https://doi.org/10.33778/kcsa.2024.24.3.059

SRAM PUF 가속 노화 시험 절차 수립

김 문 석*, 전 승 배**, 박 준 영***

요 약

이 논문은 SRAM PUF(Static Random Access Memory Physically Unclonable Function)의 가속 노화 시험 절차를 제안한다. PUF는 반도체 공정 편차를 이용한 반도체 지문 역할을 하는 하드웨어 보안 기술이다. 따라서, SRAM PUF의 반도체 칩의 노화에 따른 안전성과 안정성 확인이 매우 중요한데, 가속 노화 시험은 반도체 10년 생애주기를 모사하여 반도체 10년 사용 후 PUF 특성을 예측할 수 있도록 도와준다. 온도와 전압을 운영 환경보다 높게 설정하여, 10년간의 노화를 약 9일만에 재현할 수 있는 가속 수명 시험 방법을 제안한다, 이를 통하여 SRAM PUF의 특성 평가를 정량적으로 확인할 수 있다. 이 연구는 SRAM PUF 기반 시스템의 설계 및 유지 보수 시험 기술 발전에 기여할 것으로 기대한다.

Accelerated aging test procedures for SRAM PUFs

Moon-Seok Kim*, Seung-Bae Jeon**, Jun-Young Park***

ABSTRACT

This research proposes an accelerated aging test procedure for Static Random Access Memory Physically Unclonable Functions (SRAM PUFs). PUFs utilize semiconductor process variations to serve as a hardware security feature, akin to semiconductor device fingerprints. Thus, the proposed accelerated aging test simulates a semiconductor's 10-year lifecycle, enabling the prediction of PUF characteristics after a decade of use, which is crucial for verifying the safety and stability of SRAM PUFs. This research introduces test procedures that simulate 10 years of aging in approximately 9 days by setting temperature and voltage higher than operational environments. These procedures allow for the quantitative evaluation of SRAM PUF characteristics. This research is expected to contribute to the advancement of design and maintenance testing techniques for systems based on SRAM PUFs.

Key words : Physically Unclonable Functions(PUFs), Static Random Access Memory (SRAM), Accelerated aging test, Negative Bias Temperature Instability(NBTI)

접수일(2024년 08월 19일), 수정일(1차: 2024년 09월 03일, 2차: 2024년 09월 11일), 게재확정일(2024년 9월 20일)

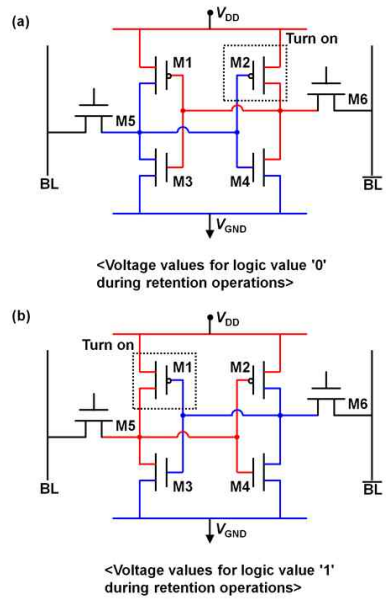
* 국립한밭대학교 반도체시스템공학과 조교수(제1저자)
** 국립한밭대학교 전자공학과 조교수(공동저자)
*** 충북대학교 반도체공학부 부교수(교신저자)

1. 서 론

물리적 복제 방지 회로(Physically Unclonable Function: PUF)는 반도체 지문으로 불리는 하드웨어 보안 기술로 꾸준히 연구되어 왔다 [1]. PUF는 식별, 위조 방지, 중요한 데이터 저장 보호와 같이 여러 보안 분야에 활용할 수 있다. 따라서, 다양한 반도체 소자 형태의 PUF와 다양한 PUF 기반 보안 프로토콜이 주목받고 있다 [2]. 그 중에서, 정적 메모리(Static Random Access Memory: SRAM)는 시스템 반도체 및 임베디드 시스템의 다양한 활용성으로 더욱 주목받고 있다 [3]. 하지만, SRAM 기반 PUF는 낮은 신뢰성으로 인해 보안 프로토콜에 적용하는데 많은 방해를 받고 있다 [4]. 신뢰성을 확인하기 위해 중요한 것은 반도체 노화에 따른 특성 변화를 확인하는 것은 중요하다. 통상적인 반도체는 10년 사용 기한을 가진다 [5]. 노화 시험을 실제 10년에 시간을 허비할 수는 없으므로 반도체 내 주요 주요 노화 요인을 모델링하여 가속 노화 시험을 수행해야 한다. 이 연구는 최초로 SRAM PUF 가속 노화 시험의 이론 모델 및 시험 절차 수립을 수행한다. 구체적으로, 아래와 같은 내용을 포함한다. 첫째, SRAM 반도체의 주요 노화 요일을 모델링하여 가속 요소를 정량적으로 계산한다. 둘째, 수립한 가속 요소를 바탕으로 시험 절차를 수립한다. 마지막으로, 시험 결과 예시를 제시하여 시험자가 시험 결과를 생산하는데 도움을 준다.

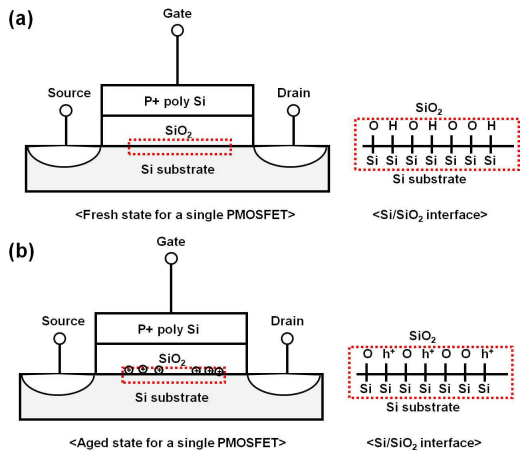
2. 가속 수명 이론 모델

SRAM PUF 가속 노화 시험의 목적은 SRAM PUF의 노화에 따른 PUF 특성 변화에 변화를 확인하는 것이 목적이다. PUF 특성은 반도체 지문의 특징인 예측 불가능성, 특이성, 견고성을 의미한다 [3]. 따라서, SRAM PUF의 10년 노화 효과를 모사하여 노화 효과에 따른 PUF 특성 변화를 추적하는 것을 SRAM PUF 가속 노화 시험의 목표로 한다. 반도체 신뢰성 가속 수명 시험은 주요 노후 메커니즘을 선정하고 그의 맞게 가속 요소(Acceleration factor)를 계산해 10년 후 반도체 제품의 신뢰성을 모사한다. SRAM PUF는 1비트 정보가 6개의 MOSFET (Metal Oxide Semiconductor Field Effect Transistors) 반도체 소자로 구성된 장치이다 [3]. MOSFET 반도체 소자로 동작하는 집적 회로 (Integrated Circuits: ICs)는 게이트 절연체 손상 (Gate oxide wear out), 연결 불량(Interconnect failure)의 주요 노후 메커니즘이 있다 [6]. 그 중, SRAM PUF의 주요 노후 메커니즘은 NBTI (Negative Bias Temperature Instability)이다 [7-8]. NBTI는 게이트 절연체가 노화되면서 PMOS (Positive Metal Oxide Semiconductor) 트랜지스터의 문턱전압이 변하는 현상이다 [9-10]. SRAM PUF의 반도체 지문 기능은 SRAM 단위 셀 내 트랜지스터들의 문턱전압의 차이에서 발생한다. 하지만, NBTI 현상은 PMOS 트랜지스터들의 문턱전압을 변화시켜 SRAM PUF의 지문 특성을 변화 시킨다. NBTI로 인한 노화 발생 현상은 PMOS 트랜지스터의 게이트 스위치 on (inversion mode) 상태일 때, 발생한다 [11-12]. (그림 1)은 SRAM 단위 셀에 데이터 저장 상태 (Retention state)일 때 전압 상태를 보여준다.



(그림 1) 논리 값에 따른 SRAM 단위셀 내 전압

논리값 0일 때는 M2 PMOS 트랜지스터가 스위치 ON 상태이고, 논리 값 1 일때는 M1 PMOS 트랜지스터가 스위치 ON 상태이다. SRAM은 반도체 칩에 전원이 인가할 때는 항상 데이터 저장 상태이다. 즉, SRAM PUF 전원을 인가하는 만큼 NBTI에 의한 SRAM PUF 노화 현상이 발생한다는 것을 의미한다. NBTI 현상은 PMOS 트랜지스터의 문턱 전압 상승, 가동 전류 (on current) 감소, 문턱전압 전 기울기 (subthreshold slope) 증가의 노화 현상을 발생시킨다 [7-8]. (그림 2)는 PMOSFET 노화에 따른 실리콘(Si) 몸체(substrate)와 산화실리콘(SiO_2) 게이트 절연체(gate dielectric) 접촉면(interface) 사이의 결합 변화를 보여준다. 노화가 없는 PMOS 트랜지스터의 경우 두 물질 표면에서 실리콘과 수소가 결합하고 있다. 하지만 PMOS 트랜지스터는 NBTI 현상을 통하여 아래 현상들이 나타난다. 첫째, PMOS 트랜지스터 스위치가 turn on 상태일 때, Si/SiO2 접촉면에서 전자(electron)들이 방출되고 정공(hole, h^+)들이 축적된다 [9]. 둘째, 축적된 정공들이 Si과 수소 결합을 약하게 만들어 실리콘은 수소 대신 정공과 결합하는 현상이 발생한다 [9]. 셋째, 실리콘과 결합한 정공은 PMOS 트랜지스터의 인터페이스 트랩 역할을 한다 [9]. 마지막으로, 인터페이스 트랩은 PMOS의 아래와 같은 노화 현상을 발생시킨다. 문턱 전압 상승, 가동 전류 (on current) 감소, 문턱전압 전 기울기 (subthreshold slope) 증가의 노화 현상을 발생시킨다. 정리하면, SRAM PUF의 주요 노후 메커니즘은 Gate 절연체 노화에 의한 PMOS 트랜지스터의 문턱전압이 변하는 현상으로 게이트 절연체 가속 노화 시험 절차 수립이 필요하다. (그림 3)은 가속 요소 (Acceleration factor) 계산 순서를 보여준다. Net acceleration factor (NAF)에 의미는 설정한 가속 수명 시험 절차는 400배 노화를 발생하는 것을 의미한다. 9일 간의 가속 시험은 10년 간의 노화와 등과 노화 효과임을 보여준다. NAF는 temperature acceleration factor (TAF)와 voltage acceleration factor (VAF)의 곱으로 계산한다 [6-7].



(그림 2) PMOSFET NBTI 노화에 따른 특성 변화

이는 온도와 전압을 운영 온도와 전압보다 높은 스트레스로 인가하여 높은 가속 효율에 가속 수명 시험을 수행하는 것을 의미한다. (그림 3)의 가속 요소 계산은 게이트 절연체(t_{ox})가 10 nm, 온도는 섭씨 영상 80도, 전압은 1.6 V로 설정하였을 때의 계산 과정을 보여준다. (그림 3)의 계산을 활용하여 시험자의 시험 환경에 맞게 온도와 전압을 설정하여 TAF와 VAF를 설정하고 가속 노화 시험 절차를 설계할 수 있다. 게이트 절연체가 더 얇은 수록 NBTI에 의한 가속 효과가 크게 나타나고, 온도와 전압을 큰 값으로 설정할수록 가속 요소가 높아진다.

<Acceleration factor>

① Net acceleration factor = TAF · VAF

TAF: Temperature acceleration factor

VAF: Voltage acceleration factor

② $TAF = exp\left(\frac{E_a}{k \cdot T_{operation}} - \frac{E_a}{k \cdot T_{stress}}\right)$

$VAF = exp(\frac{\gamma}{t_{ox}}(V_{stress} - V_{operation}))$

③ parameter values against gate oxide break down

- **E_a (activation energy) = 0.7 eV**
- **k (Boltzmann's constant) = $8.62 \cdot 10^{-5}$ eV/K**
- **γ (voltage exponent factor)= 3.2**
- **t_{ox} = 10 nm**
- **$T_{operation}$ = 298 K, T_{stress} = 353 K**
- **$V_{operation}$ = 1.5V, V_{stress} = 1.6V**

④ Net acceleration factor = 69.81 · 5.92 = 413.07

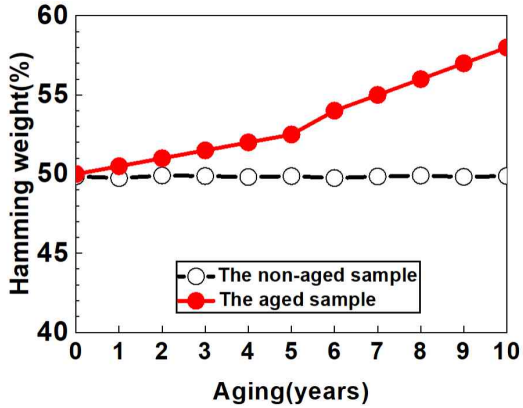
(그림 3) SRAM PUF acceleration factor 계산

3. SRAM PUF 가속 노화 시험 절차

<표 1>은 SRAM PUF 가속 노화 시험 절차를 보여준다. 온도와 전압을 운영 환경보다 높은 값으로 설정하여 가속 노화 시험을 수행한다. (그림 3)에 계산하였듯이 413.7에 가속 요소는 21시간 12분 가속 노화 시험이 SRAM PUF의 1년 노화를 모사한다. 1년 가속 노화할 때마다 PUF 특성을 측정한다. 이 절차를 10번 반복하여 결과적으로 10년 노화를 모사하는 가속 노화 시험을 수행한다. 10번 반복의 의미는 1년 단위로 가속 노화 시험 결과를 추적 관리하는 의미를 가진다.

<표 1> SRAM PUF 가속 노화 시험 절차

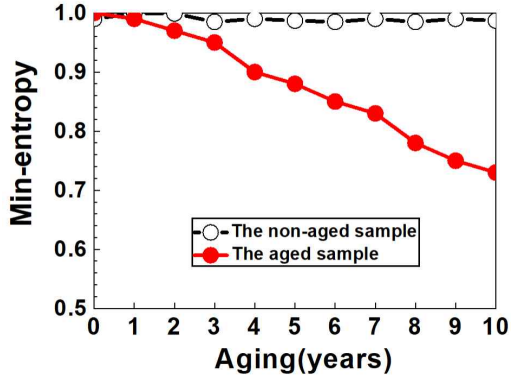
순서	내용
(1)	가속 환경 섭씨 80℃, 전압 1.6V 설정
(2)	시험 대상 가속 시험 스트레스 인가
(2)	21시간 12분(정상동작 1년 모사) SRAM PUF 스트레스 인가
(3)	정상동작 환경 섭씨 25℃, 전압 1.5V) 설정
(5)	SRAM PUF 출력 읽기 및 특성값 추출
(6)	(1)-(5) 과정 10회 반복하여 10년 노화 모사 후 PUF 특성 평가 및 분석



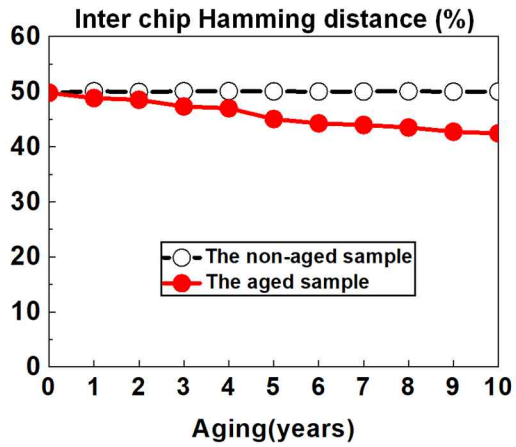
(그림 4) 해밍 웨이트 가속 노화 시험 결과 예시

4. PUF 가속 노화 시험 결과 예시

(그림 4)는 SRAM PUF 가속 노화 시험 해밍 웨이트 시험 결과 예시를 보여준다. 노화 정도에 따른 해밍 웨이트 결과를 시각적으로 확인할 수 있다. SRAM PUF가 노화의 영향을 받지 않으면, 검은 실선(The non-aged sample)과 같이 노화 전 상태를 유지한다. 반대로, SRAM PUF과 가속 노화 상태가 되면 빨간 실선(The aged sample)과 같이 해밍 웨이트 결과가 노화 정도에 따라 달라진다. (그림 5)는 SRAM PUF 가속 노화 시험 최소 엔트로피 시험 결과 예시를 보여준다. (그림 4)와 마찬가지로, 검은 실선(The non-aged sample)은 노화 면역(Aging immunity)이 있는 결과 예시이고, 빨간 실선(The aged sample)는 노화 효과로 최소 엔트로피가 감소한 예시를 보여준다. 노화 정도에 따른 최소 엔트로피 결과를 시각적으로 확인할 수 있다. (그림 6)은 SRAM PUF 가속 노화 시험 인터 칩 (Inter chip) 해밍 거리 시험 결과 예시를 보여준다. 노화 정도에 따른 인터 칩 해밍 거리를 확인하여 PUF 특이성 특성을 확인한다. SRAM PUF가 노화 효과로 특성 열화 현상이 발생하면 빨간 실선(The aged sample)처럼 해밍 거리가 감소하는 현상이 발생한다. (그림 7)은 SRAM PUF 가속 노화 시험 인트라 칩 (Intra chip) 해밍 거리 시험 결과 예시를 보여준다. 노화 정도에 따른 인트라 칩 해밍 거리를 확인하여 PUF 견고성 특성을 확인한다. SRAM PUF 노화로 인한 특성 열화 현상이 발생하면 (그림 7)의 빨간 실선(The aged sample)과 같이 인트라 칩 해밍 거리가 증가하는 현상이 발생한다.

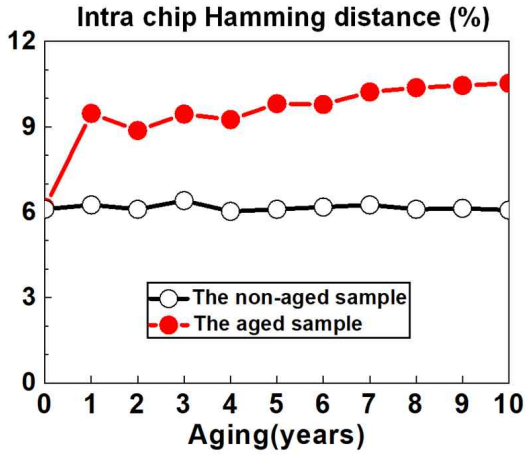


(그림 5) 최소 엔트로피 가속 노화 시험 결과 예시



(그림 6) 인터 칩 해밍거리 가속 노화 시험 결과 예시

결과적으로, PUF 가속 노화 시험을 통하여 해밍 웨이트, 최소 엔트로피, 인터 칩 해밍거리, 인트라 칩 해밍거리 결과를 시각화하여 실험군의 PUF 특성 변화를 확인할 수 있다 [13]. <표 2>는 PUF 특성 평가 지표인 해밍 웨이트, 최소 엔트로피, 인터 칩 해밍거리, 인트라 칩 해밍 거리의 가속 노화 시험 합격 판정 기준 예시를 정리하여 보여준다. <표 2>를 통하여 PUF 특성 지표들의 판정 기준을 정량적으로 명시하였다. 특성 지표에 따라 판정 기준을 만족을 못하는 것은 PUF의 기능을 못하는 것을 의미한다. 하지만, 판정기준의 정량적 수치는 PUF 응용 요구사항에 따라 달라진다 [13].



(그림 7) 인트라 칩 해밍거리 가속 노화 시험 결과 예시

<표 2> SRAM PUF 가속 노화 시험 합격 기준 예시

특성 지표	판정 기준
해밍 웨이트	0~10년 모든 노화 구간에서 45% 이상 및 55% 이하 만족 $0.45 \leq HW \leq 0.55$
최소 엔트로피	0~10년 모든 노화 구간에서 0.9 이상 만족 $0.9 \leq E_{MIN}$
인터칩 해밍거리	0~10년 모든 노화 구간에서 45% 이상 및 55% 이하 만족 $0.45 \leq HD_{inter} \leq 0.55$
인트라 칩 해밍거리	0~10년 모든 노화 구간에서 8% 이하 만족 $HD_{intra} \leq 0.08$

5. 결론

SRAM PUF의 가속 노화 시험을 위한 이론적 절차를 소개하고, 가속 노화 시험 절차 및 시험 결과 예시를 제안하였다. SRAM PUF의 안정성(신뢰성)과 안전성은 반도체 칩의 노화와 밀접하게 연관되어 있으며, SRAM PUF의 경우 Negative Bias Temperature Instability (NBTI) 현상이 주요 노화 메커니즘인 것으로 제안하고, 이에 따른 시험 절차를 수립하였다. 온도와 전압을 운영 환경보다 높게 설정하여 10년치 노화를 약 9일만에 재현할 수 있는 시험 절차이다. 제안하는 가속 노화 시험을 통하여 SRAM PUF의 예측불가능성, 특이성, 견고성 등의 PUF 주요 특성 변화를 직접적으로 평가할 수 있다. 이 연구는 SRAM PUF 기반 시스템의 설계와 유지 보수에 기여하고, 하드웨어 보안 기술 발전에도 기여할 것으로 기대한다.

참고문헌

[1] Kim, M. S., Moon, D. I., Yoo, S. K., Lee, S. H., & Choi, Y. K. (2015). Investigation of physically unclonable functions using flash memory for integrated circuit authentication. IEEE Transactions on Nanotechnology, 14(2), 384-389.

[2] Chatterjee, U., Chakraborty, R. S., & Mukhopadhyay, D. (2017). A PUF-based secure communication protocol for IoT. ACM Transactions on Embedded Computing Systems (TECS), 16(3), 1-25.

[3] Kim, M. S., Kim, S., Yoo, S. K., Lee, B. S., Yu, J. M., Tcho, I. W., & Choi, Y. K. (2023). Error reduction of SRAM-based physically unclonable function for chip authentication. International Journal of Information Security, 22(5), 1087-1098.

[4] Wang, W., Singh, A. D., & Guin, U. (2022). A systematic bit selection method for robust SRAM PUFs. Journal of Electronic Testing, 38(3), 235-246.

[5] Yun, G., Jung, H. W., & Park, S. (2018). Prediction of field failure rate using data mining in the automotive semiconductor. Procedia computer science, 139, 512-520.

[6] Intel, (2023). High reliability design guidance.

[7] Yang, S. F., & Chien, W. T. K. (2009). Failure rate calculation: Extending JESD74/JESD74A to any sample size. In 2009 IEEE International Conference on Industrial Engineering and Engineering Management (pp. 204-207). IEEE.

[8] Velamala, J. B., Sutaria, K. B., Ravi, V. S., & Cao, Y. (2012). Failure analysis of asymmetric aging under NBTI. IEEE Transactions on Device and Materials Reliability, 13(2), 340-349.

[9] Ceratti, A., Copetti, T., Bolzani, L., & Vargas, F. (2012, April). On-chip aging sensor to monitor NBTI effect in nano-scale SRAM. In 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS) (pp. 354-359). IEEE.

[10] Alam, M. A., & Mahapatra, S. (2005). A comprehensive model of PMOS NBTI degradation. Microelectronics Reliability, 45(1), 71-81.

[11] Bhatta, N. P., Al Majmaie, S., Amsaad, F., Jhanjhi, N., & Soomro, T. R. (2024, January). SRAM PUFs: A Study of Aging Impact and Potential Mitigation. In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-5). IEEE.

[12] Zhang, J. F., Gao, R., Duan, M., Ji, Z., Zhang, W., & Marsland, J. (2022). Bias temperature instability of mosfets: Physical processes, models, and prediction. Electronics, 11(9), 1420.

[13] Kim, M. S. (2023). A Study of Quantitative Characterization of Physically Uncloanble Functions. Convergence Security Journal, 23(5), 143-150.

〔저자소개〕

김 문 석 (Moon-Seok Kim)
2011년 2월 중앙대학교 학사
2013년 2월 한국과학기술원 석사
2022년 2월 한국과학기술원 박사
2023년 9월~현재: 국립한밭대학교 반도체시스템공학과 조교수
email : mskim@hanbat.ac.kr

전 승 배 (Seung-Bae Jeon)
2013년 2월 한국과학기술원 학사
2015년 2월 한국과학기술원 석사
2019년 2월 한국과학기술원 박사
2021년 9월~현재: 국립한밭대학교 전자공학과 조교수
email : sbjeon@hanbat.ac.kr

박 준 영 (Jun-Young Park)
2014년 2월 연세대학교 학사
2016년 2월 한국과학기술원 석사
2020년 2월 한국과학기술원 박사
2020년 9월~현재: 충북대학교 반도체공학부 부교수
email : junyoung@cbnu.ac.kr