

SRAM 기반 PUF 시스템의 Discard-rate 분석

¹유지민, ¹남재원, ²홍종필

¹서울과학기술대학교, ²충북대학교

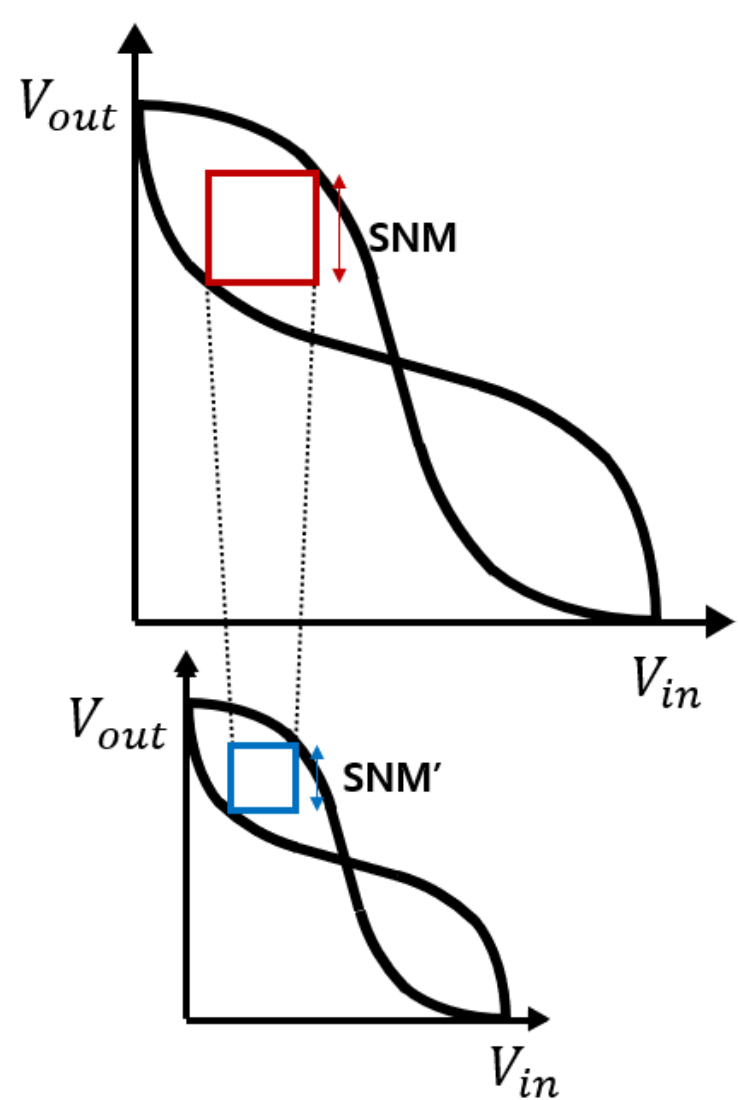
● Introduction

- 반도체 PUF: 공정의 미세구조 차이를 활용, 물리적 복제 불가능한 보안키 생성회로
- SRAM-based PUF + 고집적화 + CRP기술
 - 난수 생성의 확장성 증대 😊
 - 불안정한 셀 존재 → 시스템 BER ↓ 😞
- This work: SRAM-based PUF 상위수준 모델링
 - Process mismatch & Active circuit noise 반영
 - 불안정한 셀을 배제하는 **Discard 기법**에 관한 연구

● Objectives

- 이상적인 PUF 특징의 지표화: 신뢰성, 고유성, 일관성 (NIST 800 22A 기준을 준수)
- SRAM-PUF의 기술적 한계 분석
 - 일관성 지표달성의 어려움: 공정편차 ↑ but, SNM ↓
 - 목표 BER 달성을 위한 **Discard-rate ↑**
- 공정 미세화에 따른 Discard-rate의 정확한 예측 필요
 - SRAM PUF의 상위수준 모델링
 - Power-up 동작에서 잡음에 따른 BER 열화 예측

● SNM change by technode scaling



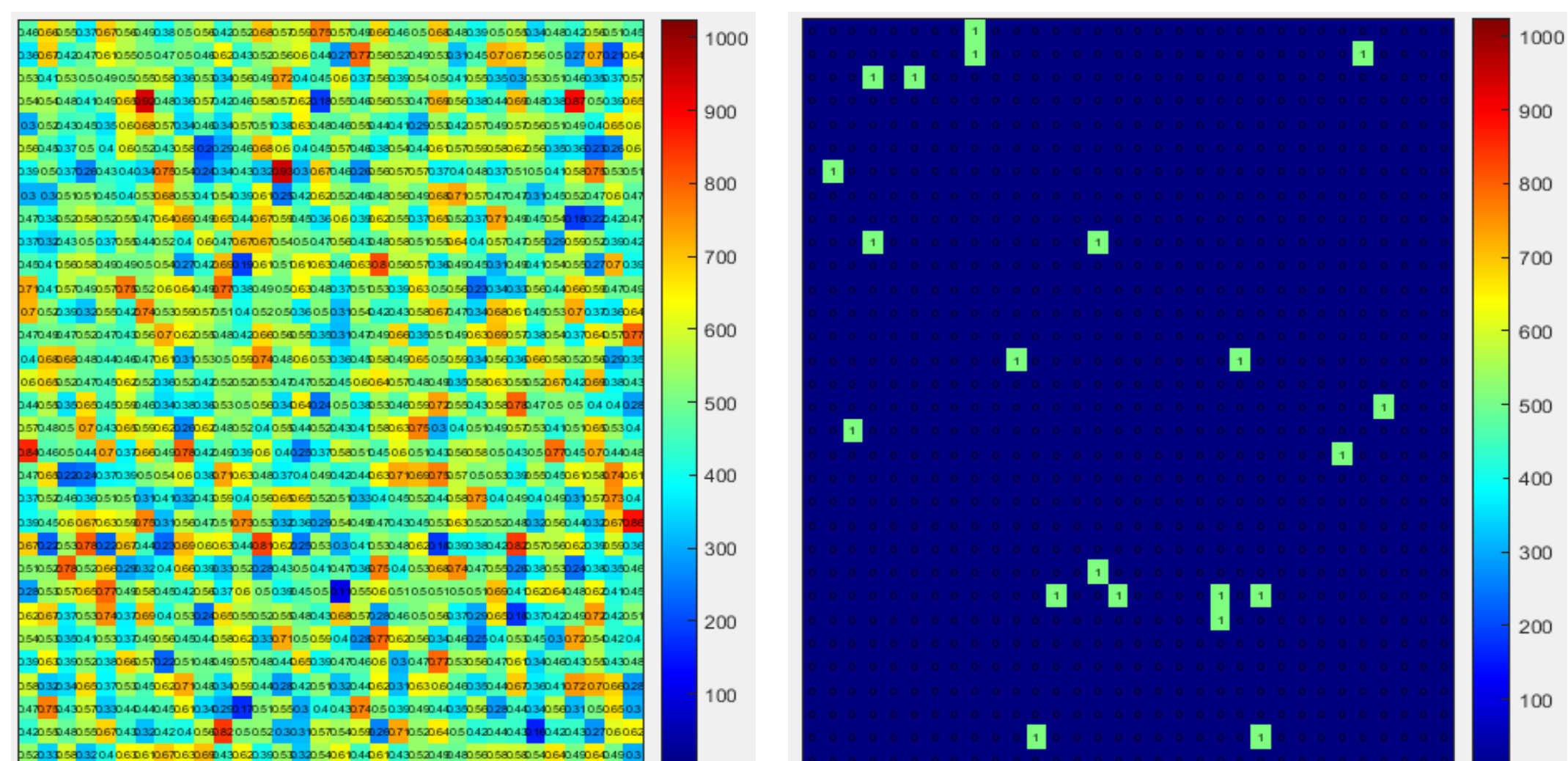
- 공정 미세화 기술 발달
 - 소형화로 인한 SNM 감소
 - 잡음 크기 변화 없음
 - 잡음 취약 SRAM cell 증가
- (상) 기존 공정의 SNM
- (하) 미세화 공정의 감소한 SNM

● Operating Principles

- SRAM-PUF의 일관된 출력: 공정 편차의 영향
 - 잡음 > 공정 편차: 일관된 출력 생성 불가
 - 공정 편차 ↓ = 외부 요인 영향 ↑ = 일관성 ↓
 - Discard-rate ↑
- Discard-rate 계산 방법
 - 공정 편차와 잡음 크기 비교
 - 목표 BER과 노이즈 크기에 따른 Discard-rate 예측

● High-level behavior modeling

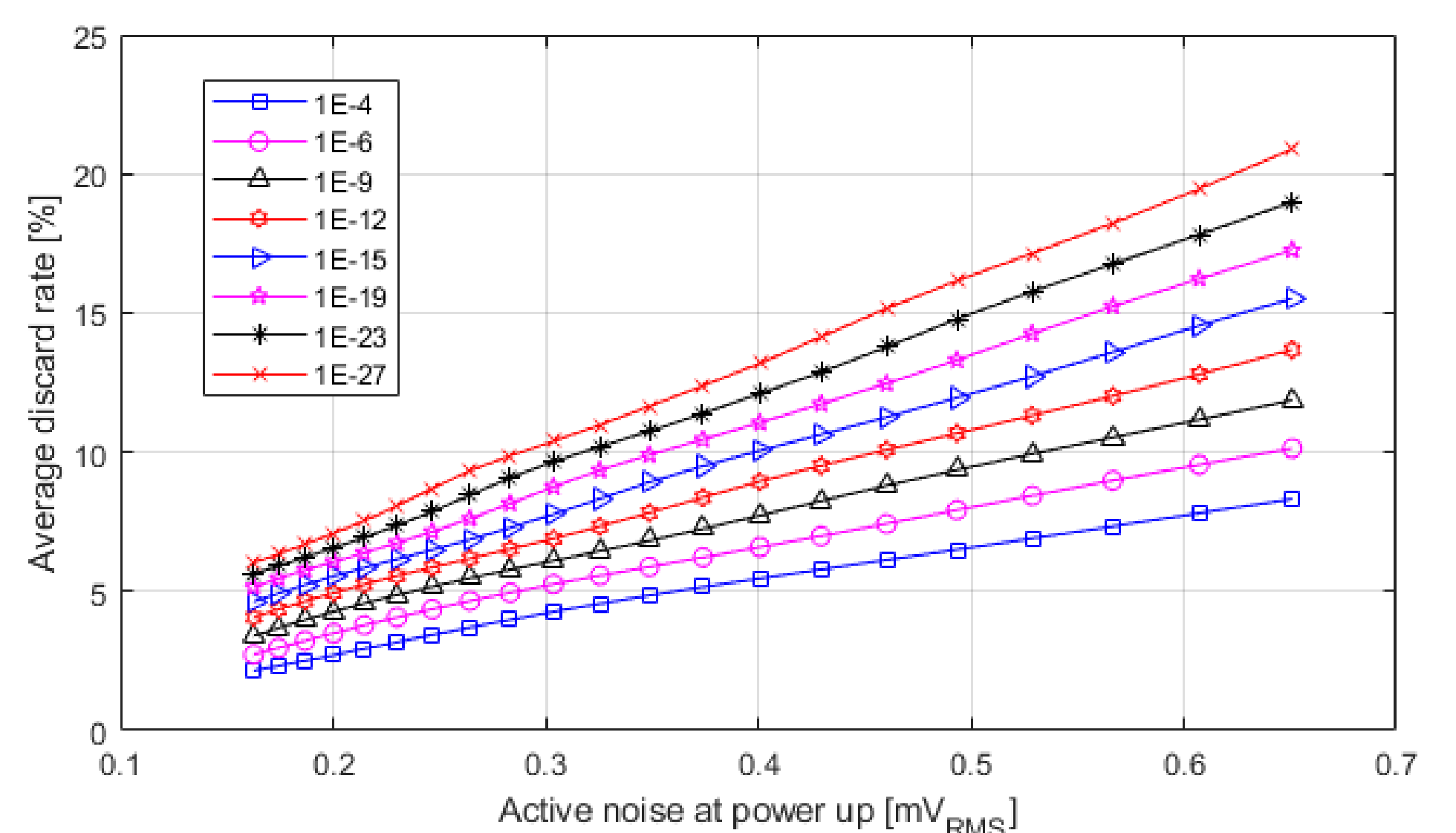
- SRAM PUF 상위수준 모델링 (MATLAB)
 - 32x32 SRAM Array 모델링 (공정편차 반영)
 - Power-up Sequence 능동잡음 반영 (2mV_{RMS})
 - 복수의 Power-up 동작을 통한 불안정한 셀 계측



- (좌) 32x32 SRAM 셀 공정 편차 시각화 결과
- (우) 계측된 불안정한 셀 시각화 결과
 - 1024개의 셀 중 21개의 셀이 불안정한 셀로 계측됨

● Conclusion

- SRAM 기반 PUF의 Average discard-rate 분석 결과



- SNM 차이와 Power-up Sequence 능동잡음 비교
 - 능동잡음 증가 → Average discard rate 증가
- 목표 BER에 따른 불안정 셀 계측
 - 목표 BER 증가 → Average discard rate 증가