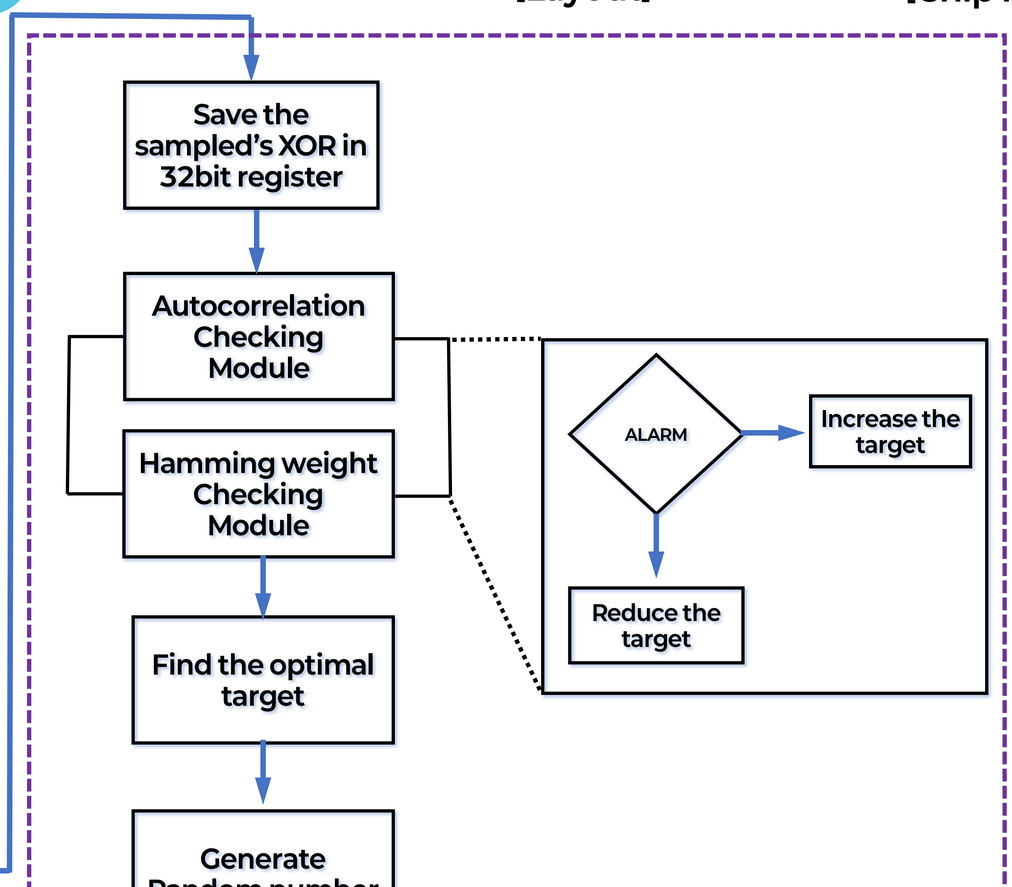
OBJECTIVES

TRNG의 성능의 2가지 관점

- Throughput
  → 일정 시간 안에 몇 개의 Random number를 생성하는가
- Random
  → P(1)의 값이 0.5에 얼마나 유사한 값을 가지는가

METHODOLOGY

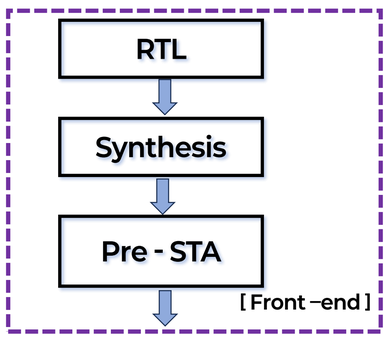


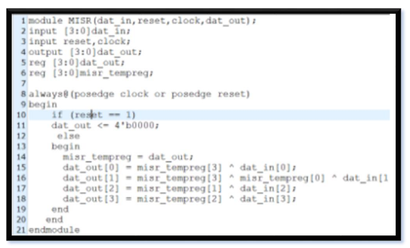


<Random number 생성>

1. Entropy Source
   - Jitter in FRO 활용
2. Post – Processing
   - ACF check Module
   - HW check Module
   → ALARM 설정
   : Jitter Integration에 필요한 시간 결정

RESULT

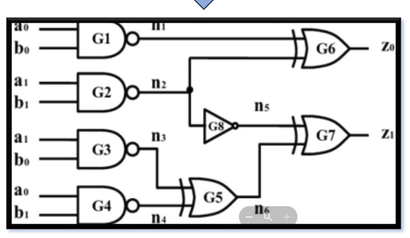




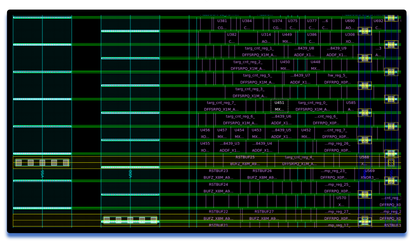
```
module MISR(dat_in,reset,clock,dat_out);
input [3:0]dat_in;
input reset,clock;
output [3:0]dat_out;
reg [3:0]dat_out;
reg [3:0]misr_tempreg;

always@(posedge clock or posedge reset)
begin
  if (reset == 1)
  dat_out <= 4'b0000;
  else
  begin
    misr_tempreg = dat_out;
    dat_out[0] = misr_tempreg[3] ^ dat_in[0];
    dat_out[1] = misr_tempreg[3] ^ misr_tempreg[0] ^ dat_in[1
    dat_out[2] = misr_tempreg[1] ^ dat_in[2];
    dat_out[3] = misr_tempreg[2] ^ dat_in[3];
  end
end
endmodule
```

[System Level Design : RTL code]

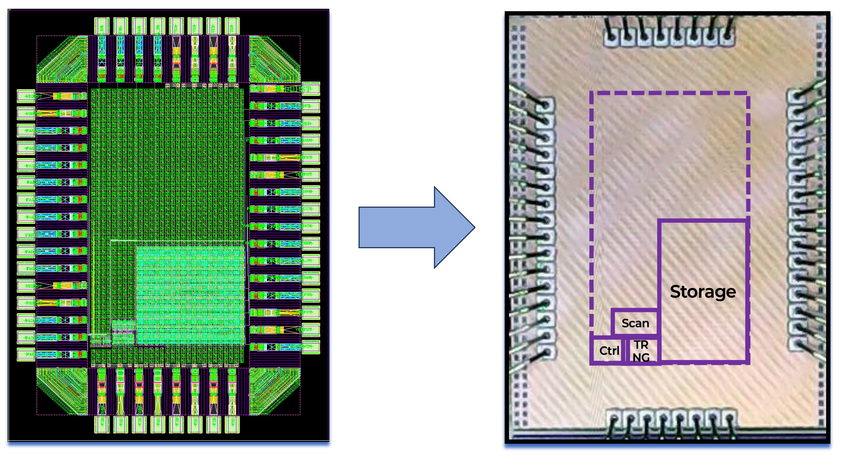


[Logic Design : gate –level netlist]

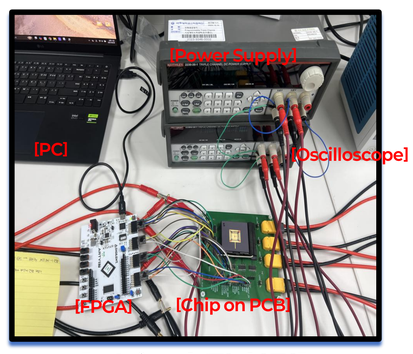


[Physical Design : GDS]

CONCLUSIONS



[Layout] [Chip in TSMC 65nm]



[Chip 측정 환경]

아주대학교 | 전자공학과 KIAT 반도체특성화대학사업단 GUIP 경기도 대학혁신플랫폼