

진성난수 생성기를 위한 베타선 센서 설계에 관한 연구

김영희*, 김홍주*, 박경환**, 김종범***, 하판봉*

A Study on the Design of a Beta Ray Sensor for True Random Number Generators

Young-Hee Kim*, HongZhou Jin*, Kyunghwan Park**, Jongbum Kim***, Pan-Bong Ha*

요약 본 논문에서는 진성난수 생성기를 위한 베타선 센서를 설계하였다. PMOS 피드백 트랜지스터의 게이트를 DC 전압으로 바이어스하는 대신 PMOS 피드백 트랜지스터에 흐르는 전류가 PVT 변동에 둔감하도록 설계된 전류 바이어스 회로를 mirroring하게 흐르도록 하므로 CSA의 signal voltage의 변동을 최소화하였다. 그리고 BGR (Bandgap Reference) 회로를 이용하여 공급된 정전류를 이용하여 신호 전압을 VCOM 전압 레벨까지 충전하므로 충전 시간의 변동을 줄여 고속 감지가 가능하도록 하였다. 0.18 μ m CMOS 공정으로 설계된 베타선 센서는 corner별 모의실험 결과 CSA 회로의 최소 신호전압과 최대 신호전압은 각각 205mV와 303mV이고, pulse shaper를 거친 출력 신호를 비교기의 VTHR (Threshold Voltage) 전압과 비교해서 발생된 펄스의 최소와 최대 폭은 각각 0.592 μ s와 1.247 μ s로 100kHz의 고속 감지가 가능한 결과가 나왔으며, 최대 100Kpulse/sec로 계수할 수 있도록 설계하였다.

Abstract In this paper, we designed a beta ray sensor for a true random number generator. Instead of biasing the gate of the PMOS feedback transistor to a DC voltage, the current flowing through the PMOS feedback transistor is mirrored through a current bias circuit designed to be insensitive to PVT fluctuations, thereby minimizing fluctuations in the signal voltage of the CSA. In addition, by using the constant current supplied by the BGR (Bandgap Reference) circuit, the signal voltage is charged to the VCOM voltage level, thereby reducing the change in charge time to enable high-speed sensing. The beta ray sensor designed with 0.18 μ m CMOS process shows that the minimum signal voltage and maximum signal voltage of the CSA circuit which are resulted from corner simulation are 205mV and 303mV, respectively. and the minimum and maximum widths of the pulses generated by comparing the output signal through the pulse shaper with the threshold voltage (VTHR) voltage of the comparator, were 0.592 μ s and 1.247 μ s, respectively. resulting in high-speed detection of 100kHz. Thus, it is designed to count up to 100 kilo pulses per second.

Key Words : beta ray sensor, BGR, Charge Sensitive Amplifier, PVT insensitive, true random number generator

This research was supported by Nuclear Technology Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (No. 2018M2A8A1083094). The EDA tool was also supported by the IC Design Education Center(IDEA), Korea.

*Department of Electronic Engineering, Changwon National University

**Electronics and Telecommunications Research Institute

***Korea Atomic Energy Research Institute

*Corresponding Author : Department of Electronic Engineering, Changwon National University (youngkim@changwon.ac.kr)

Received November 25, 2019

Revised December 09, 2019

Accepted December 10, 2019

1. 서론

난수 (random number)는 암호화와 모의실험 등의 다양한 과학, 기술 분야에서 활용되고 있다 [1]. 대부분은 유사난수 (pseudo random number)를 사용하고 있으나 높은 보안등급, 고신뢰성을 요구하는 IoT 보안 분야에서는 날로 고도화되고 있는 해킹 (hacking)을 방지하는데 가장 효과적인 진성난수 (true random number)를 사용하고 있다[2].

한편 양자역학적 물리현상을 이용한 난수생성기는 하드웨어 기반의 난수생성기중 가장 이상적인 난수를 생성할 수 있다[3][4]. 방사성 동위원소 (베타선 or 감마선 or X선)의 자연붕괴 현상은 붕괴 이벤트의 랜덤성, 이전 이벤트와의 무상관성, 물리적 환경 조건에 무관성 등 진성 난수용 엔트로피로 사용될 수 있는 특징을 모두 가지고 있으므로 이상적인 난수를 발생할 수 있으며 [2], 동위원소 기반의 난수생성기에 대한 연구결과는 발표되었다 [5-7]. 방사선 중 베타선의 베타 붕괴를 이용하는 경우가 차폐가 용이하고, 크기가 작고, 휴대성이 높고, 발생속도가 높고 반도체 손상이 낮은 장점이 있다. Ni-63 베타선원은 PIN 다이오드에서 생성된 전하를 CSA (Charge Sensitive Amplifier) 회로를 이용한 모듈회로에서 검출이 가능하다.

그리고 X선의 경우는 CSA 회로를 포함한 ASIC 칩에 대한 연구 결과가 있다[8][9]. CSA (Charge-Sensitive Amplifier)는 CMOS OPAMP의 negative 입력단과 출력 노드인 CSA_OUT 에 피드백 커패시터 C_f 와 게이트가 GND인 저항 R_f 가 병렬로 연결되어 있다. CSA는 PIN 다이오드에서 생성되는 입력 전하 펄스 (input charge pulse)를 적분하여 출력 전압 signal voltage인 ΔV_s 로 변환하여 VCOM 레벨에서 떨어진다[9][10]. 그리고 출력 전압 펄스는 저항에 의해 OPAMP의 positive 입력단에 연결된 VCOM (Common Voltage) 전압으로 $\tau = R_f \cdot C_f$ 의 시상수 (time constant)를 가지고 충

전한다. 피드백 저항을 사용할 경우 CMOS 공정상에 기생 커패시턴스가 존재하여 signal voltage가 작고 피드백 저항이 차지하는 레이아웃 면적이 큰 단점이 있으므로 PMOS 트랜지스터를 이용하여 피드백 저항을 구현된다[9].

PMOS 트랜지스터를 사용하는 CSA 회로에서 PMOS 트랜지스터의 게이트는 GND 또는 DC 전압을 인가할 수 있다. 이 경우 PMOS 피드백 트랜지스터의 구동 전류가 MOS 모델 파라미터, 온도와 공급전압 VDD에 따라 변하므로 피드백 저항이 PVT (Process - Voltage - Temperature) 변동에 따라 민감하게 변하게 된다.

본 논문에서는 진성난수 생성기를 위한 베타선 센서를 설계하였다. PMOS 피드백 트랜지스터의 게이트를 DC 전압으로 바이어스하는 대신 PMOS 피드백 트랜지스터에 흐르는 전류가 PVT 변동에 둔감하도록 설계된 전류 바이어스 회로를 mirroring하게 흐르도록 하므로 CSA의 signal voltage의 변동을 최소화하였다. 그리고 BGR (Bandgap Reference) 회로를 이용하여 공급된 정전류를 이용하여 신호 전압을 VCOM 전압레벨까지 충전하므로 충전 시간의 변동을 줄여 고속 감지가 가능하도록 하였다. 또한 노이즈를 줄이고 shaping time을 줄이기 위해 미분기와 적분기를 사용한 pulse shaper를 사용하였다. 0.18 μ m CMOS 공정으로 설계된 베타선 센서는 corner별 모의실험 결과 CSA 회로의 최소 신호 전압과 최대 신호전압은 각각 205mV와 303mV 이고, pulse shaper를 거친 출력 신호를 비교기의 VTHR (Threshold Voltage) 전압과 비교해서 발생된 펄스의 최소와 최대 폭은 각각 0.592 μ s와 1.247 μ s로 100KHz의 고속 감지가 가능한 결과가 나왔다.

2. 회로 설계

PIN 다이오드를 사용하여 Ni-63 베타 선원에 의해 발생된 EHP (Electron-Hole Pair) 전하를 검출하는 베타선 센서 회로는 그림 1에서 보는

바와 같다. 베타선 센서 회로는 CSA 회로, 전압 버퍼 (voltage buffer)로 사용되는 voltage follower, pulse shaper 역할을 하는 미분기 (differentiator)와 적분기 (integrator) 회로, pulse shaper의 출력 신호와 VTHR (Threshold Voltage) 전압과 비교하여 PIN 다이오드에 베타선이 들어왔는지 감지하기 위한 비교기 (comparator) 회로로 구성되어 있다.

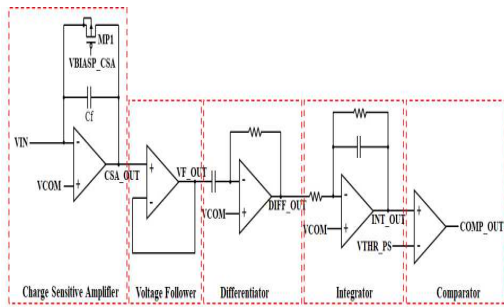


그림 1. 베타선 검출용 센서 회로의 블록도.
Fig. 1. Block diagram of beta ray sensor.

그림 2는 PIN 다이오드, 테스트 커패시터와 CSA 회로로 구성된 AFE (Analog Front end) 회로도 보여주고 있다. PIN 다이오드의 양극 (anode)은 CSA 회로에 사용되는 OPAMP의 negative 입력단에 연결되고, 음극 (cathode)는 VHH (=5V) 전압원에 연결된다. 높은 에너지를 갖는 Ni-63 베타선에 의해 발생된 EHP (Electron-Hole Pair) 전하 중 전자 (electron)는 VHH 전압으로 이동하고 정공 (hole)은 OPAMP의 negative 입력단으로 이동한다. 이때 CSA 회로에 의해 전하를 적분하여 CSA 출력인 CSA_OUT에 신호전압인 ΔV_s 를 출력한다. 만약 CSA 회로의 OPAMP에 있는 negative 입력단인 VIN과 출력인 CSA_OUT 사이에 연결된 피드백 저항 R_f 와 피드백 커패시터 C_f 의 시상수인 $\tau = R_f \cdot C_f$ 의가 PIN 다이오드에서 입사되는 전하의 펄스 폭보다 훨씬 큰 경우 ΔV_s 는 최대 전압인 $-Q_s/C_f$ 를 출력한다[9][10]. Q_s 는 베타선 입자에 의해 PIN 다이오드에 의해 EHP가 생성되어

OPAMP의 입력단을 통해 전류에 기여하는 신호 전하 (signal charge)이다. 만약 피드백 저항 R_f 가 없는 경우는 적분기처럼 동작하여 신호전압 ΔV_s 를 그대로 유지하겠지만 CSA 회로는 C_f 에 병렬로 피드백 저항 R_f 가 연결되어 있으므로 CSA의 출력 신호인 CSA_OUT은 τ 의 시상수를 가지고 OPAMP의 positive 입력단 전압인 VCOM 레벨로 충전하게 된다[9]. R_f 가 작을수록 방전시간이 빨라져 고속 감지가 가능한 반면, 신호 전하를 적분하면서 R_f 에 의해 방전을 빠르게 하므로 신호 전압 ΔV_s 가 낮아지는 단점이 있다. 한편 피드백 저항으로 선형 저항인 폴리실리콘을 사용할 경우 CMOS 공정상에 저항 layer인 폴리실리콘과 p-substrate 사이에 기생 커패시턴스 (parasitic capacitance)가 존재하여 signal voltage가 작아지고 피드백 저항이 차지하는 레이아웃 면적이 큰 단점이 있으므로 PMOS 트랜지스터를 이용하여 피드백 저항을 구현할 수 있다[9]. 그림 2의 회로에서 테스트 커패시터 C_{TEST} 는 VTEST에 신호 펄스를 인가하여 CSA 회로의 동작을 테스트 해보기 위한 회로소자이다.

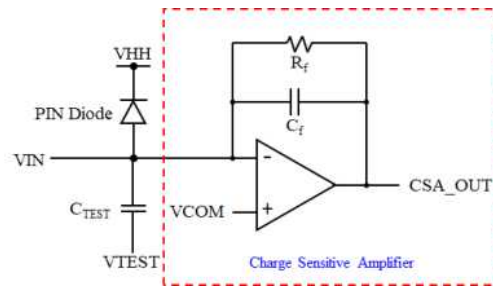


그림 2. PIN 다이오드, 테스트 커패시터와 CSA 회로로 구성된 AFE (Analog Front End) 회로도.
Fig. 2. Analog front end (AFE) schematic consisting of a PIN diode, test capacitor, and a CSA circuit.

그림 3은 PMOS 피드백 트랜지스터를 저항으로 사용하는 기존의 CSA 회로도이며, PMOS 트랜지스터의 게이트 노드는 VBIASP_CSA의 DC 전압을 인가하고 있다. 그림 3의 VBIASP_CSA 전압은 BGR (Bandgap Reference) 회로에서

만들어지는 2.5 μ A의 정전류인 IREF_2p5uA를 그림 4(a)에서 보는 바와 같이 전류-전압 변환기 (I-to-V converter)를 통해서 VREF_VBIASP (=1.522V)로 변환된다. 이때 VREF_VBIASP는 구동전류 능력이 떨어지므로 그림 4(b)에서 보는 바와 같이 OPAMP를 이용한 voltage follower로 VBIASP_CSA (=VREF_VBIASP)를 만들어준다. 그림 4(b)의 DC 전압인 VBIASP_CSA 전압을 그림 3의 PMOS 피드백 트랜지스터의 게이트 노드에 연결하는 경우 MOS 트랜지스터나 저항 값은 CMOS 공정 (process), 공급전압 VDD와 온도 (temperature)인 PVT (Process - Voltage - Temperature) 변동에 따라 베타선에 의해 signal charge가 CSA의 입력단으로 주입되었을 때 PMOS 피드백 트랜지스터의 소스-드레인 전류 변동이 크게 나타난다. 그래서 PVT 변동에 따라 CSA 회로의 신호 전압 ΔV_s 의 변동이 크고 charge integration 이후 VCOM 전압으로 방전하는데 시간이 많이 걸리면서 고속 감지가 불가능하다.

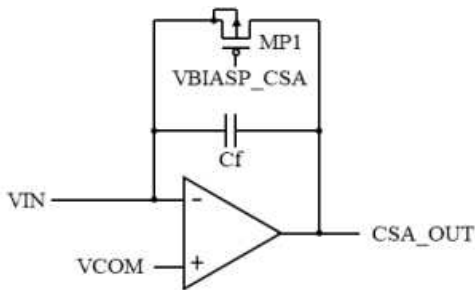
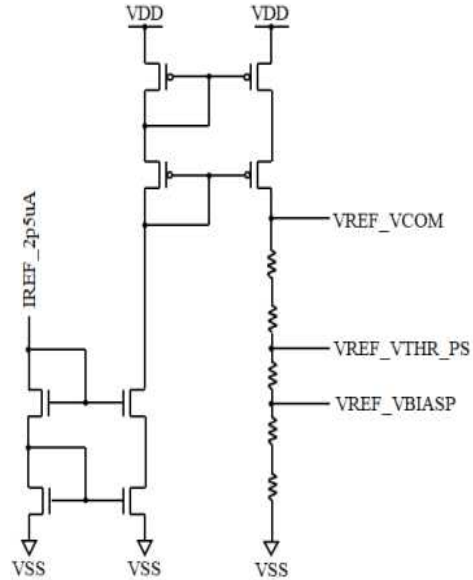
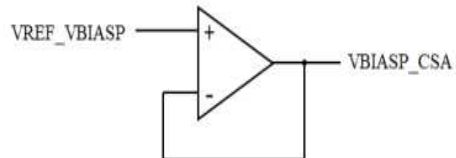


그림 3. PMOS 피드백 트랜지스터의 게이트에 DC 전압을 인가하는 기존의 CSA 회로.
Fig. 3. Conventional CSA circuit for applying DC voltage to the PMOS feedback transistor gate.



(a) I-to-V 변환기



(b) voltage follower

그림 4. 기존 CSA 회로의 PMOS 피드백 트랜지스터 게이트에 DC 전압을 인가해주는 회로도.

Fig. 4. Circuit diagram that applies DC voltage to the PMOS feedback transistor gate of a conventional CSA circuit: (a) I-to-V converter and (b) voltage follower.

표 1은 그림 3의 DC 전압 VBIASP_CSA를 인가하는 CSA 회로의 PVT 변동에 대한 신호전압 모의실험 결과를 보여주고 있다. MOS 트랜지스터의 모델 파라미터는 표 1에서 보는바와 같이 SS(Slow NMOS Slow PMOS), SF(Slow NMOS Fast PMOS), TT(Typical NMOS Typical PMOS), FS(Fast NMOS Slow PMOS), FF(Fast NMOS Fast PMOS)가 있다. 그리고 표 2는 그림 3의 DC 전압 VBIASP_CSA를 인가하는 CSA 회로를 사용한 베타선 센서의 PVT 변동에 대한 비교기 출력 펄스 폭 모의실험 결과를 보여주고

있다. 그림 3의 DC 전압 VBIASP_CSA를 인가하는 CSA 회로를 사용하여 0.18 μ m CMOS 공정으로 설계된 베타선 센서는 corner별 모의실험 결과 표 1과 표 2에서 보는 바와 같이 CSA_OUT 신호의 최소 신호전압과 최대 신호전압은 각각 66mV와 320mV이고, pulse shaper를 거친 출력 신호를 비교기의 VTHR (Threshold Voltage) 전압과 비교해서 발생된 펄스의 최소와 최대 폭은 각각 Fail과 2.29 μ s로 일부 모의실험 조건에서 센싱 불량이나 폭의 변동이 큰 것을 볼 수 있다. CSA_OUT의 신호전압 크기는 PIN 다이오드에서 생성되는 입력 전하 펄스를 CSA 회로에서 적분하여 VCOM 레벨에서 Δ Vs만큼 떨어지는 전압을 의미한다.

표 1. 그림 3의 DC 전압 VBIASP_CSA를 인가하는 CSA 회로의 PVT 변동에 대한 신호전압 모의실험 결과.
Table 1. Signal voltage simulation results for PVT fluctuations in the CSA circuit applying the DC voltage VBIASP_CSA in Figure 3.

VDD	TEMP	SS Model	SF Model	TT Model	FS Model	FF Model
4.5V	-40°C	278mV	224mV	249mV	320mV	199mV
	25°C	229mV	165mV	183mV	262mV	146mV
	85°C	169mV	134mV	142mV	188mV	119mV
5V	-40°C	280mV	219mV	243mV	320mV	192mV
	25°C	220mV	157mV	176mV	253mV	139mV
	85°C	125mV	113mV	117mV	150mV	106mV
5.5V	-40°C	237mV	166mV	189mV	276mV	157mV
	25°C	126mV	109mV	118mV	160mV	105mV
	85°C	66mV	70mV	73mV	82mV	74mV

표 2. 그림 3의 DC 전압 VBIASP_CSA를 인가하는 CSA 회로를 사용한 베타선 센서의 PVT 변동에 대한 비교기 출력 펄스 폭 모의실험 결과.

Table 2. Comparator output pulse width simulation results for PVT fluctuations of a beta ray sensor using a CSA circuit applying the DC voltage VBIASP_CSA in Figure 3.

VDD	TEMP	SS Model	SF Model	TT Model	FS Model	FF Model
4.5V	-40°C	2.29 μ s	0.610 μ s	0.733 μ s	1.553 μ s	0.345 μ s
	25°C	1.157 μ s	0.424 μ s	0.481 μ s	0.845 μ s	0.267 μ s
	85°C	0.676 μ s	0.350 μ s	0.362 μ s	0.503 μ s	0.219 μ s
5V	-40°C	2.153 μ s	0.547 μ s	0.655 μ s	1.417 μ s	0.317 μ s
	25°C	0.964 μ s	0.391 μ s	0.430 μ s	0.729 μ s	0.245 μ s
	85°C	0.361 μ s	0.228 μ s	0.248 μ s	0.338 μ s	0.169 μ s
5.5V	-40°C	1.028 μ s	0.365 μ s	0.417 μ s	0.816 μ s	0.255 μ s
	25°C	0.323 μ s	0.207 μ s	0.237 μ s	0.335 μ s	0.161 μ s
	85°C	Fail	Fail	Fail	Fail	Fail

그림 5는 PMOS 피드백 트랜지스터의 게이트에 DC 전류 바이어스를 인가하는 제안된 CSA 회로도이다. 그림 5의 IBIASP_CSA 전류 바이어스는 125nA의 정전류인 IADAPTIVE_CSA를 MN1과 MN2의 current mirror 비를 25:1로 하므로 MP3를 통해서 흐르는 전류를 5nA로 줄였다. 이 전류를 그림 6의 게이트와 드레인을 연결한 노드인 IBIASP_CSA와 소스인 VCOM 사이에 PMOS 다이오드 형태의 트랜지스터인 MP3를 연결하여 MN2의 5nA의 전류를 흘려줄 수 있는 전압 IBIASP_CSA가 걸리게 한다. 한편 그림 5의 MP2는 신호전하가 인가가 되지 않는 구간동안 VIN 전압은 OPAMP의 negative 피드백 동작에 의해 OPAMP의 positive 입력전압인 VCOM 전압을 따라간다. 한편 그림 6의 MP3와 그림 5의 MP2는 current mirror 구조는 아니지만 VIN 노드로 입력신호 전하가 인가되었을 때 current mirror 처럼 동작하게 된다. 그래서 VIN 노드로 입력신호 전하가 인가되면 CSA 회로의 출력인 CSA_OUT 신호에 신호전압 Δ Vs가 develop되었다가 그림 5

의 MP2와 그림 6의 MP3에 의해 current mirror 형태로 동작하면서 CSA_OUT 전압은 VCOM 레벨로 충전하는데, 충전되는 전류는 BGR에 의해 PVT 변동에 둔감한 전류가 흐른다. 이때 흐르는 전류는 MP3와 MP2의 폭 W는 동일하지만 길이 L이 MP2가 MP3의 5배로 설계되었으므로 충전전류는 1nA 정도로 흐르게 된다. 이와같이 PMOS 피드백 트랜지스터의 게이트에 DC 전류 바이어스를 인가하는 제안된 CSA 회로는 베타선에 의해 signal charge가 CSA의 입력단으로 주입되었을 때 PVT 변동에 따라 PMOS 피드백 트랜지스터의 소스-드레인 전류 변동이 작게 나타난다. 그래서 PVT 변동에 따라 CSA 회로의 신호전압 ΔV_s 의 변동이 작고 charge integration 이후 VCOM 전압으로 충전하는데 걸리는 시간도 짧아서 고속 감지가 가능하다.

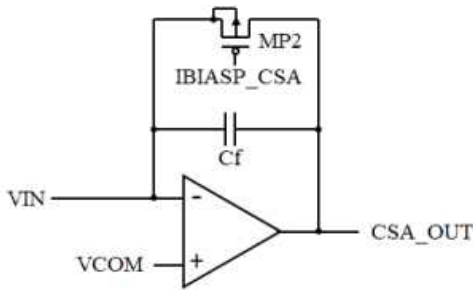


그림 5. PMOS 피드백 트랜지스터의 게이트에 DC 전류 바이어스를 인가하는 제안된 CSA 회로.

Fig. 5. A proposed CSA circuit applying a DC current bias to the PMOS feedback transistor gate.

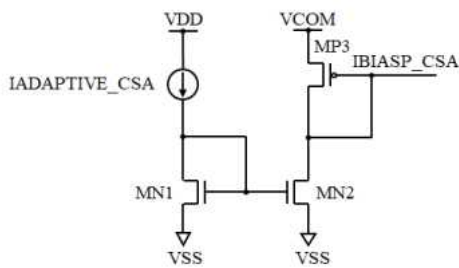


그림 6. 제안된 CSA 회로의 PMOS 피드백 트랜지스터 게이트에 DC 전류 바이어스를 공급하는 전류 바이어스 회로.

Fig. 6. A current bias circuit that supplies a DC current bias to the PMOS feedback transistor gate of the proposed CSA circuit.

3. 모의실험 결과

신호 전하가 VIN으로 입력되었을 때 CSA 회로의 출력인 CSA_OUT 신호에 신호전압 ΔV_s 가 develop되었다가 그림 5의 MP2와 그림 6의 MP3에 의해 current mirror 형태로 동작하면서 CSA_OUT 전압은 VCOM 레벨로 PVT 변동에 둔감한 정전류로 충전하도록 DC 전류 바이어스 IBIASP_CSA를 인가하는 CSA 회로의 PVT 변동에 대한 신호전압 모의실험 결과를 표 3에서 보여주고 있다. 그리고 표 4는 그림 5의 DC 전류 바이어스 IBIASP_CSA를 인가하는 CSA 회로를 사용한 베타선 센서의 PVT 변동에 대한 비교기 출력 펄스 폭 모의실험 결과를 보여주고 있다. 그림 5의 DC 전류 바이어스 IBIASP_CSA를 인가하는 CSA 회로를 사용하여 0.18 μ m CMOS 공정으로 설계된 베타선 센서는 corner별 모의실험 결과 표 3과 표 4에서 보는 바와 같이 CSA_OUT 신호의 최소 신호전압과 최대 신호전압은 각각 205mV와 303mV이고, pulse shaper를 거친 출력 신호를 비교기의 VTHR (Threshold Voltage) 전압과 비교해서 발생된 펄스의 최소와 최대 폭은 각각 0.579 μ s와

표 3. 그림 5의 DC 전류 바이어스 IBIASP_CSA를 인가하는 제안된 CSA 회로의 PVT 변동에 대한 신호전압 모의실험 결과.

Table 3. Signal voltage simulation results for PVT variation of the proposed CSA circuit applying the DC current bias IBIASP_CSA in Figure 5.

VDD	TEMP	SS Model	SF Model	TT Model	FS Model	FF Model
4.5V	-40°C	225mV	256mV	253mV	251mV	287mV
	25°C	215mV	243mV	241mV	239mV	274mV
	85°C	205mV	277mV	235mV	215mV	281mV
5V	-40°C	230mV	262mV	258mV	255mV	292mV
	25°C	220mV	251mV	248mV	246mV	280mV
	85°C	211mV	289mV	241mV	222mV	291mV
5.5V	-40°C	233mV	264mV	261mV	260mV	295mV
	25°C	225mV	252mV	251mV	250mV	283mV
	85°C	215mV	293mV	245mV	228mV	303mV

1.247 μ s로 일부 모의실험 조건에서 폭의 변동이 DC 전압 VBIASP_CSA를 인가하는 CSA 회로보다 작은 것을 볼 수 있다.

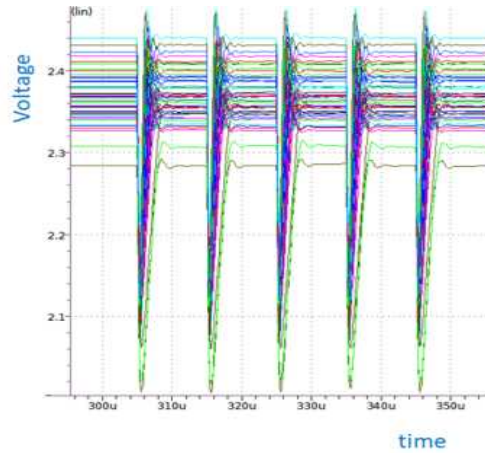
표 4. 그림 5의 DC 전류 바이어스 IBIASP_CSA를 인가하는 CSA 회로를 사용한 베타선 센서의 PVT 변동에 대한 비교 출력 펄스 폭 모의실험 결과.

Table 4. Comparator output pulse width simulation results for PVT fluctuations of a beta ray sensor using a CSA circuit applying the DC current bias IBIASP_CSA in Figure 5.

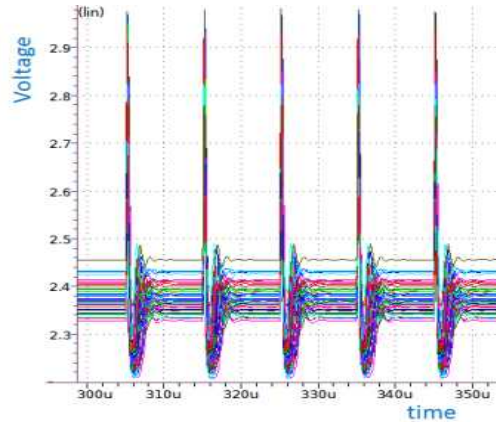
VDD	TEMP	SS Model	SF Model	TT Model	FS Model	FF Model
4.5V	-40 $^{\circ}$ C	1.247 μ s	0.885 μ s	0.876 μ s	0.863 μ s	0.637 μ s
	25 $^{\circ}$ C	1.144 μ s	0.828 μ s	0.812 μ s	0.801 μ s	0.605 μ s
	85 $^{\circ}$ C	1.077 μ s	1.144 μ s	0.805 μ s	0.692 μ s	0.660 μ s
5V	-40 $^{\circ}$ C	1.233 μ s	0.878 μ s	0.861 μ s	0.851 μ s	0.629 μ s
	25 $^{\circ}$ C	1.125 μ s	0.824 μ s	0.806 μ s	0.788 μ s	0.592 μ s
	85 $^{\circ}$ C	1.065 μ s	1.180 μ s	0.794 μ s	0.678 μ s	0.657 μ s
5.5V	-40 $^{\circ}$ C	1.217 μ s	0.864 μ s	0.853 μ s	0.847 μ s	0.619 μ s
	25 $^{\circ}$ C	1.125 μ s	0.807 μ s	0.787 μ s	0.779 μ s	0.579 μ s
	85 $^{\circ}$ C	1.044 μ s	1.183 μ s	0.778 μ s	0.672 μ s	0.668 μ s

그림 7은 제안된 CSA 회로를 사용한 베타선 센서 회로에서 MOS 트랜지스터 모델 파라미터(SS/SF/TT/FS/FF), VDD(4.5V/5V/5.5V)와 Temp.(-40 $^{\circ}$ C/25 $^{\circ}$ C/85 $^{\circ}$ C)별 corner 모의실험 조건별 신호전압인 CSA_OUT, DIFF_OUT, INT_OUT과 COMP_OUT에 대한 모의실험 결과를 보여주고 있다, 그림 1의 미분기와 적분기를 사용한 pulse shaper는 저주파와 고주파 노이즈를 필터링하는 BPF (Band Pass Filter) 역할을 한다. Pulse shaper를 거친 출력 신호를 비교기의 VTHR (Threshold Voltage) 전압과 비교해서 발생된 출력신호인 COMP_OUT의 모의실험 결과는 그림 7(d)에서 보는바와 같으며, COMP_OUT의 펄스 폭은 표 4에서 보는바와 같다. 한편 COMP_OUT 펄스의 최소와 최대 폭은 각각 0.579 μ s와 1.247 μ s로 폭의 변동이 DC 전압 VBIASP_CSA를 인가하는 CSA 회로보다

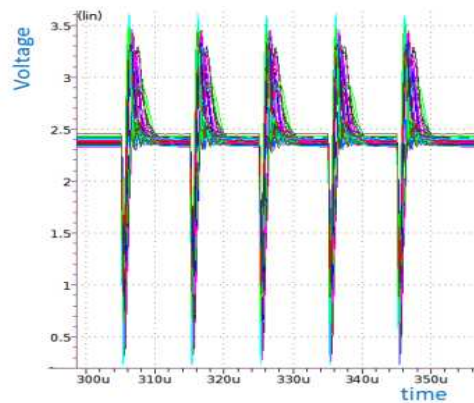
작은 것을 볼 수 있다.



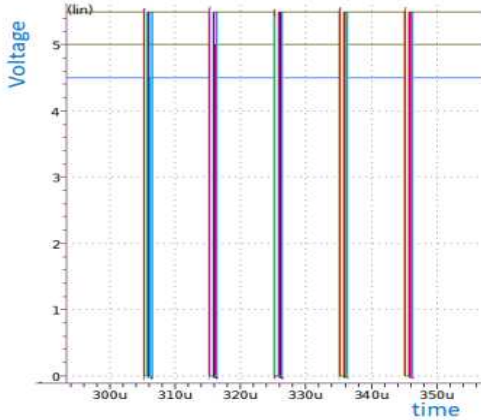
(a) CSA_OUT



(b) DIFF_OUT



(c) INT_OUT



(d) COMP_OUT

그림 7. 제안된 CSA 회로를 사용한 베타선 센서 회로에서 corner별 신호전압에 대한 모의실험 결과.

Fig. 7. Corner simulation results for signal voltage in the beta ray sensor circuit using the proposed CSA circuit.

한편 그림 8은 0.18 μ m CMOS 공정으로 설계된 베타선 센서 칩의 레이아웃 이미지를 보여주고 있다.

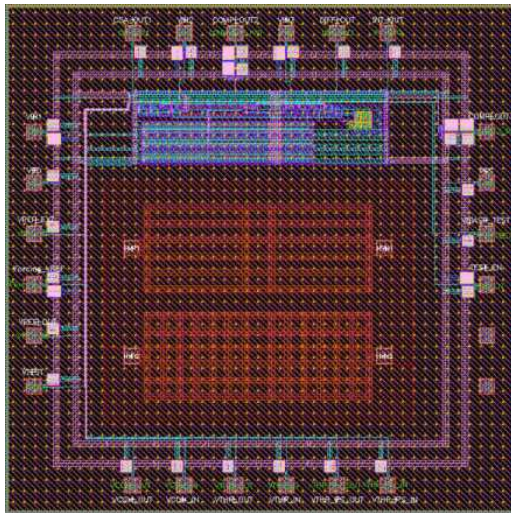


그림 8. 0.18 μ m CMOS 공정으로 설계된 베타선 센서 칩의 레이아웃 이미지.

Fig. 8. Layout image of beta ray sensor chip designed with 0.18 μ m CMOS process.

4. 결론

난수는 암호화와 모의실험 등의 높은 보안등급, 고신뢰성을 요구하는 IoT 보안 분야에서는 날로 고도화되고 있는 해킹을 방지하는데 가장 효과적인 진성난수를 사용하고 있다.

본 논문에서는 방사선 중 Ni-63 베타선원은 차폐가 용이하고, 크기가 작고, 휴대성이 높고, 발생속도가 높고 반도체 손상이 낮은 장점이 있으므로 진성난수 생성기를 위한 베타선 센서를 설계하였다. PMOS 피드백 트랜지스터의 게이트를 DC 전압으로 바이어스하는 대신 PMOS 피드백 트랜지스터에 흐르는 전류가 PVT 변동에 둔감하도록 설계된 전류 바이어스 회로를 mirroring하게 흐르도록 하므로 CSA의 signal voltage의 변동을 최소화하였다. 그리고 BGR 회로를 이용하여 공급된 정전류를 이용하여 신호 전압을 VCOM 전압레벨까지 충전하므로 충전 시간의 변동을 줄여 고속 감지가 가능하도록 하였다. 또한 노이즈를 줄이고 shaping time을 줄이기 위해 미분기와 적분기를 사용한 pulse shaper를 사용하였다. 0.18 μ m CMOS 공정으로 설계된 베타선 센서는 corner별 모의실험 결과 CSA 회로의 최소 신호전압과 최대 신호전압은 각각 205mV와 303mV이고, pulse shaper를 거친 출력 신호를 비교기의 VTHR 전압과 비교해서 발생된 펄스의 최소와 최대 폭은 각각 0.592 μ s와 1.247 μ s로 100kHz의 고속 감지가 가능한 결과가 나왔으며, 최대 100Kpulse/sec로 계수할 수 있도록 설계하였다.

REFERENCES

[1] M. Herrero-Collantes et al., "Quantum Random Number Generators," Reviews of Modern Physics, Feb. 2017.

[2] K. H. Park et al., "Apparatus and Method for Generating Quantum Random Number," Korean Patent applied no. 10-2018-0054533, May 2018.

[3] John Gribbin, Q is for Quantum, ISBN-13: 978-0684855783, pp. 291-292, 1998.

[4] Anil and Ananthaswamy. How to Turn a Quantum Computer into the Ultimate Randomness Generator. Quanta Magazine. June 19, 2019.

[5] Glen F. Knoll, Radiation Detection and Measurement, Third Edition, John Wiley & Sons Inc., 2000.

[6] W. R. Wampler, B. L. Doyle, "Low-Energy Beta Spectroscopy Using PIN Diodes to Monitor Tritium Surface Contamination", Nuclear Instruments and Methods in Physics Research, A349, pp. 473-480, 1994.

[7] Mihai Culcer, Mariana Iliescu, Marian Curuia, Adrian Enache, Ioan Stefanescu, Catalin Ducu, Viorel Malinovschi, "Tritium Contaminated Surface Monitoring with a Solid-State Device," Proceedings of the International Conference Nuclear Energy for New Europe, 713.1-6, Sep. 2004.

[8] P. Grybos et al., "Measurements of Matching and High Count Rate Performance of Multichannel ASIC for Digital X-Ray Imaging Systems," IEEE Transactions on Nuclear Science, vol. 54, no. 4, Aug. 2007.

[9] S. B. Baek et al., "A Design of Single Pixel Photon Counter for Digital X-ray Image Sensor," Journal of the Korea Institute of Information and Communication Engineering vol. 11, no. 2, Feb. 2007.

[10] Solid State Division Technical Information, "Characteristics and use of Charge amplifier," HAMAMATSU, Oct. 2001.

저자약력

김 영 희(Young-Hee Kim)

[종신회원]



- 1989년 2월 : 경북대학교 전자공학과 (공학사)
- 1997년 2월 : 포항공과대학교 전기전자공학과 (공학석사)
- 2000년 8월 : 포항공과대학교 전기전자공학과 (공학박사)
- 1989년 1월 ~ 2001년 2월 : 현대전자 책임연구원
- 2001년 3월 ~ 현재 : 창원대학교 전자공학과 교수

<관심분야> 메모리 IP 설계, 아날로그 회로 설계, SoC 설계

김 홍 주(HongZhou Jin)

[학생회원]



- 2017년 6월 : 연변대학교 전자정보통신학과 (공학사)
- 2017년 9월 ~ 현재 : 창원대학교 전자공학과 석·박사과정

<관심분야> NVM IP 설계

박 경 환(Kyung-Hwan Park)

[정회원]



- 1993년 : KAIST 전기전자공학과 (공학석사)
- 1997년 : KAIST 전기전자공학과 (공학박사)
- 1997년 ~ 2000년 : 대전 DACOM R&D Center
- 2001년 1월 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야> Radiation 기반 난수 생성기, 무선통신

김 중 범(Jong-Bum Kim)

[정회원]



- 2000년 : 충남대학교 전기공학과 (공학석사)
- 2011년 : KAIST 원자력양자공학과 (공학박사)
- 2000년 1월 ~ 현재 : 한국원자력연구원 책임연구원

〈관심분야〉 양자 난수 생성기
방사성 동위원소 어플리케이션

하 판 봉(Pan-Bong Ha)

[중신회원]



- 1981년 2월 : 부산대학교 전기공학과 (공학사)
- 1983년 2월 : 서울대학교 전자공학과 (공학석사)
- 1993년 2월 : 서울대학교 전자공학과 (공학박사)
- 1987년 3월 ~ 현재 : 창원대학교 전자공학과 교수

〈관심분야〉 임베디드 시스템, SoC 설계