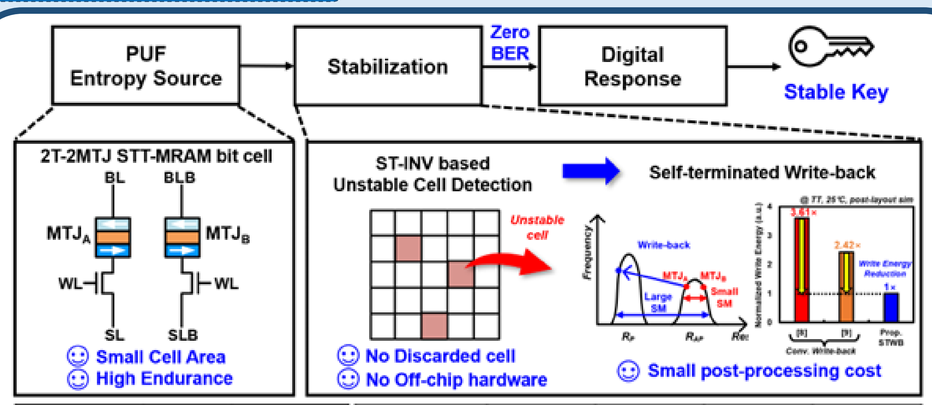
IDEC Chip Design Contest

A Highly Reliable Embedded STT-MRAM Physical Unclonable Function with Two-Step Post-Processing

[1]Donghan Ko, [1]Wangyu Lee, and [1]Seong-Ook Jung
[1]*Yonsei University, Korea*

1. Introduction

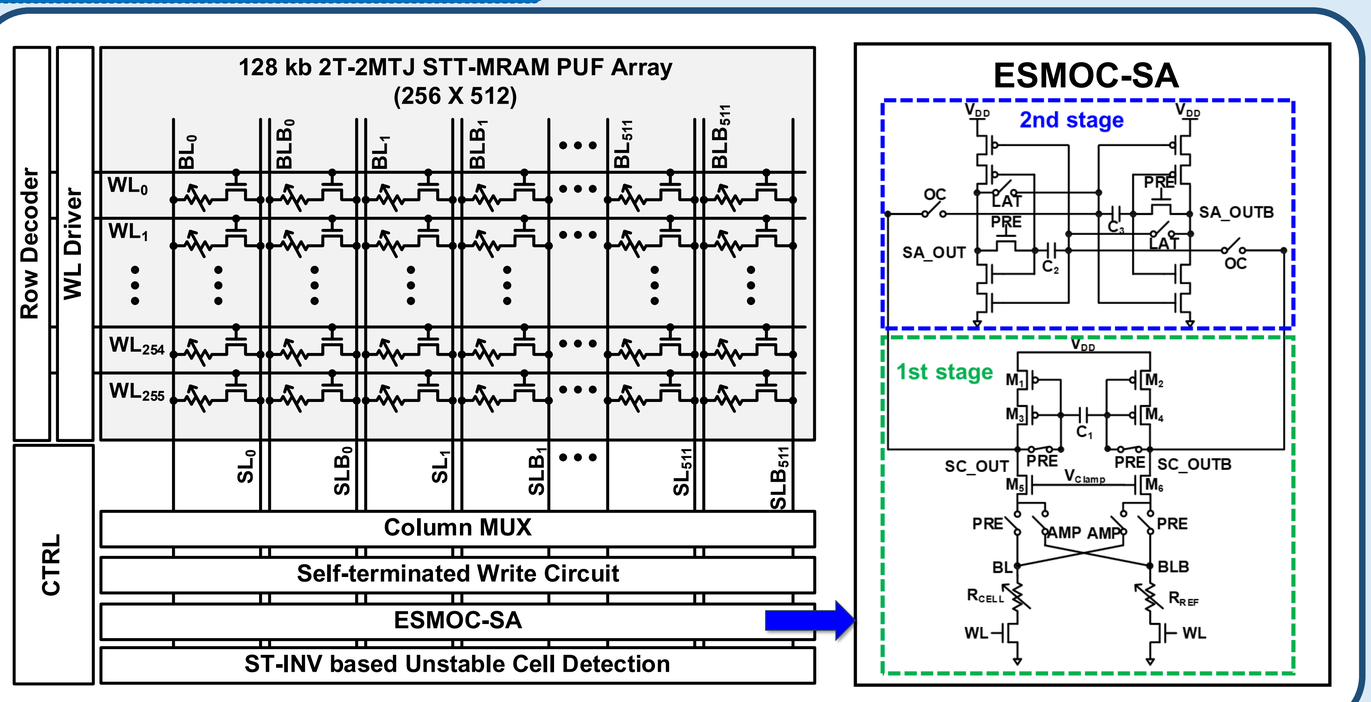


Entropy Source	Cell Area (F^2)	Endurance
RO	>10000	High
SRAM	>400	High
Arbiter	>10000	High
Diode INV.	>500	High
RRAM	169	Low (<10^5)
STT-MRAM (This work)	115	High (>10^{14})

Stabilization Method	Discarded Cell	On-chip Hardware	Off-chip Hardware	Test Time
ECC	No	High	High	Medium
Remapping	No	Low	High	Medium
TMV	No	Low	Low	Medium
Masking	Yes	High	High	Medium
HCI burn-in	No	Low	Low	High
This work	No	Low	Low	Low

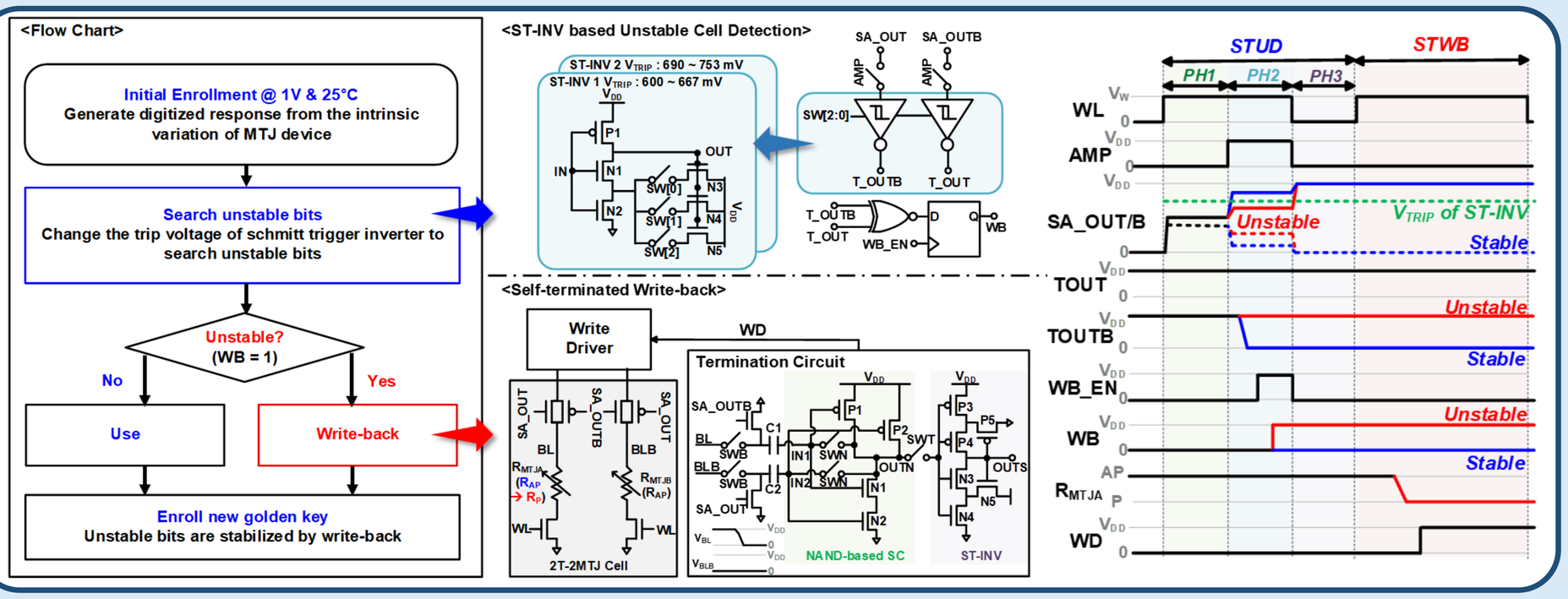
- 기존 PUF Cell은 높은 면적을 가지고 있으며, post-processing 적용 시 높은 hardware overhead의 한계를 보임
- 제안 PUF는 2T-2MTJ cell을 사용하여 면적이 작으며, hardware overhead가 적으며 동시에 낮은 BER 달성이 가능한 post-processing을 제안함.

2. Proposed ESMOC-SA



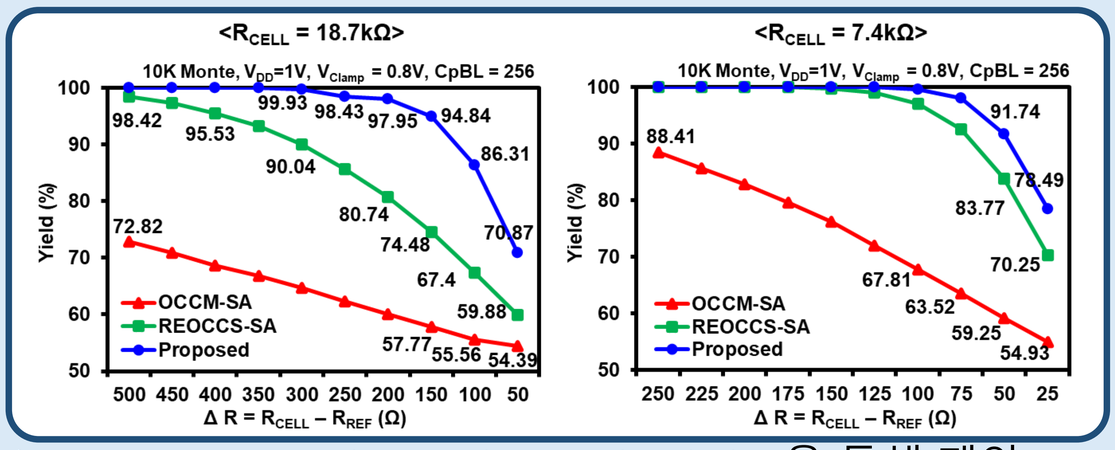
- PUF는 device의 variation 차이를 sensing 하기 때문에, sensing margin이 적으며 transistor mismatch에 의한 randomness 저하가 발생함
- ➔ Enhanced sensing margin offset-cancel SA (ESMOC-SA)를 제안
- 제안 SA은 dual-input stacked inverter based latch를 이용하여 sensing margin이 높으며, offset-cancel capacitor로 인해 mismatch 영향 적음

3. Proposed Post-Processing



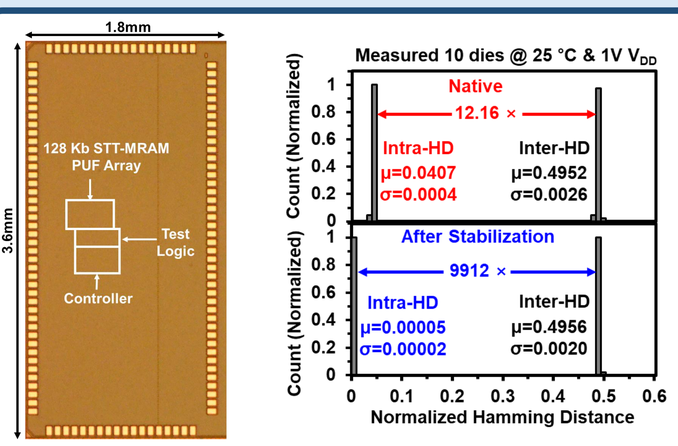
- 제안post-processing은 Schmitt-trigger inverter의 trip voltage를 trimming하여 unstable cell 판별
- 이후 unstable cell은 self-terminated write-back을 이용하여, stabilization 진행
- Masking과 비교하여,Off-chip hardware가 필요하지 않아, hardware overhead가 적음

4. Simulation Results



- 10K Monte Carlo post-layout simulation을 통해 제안 SA의 read yield를 검증함
- MTJ device의 resistance가 적은 상황에서도, 최신 SA 구조와 비교하여 높은 read yield 달성이 가능
- ➔ PUF의 high randomness 달성에 적합

5. Chip Measurement Results & Conclusion



	Specification
Technology	28nm
Entropy Source	STT-MRAM
PUF Cell structure	2T2MTJ
PUF Cell Area/Bit (F^2)	115
Total Entropy	128 Kb
Voltage (V)	0.8-1.2
Temperature (°C)	-25-75
Native BER	4.07E-01
BER after Stabilization	4.6E-05
Energy/bit (pJ)	0.149

- 28nm FDSOI 공정에서, PUF의 성능 test 진행
- 제안 PUF는 0.4956의 Inter-HD를 달성하여, 높은 randomness 검증
- 0.8V~1.2V, -25°C~75 °C 구간에서 worst BER 0.0046% 달성