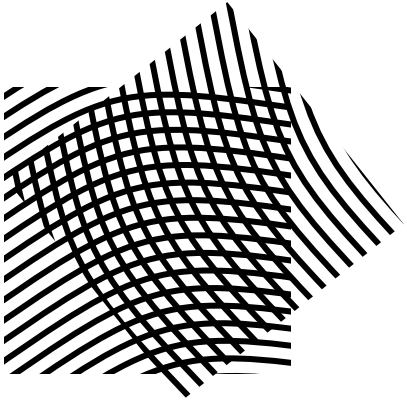


A Cautionary Note When Looking For a Truly Reconfigurable Resistive RAM PUF

Kai-Hsin Chuang, Robin Degraeve, Andrea Fantini,
Guido Groeseneken, Dimitri Linten, Ingrid Verbauwhede

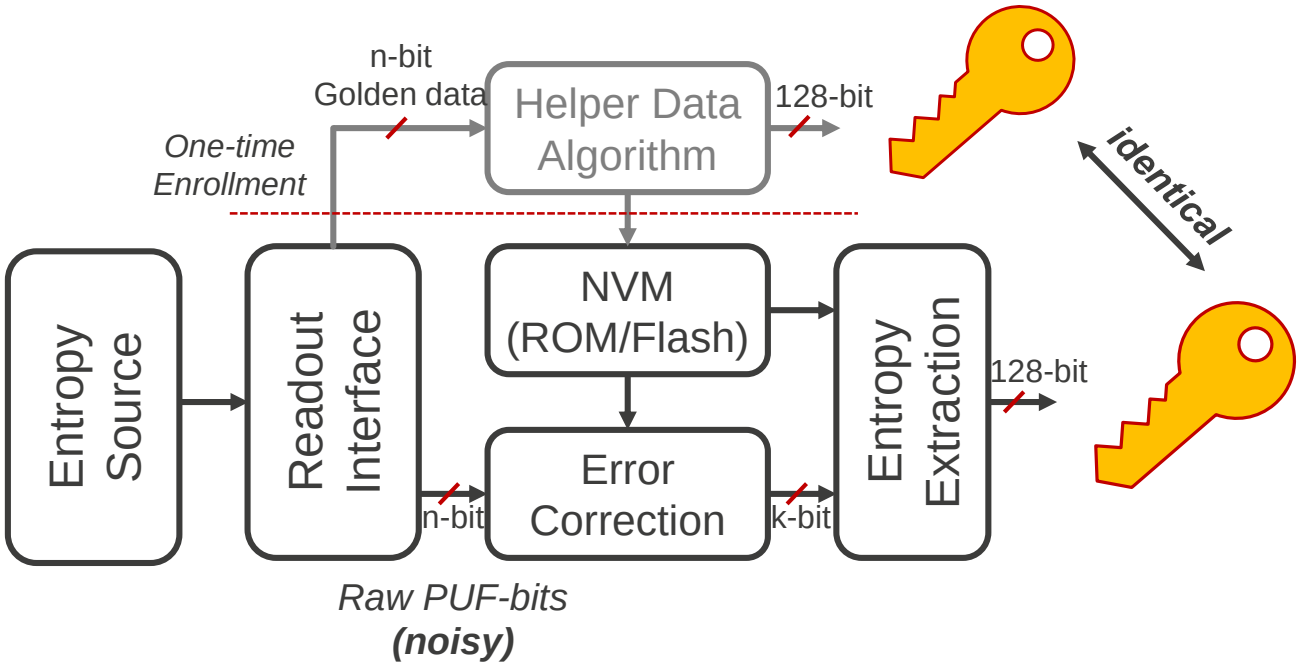
imec

KU LEUVEN

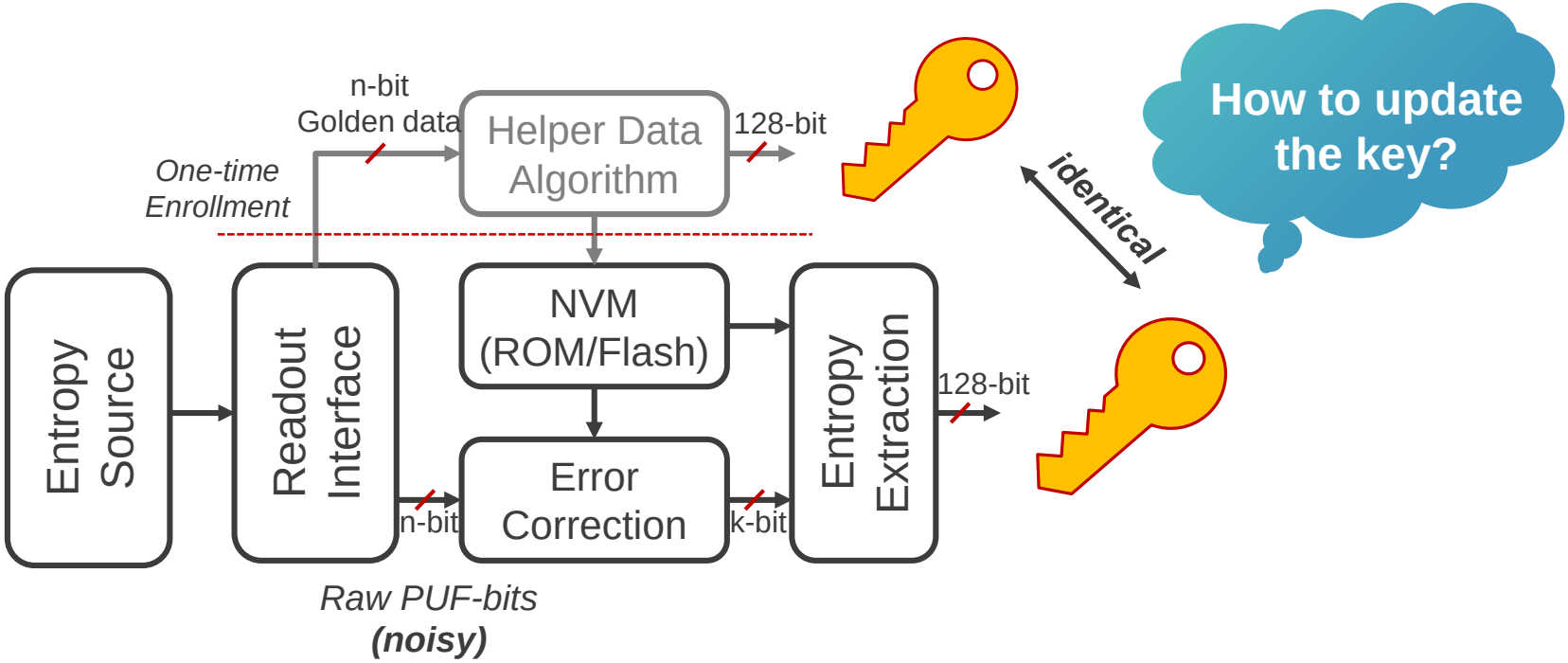
Outline

- Introduction
  - Reconfigurable PUF
  - Variability of RRAM
- RRAM PUF implementations
- Non-ideal reconfigurability
- Conclusion

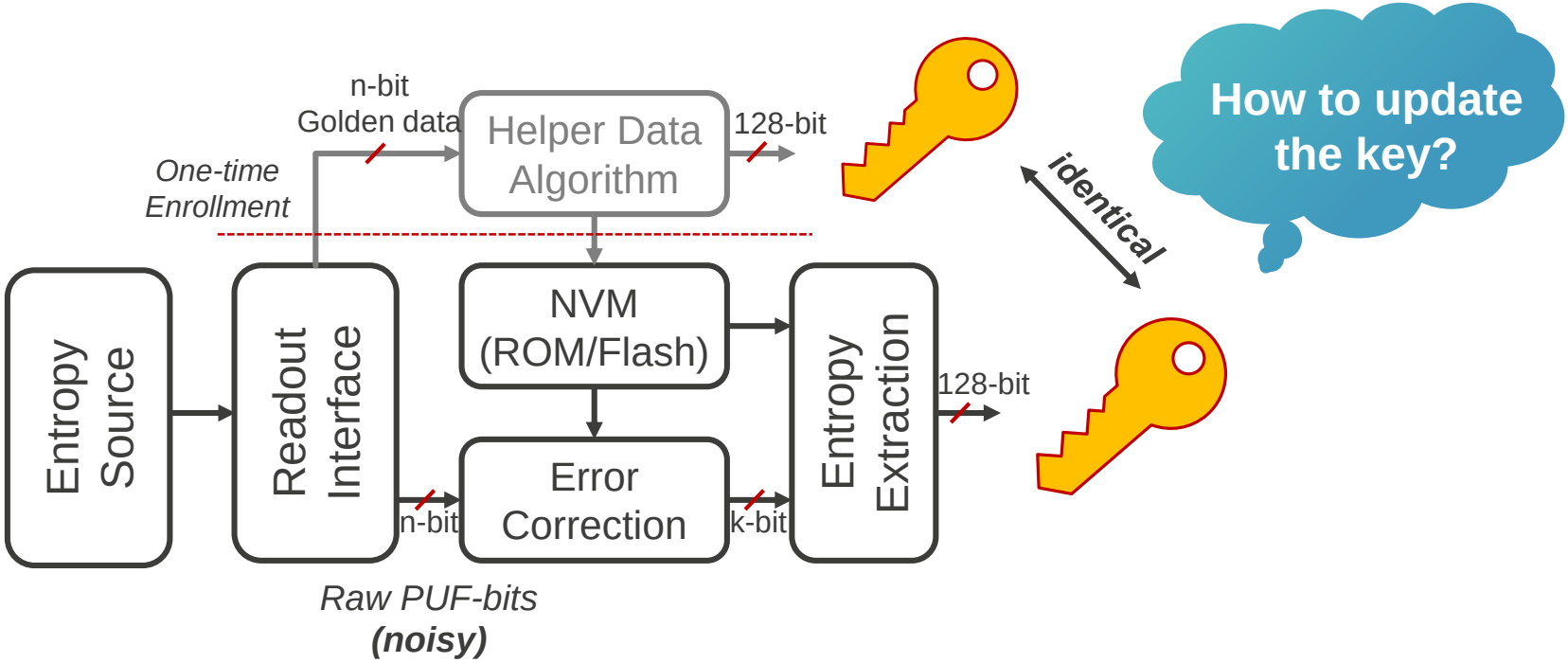
PUF-based key generation



PUF-based key generation

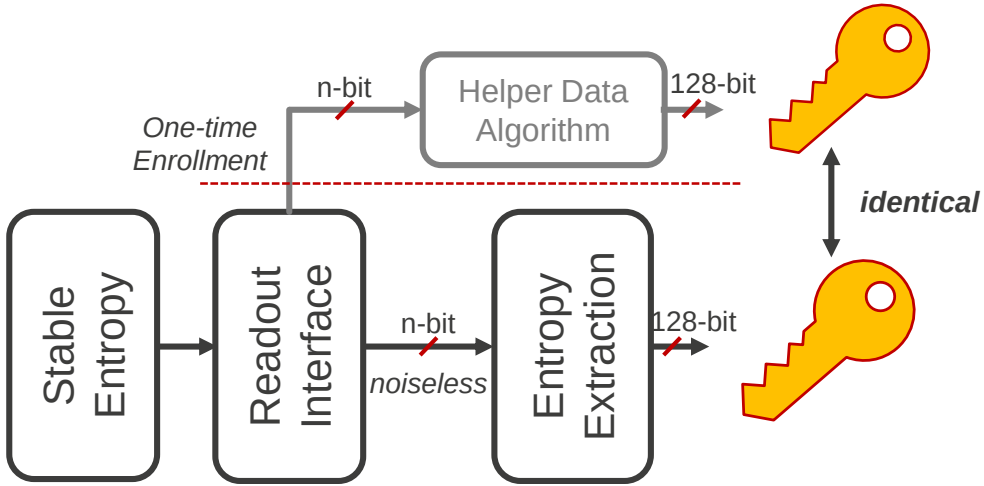


PUF-based key generation



Re-enrollment → new golden data → new helper data → **new key**

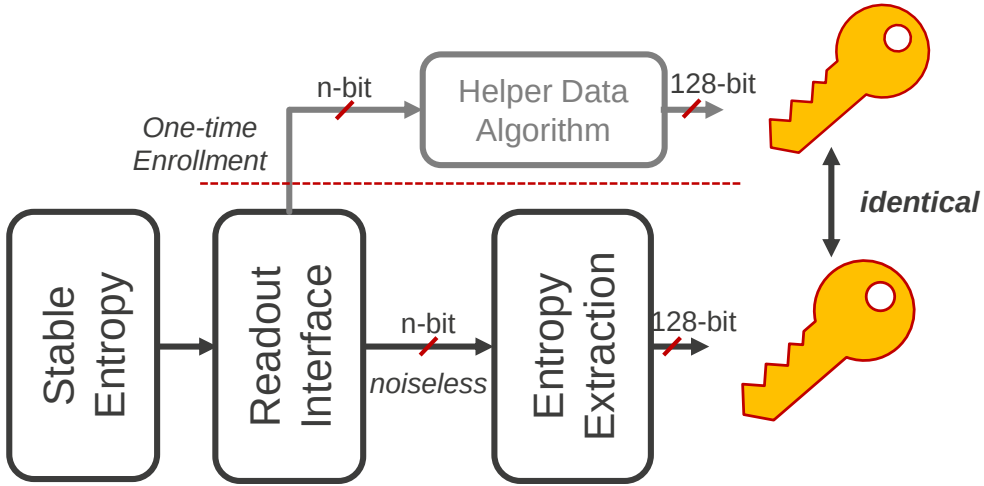
Why we need reconfigurable PUF?



PUF-based key generation with 100% stable entropy source

Re-enrollment → always the **same key**

Why we need reconfigurable PUF?

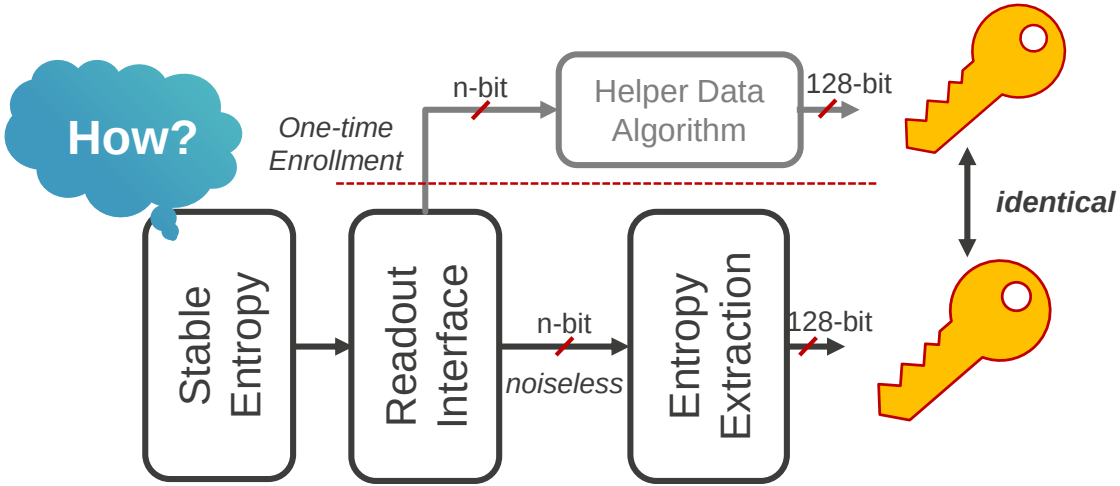


PUF-based key generation with 100% stable entropy source

Re-enrollment → always the **same key**

- Problems for re-enrollment:
  - Not suitable if readout is 100% stable, e.g. RRAM, MRAM or anti-fuse based PUFs
  - Relies on the unstable cells → difficult for security analysis

Why we need reconfigurable PUF?



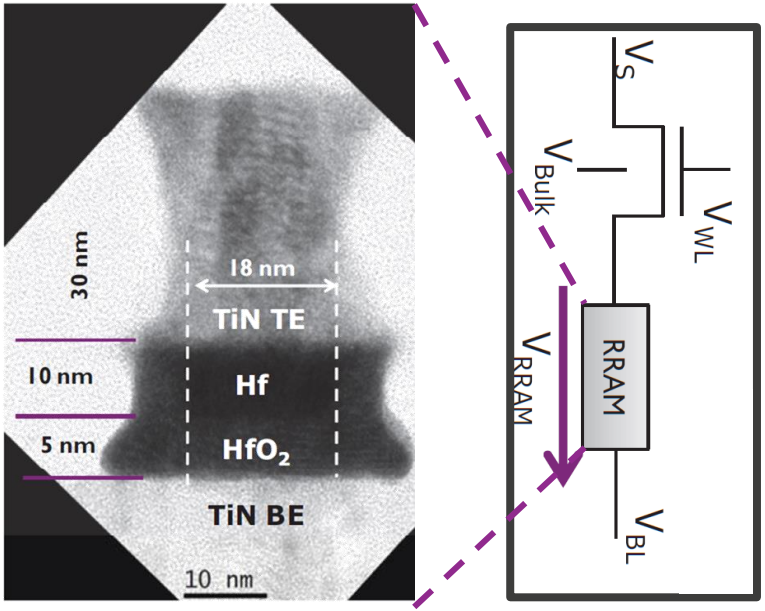
PUF-based key generation with 100% stable entropy source

Re-enrollment → always the **same key**

Need reconfiguration!

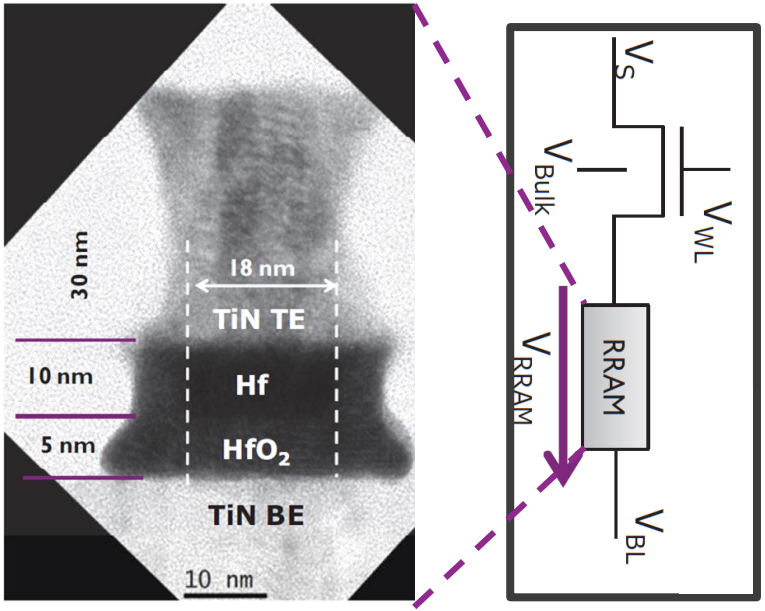
- Problems for re-enrollment:
  - Not suitable if readout is 100% stable, e.g. RRAM, MRAM or anti-fuse based PUFs
  - Relies on the unstable cells → difficult for security analysis

Operating the Oxygen-vacancy based RRAM

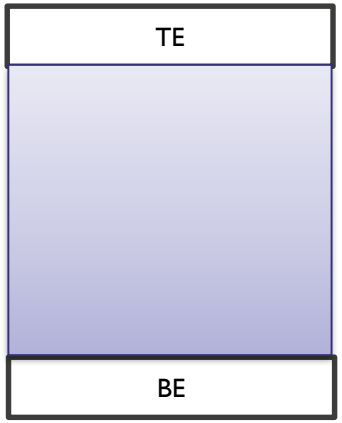


HfO_x RRAM

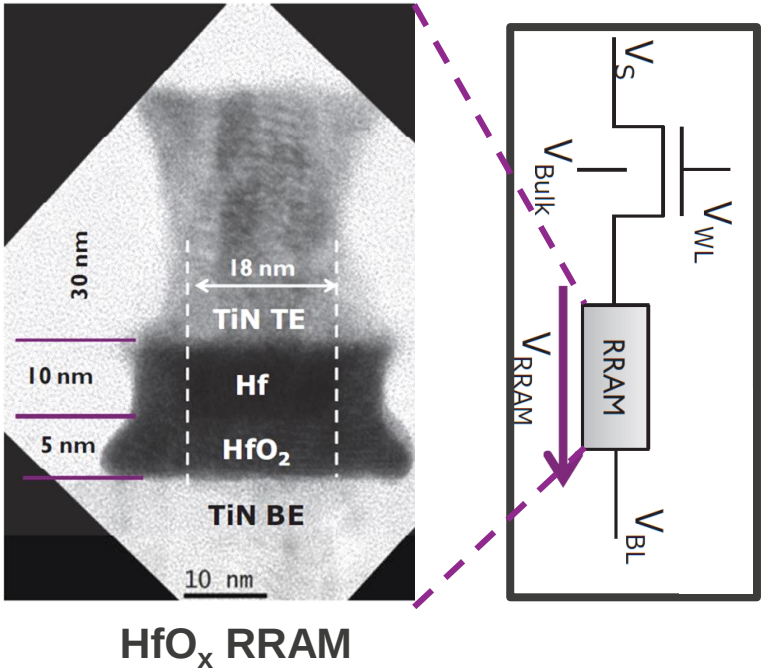
Operating the Oxygen-vacancy based RRAM



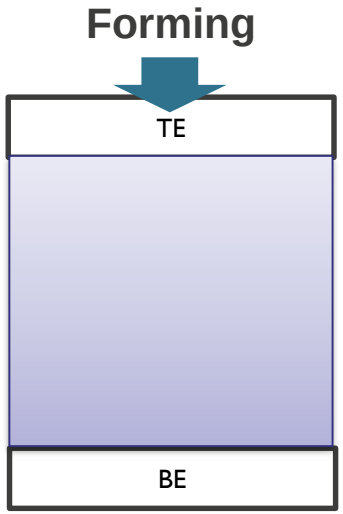
HfO_x RRAM



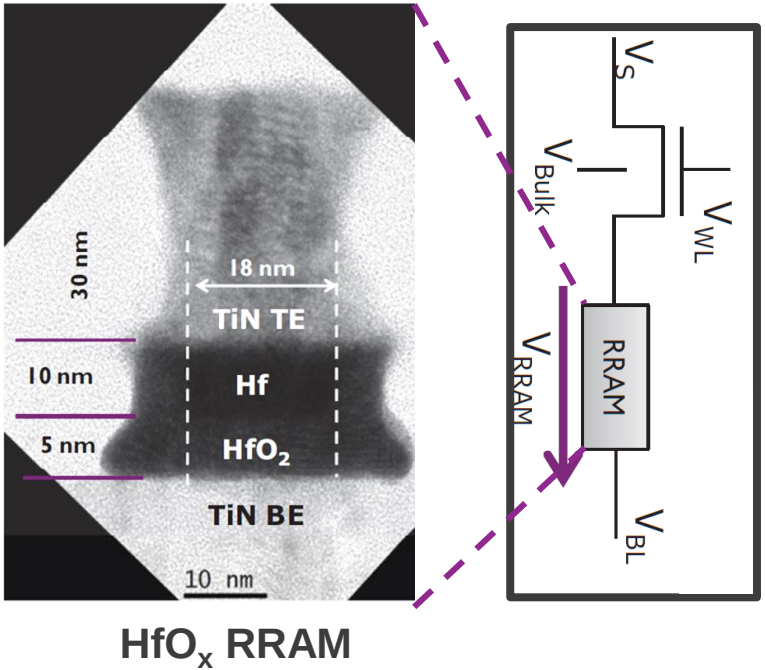
Operating the Oxygen-vacancy based RRAM



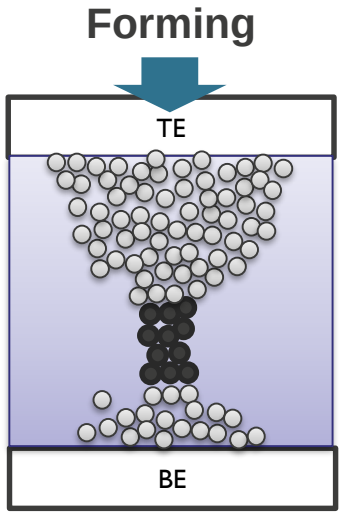
HfO_x RRAM



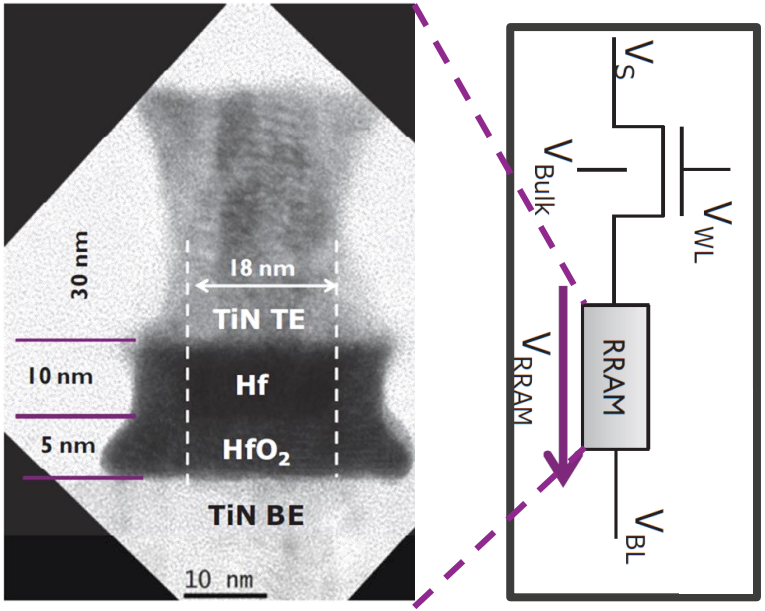
Operating the Oxygen-vacancy based RRAM



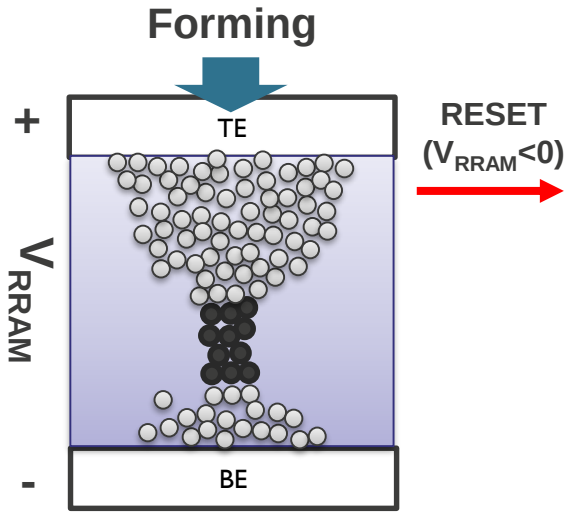
HfO_x RRAM



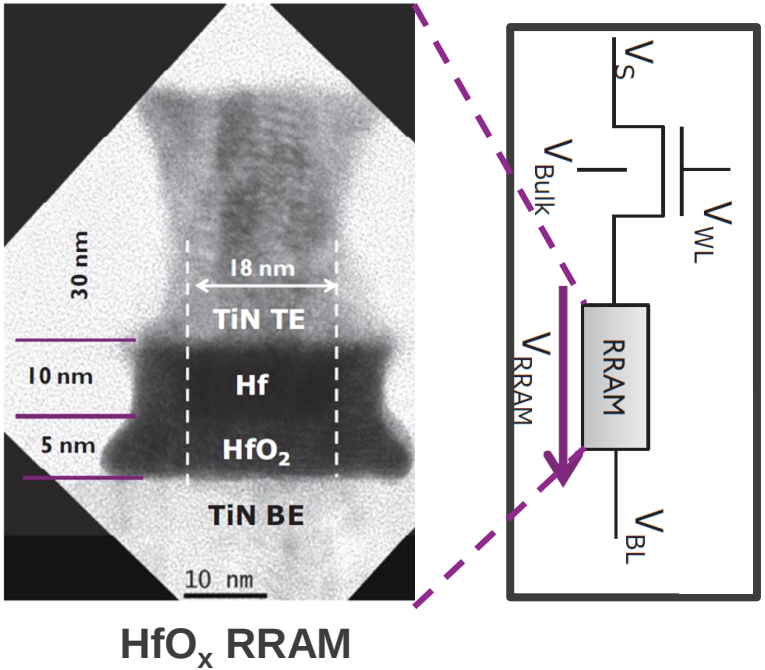
Operating the Oxygen-vacancy based RRAM



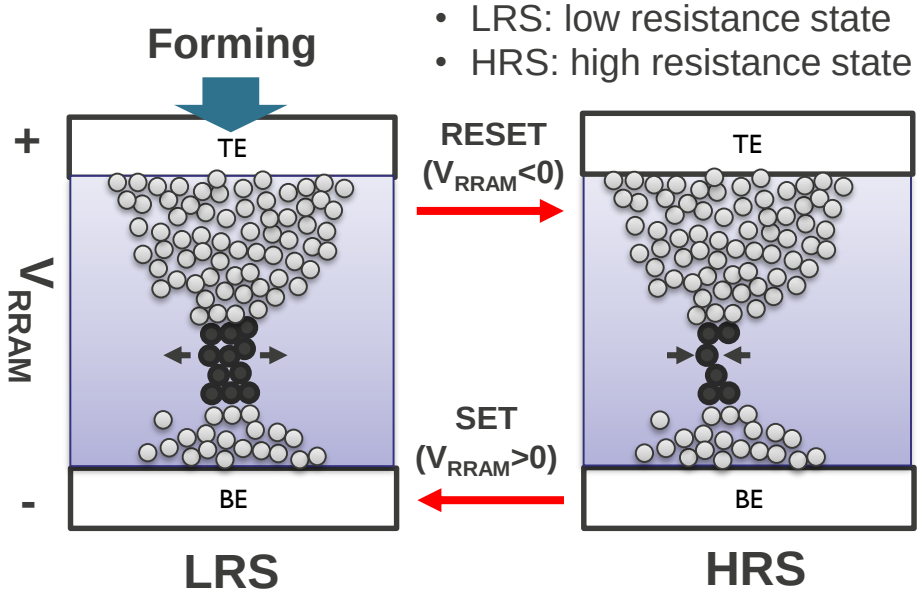
HfO_x RRAM



Operating the Oxygen-vacancy based RRAM

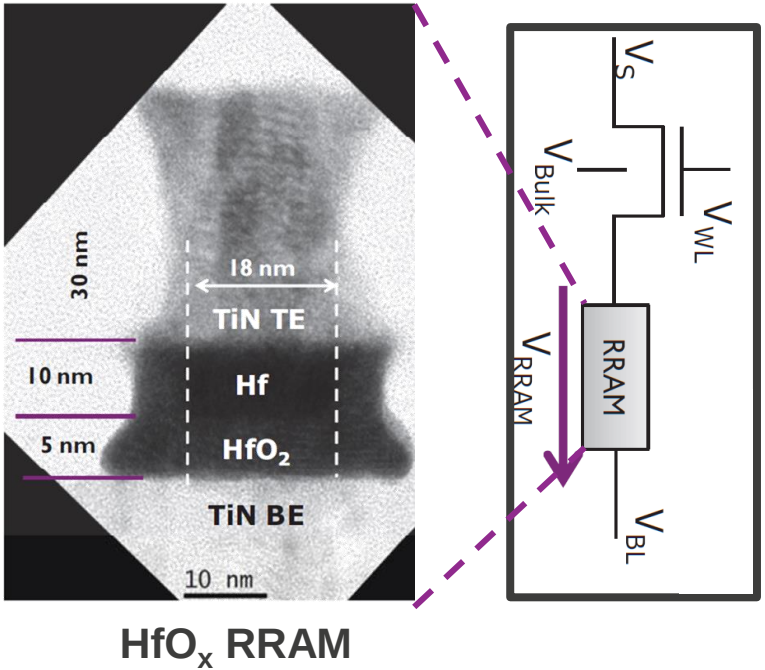


HfO_x RRAM

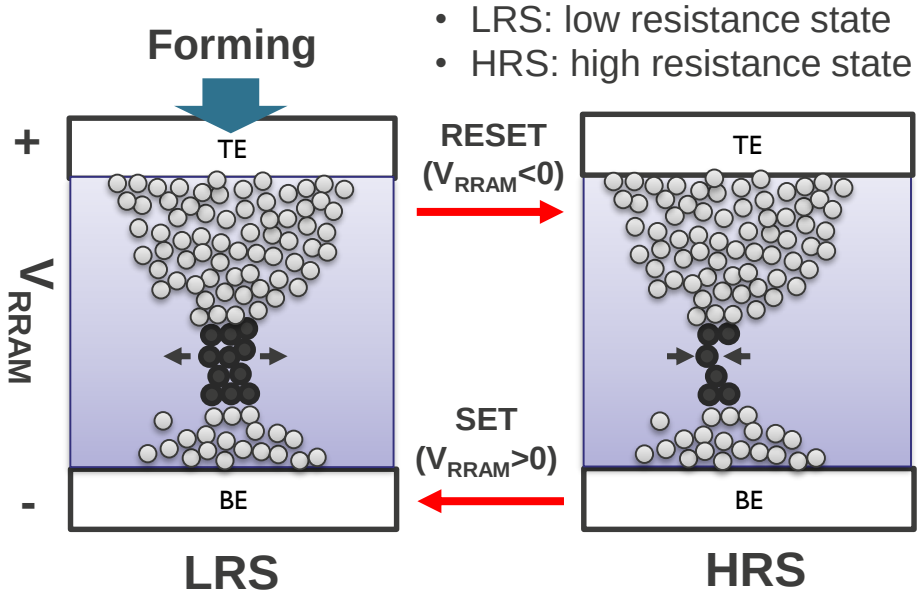


- LRS: low resistance state
- HRS: high resistance state

Operating the Oxygen-vacancy based RRAM



HfO_x RRAM

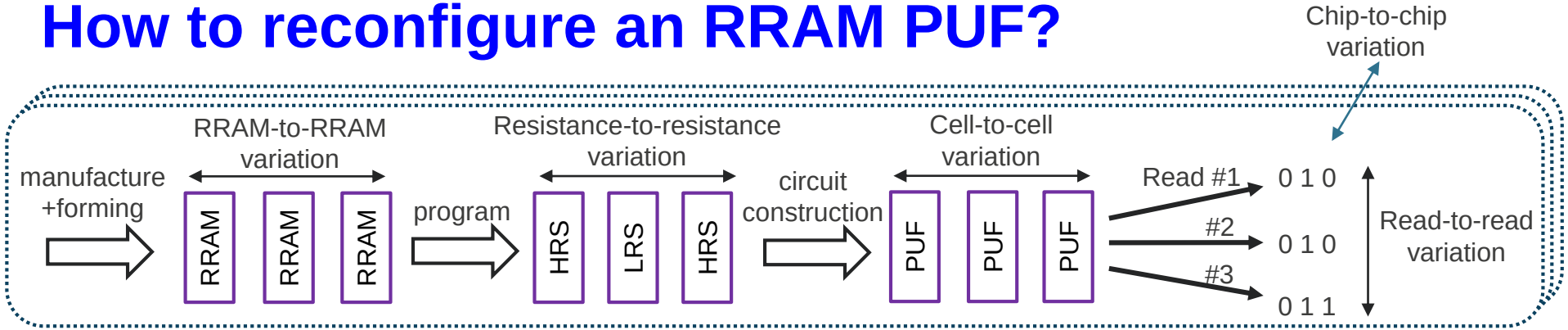


- LRS: low resistance state
- HRS: high resistance state

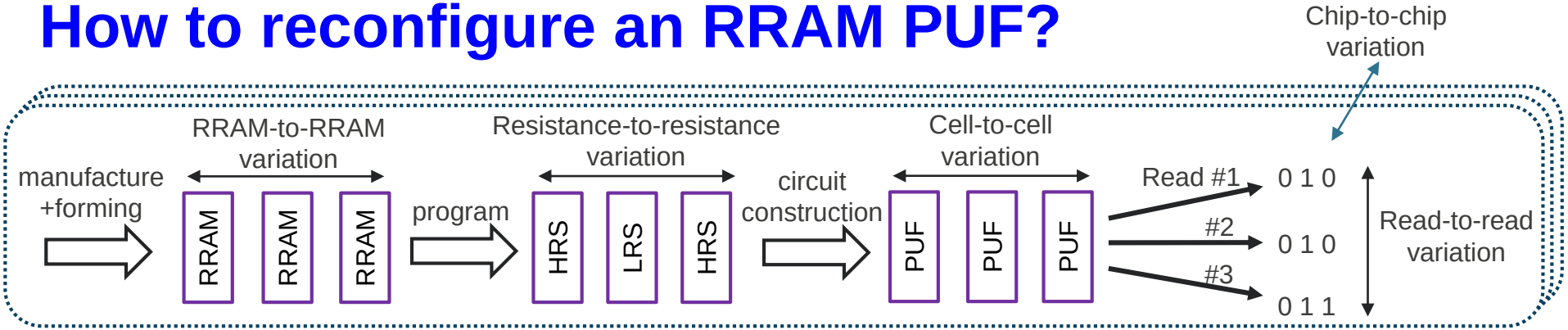
Unpredictable particle movement

→ Different ***shape*** and ***number*** for each set/reset cycle

How to reconfigure an RRAM PUF?



How to reconfigure an RRAM PUF?

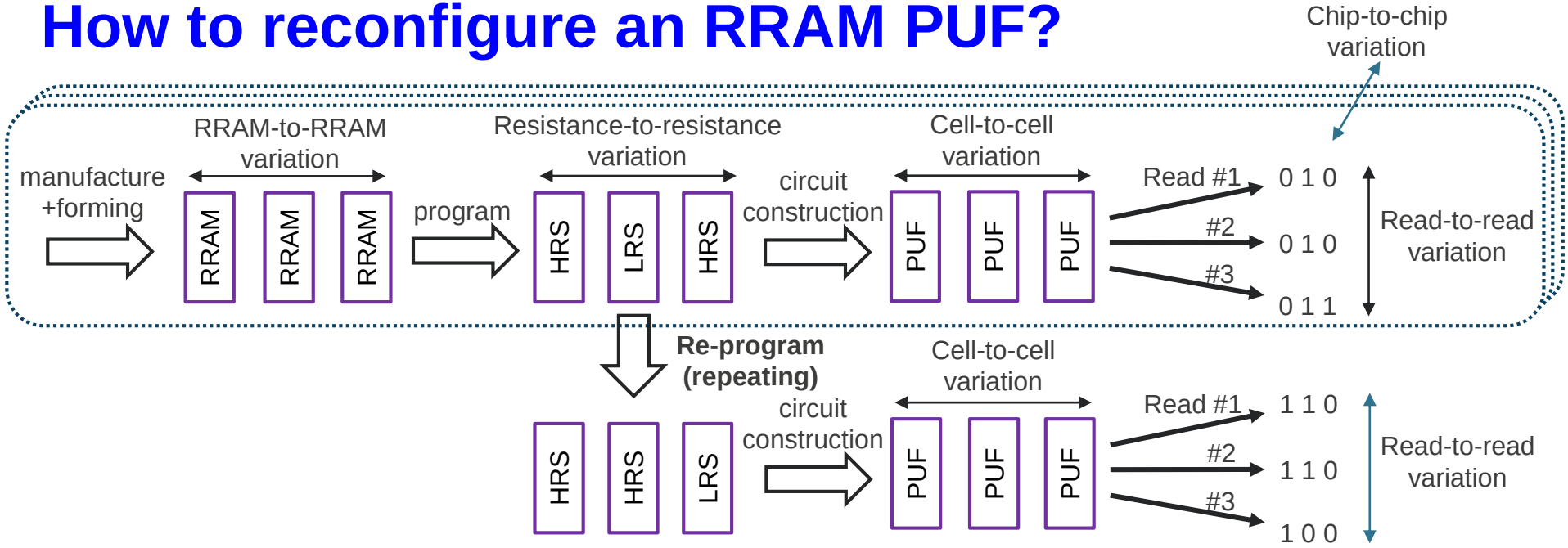


- Conventional PUFs: cell-to-cell, chip-to-chip and read-to-read variations
  - Not an issue for most RRAM PUFs [YKO+16, LWP+16, CPB14]

imec

COSIC

How to reconfigure an RRAM PUF?

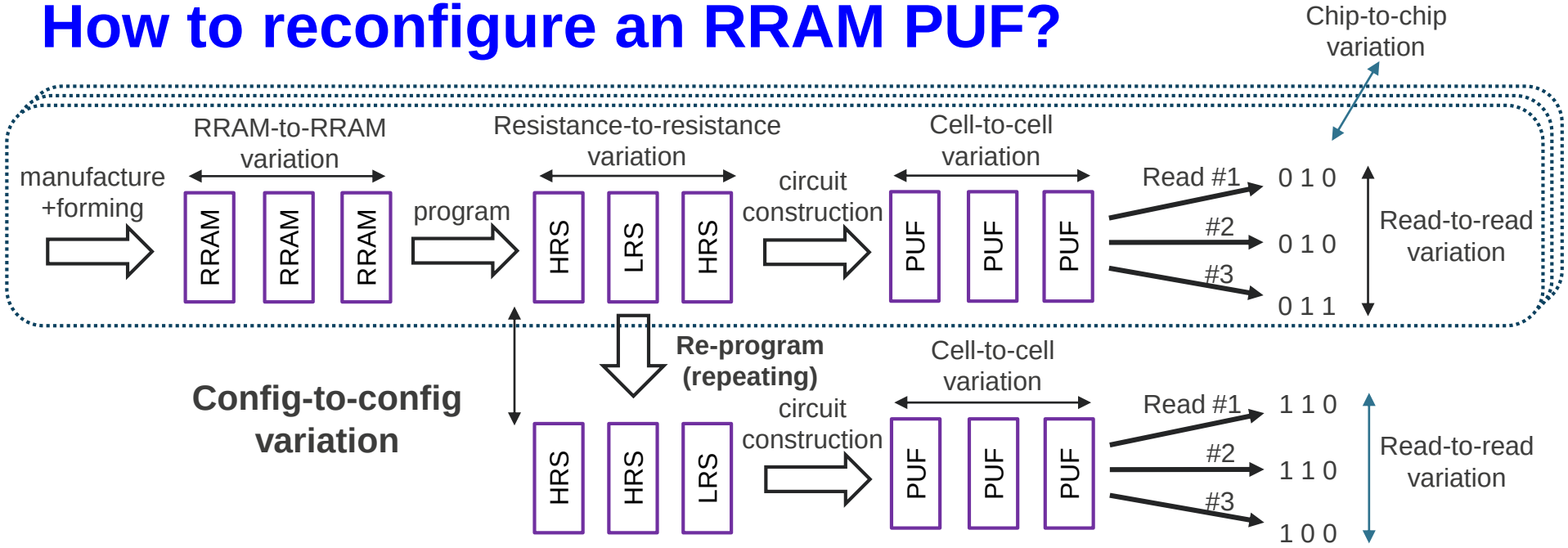


- Conventional PUFs: cell-to-cell, chip-to-chip and read-to-read variations
  - Not an issue for most RRAM PUFs [YKO+16, LWP+16, CPB14]

imec

COSIC

How to reconfigure an RRAM PUF?

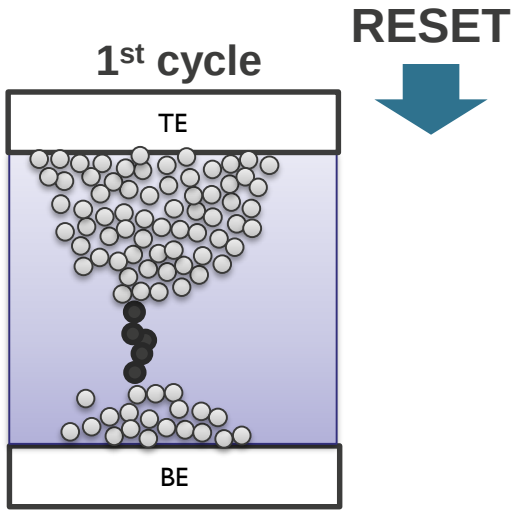


- Conventional PUFs: cell-to-cell, chip-to-chip and read-to-read variations
  - Not an issue for most RRAM PUFs [YKO+16, LWP+16, CPB14]
- Focus: **Configuration-to-configuration variation**

imec

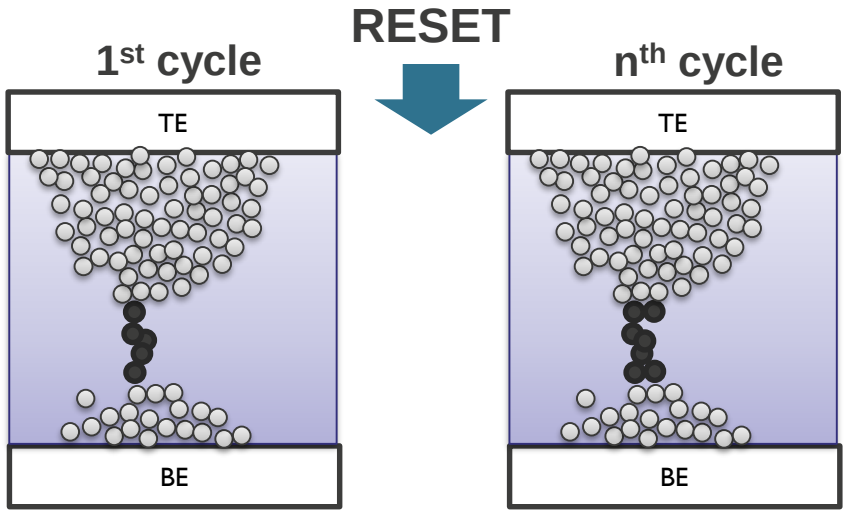
COSIC

Is there sufficient config-to-config variation?



Less conductive vacancies → **higher R**

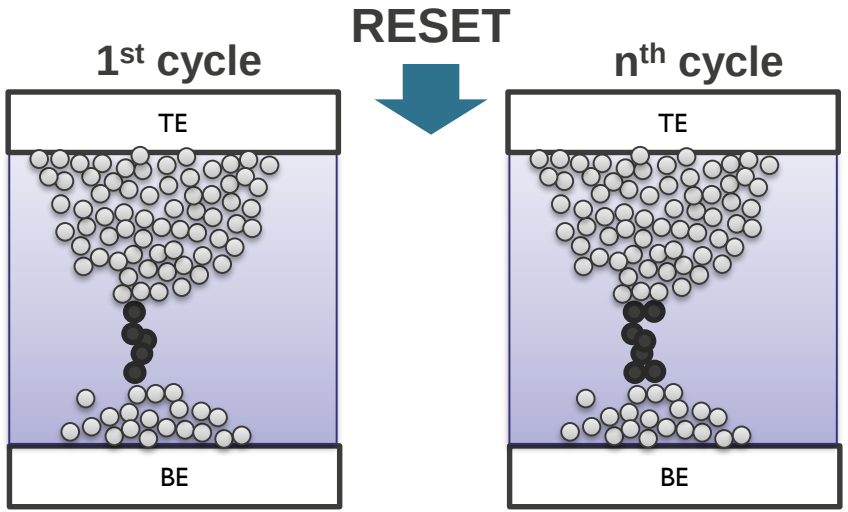
Is there sufficient config-to-config variation?



Less conductive vacancies → **higher R**

More conductive vacancies → **lower R**

Is there sufficient config-to-config variation?



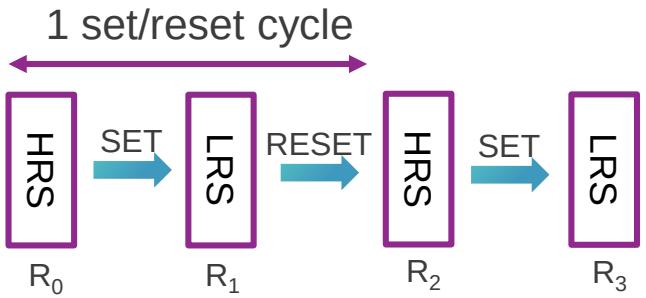
HRS

Less conductive vacancies → **higher R**

HRS

More conductive vacancies → **lower R**

Randomness

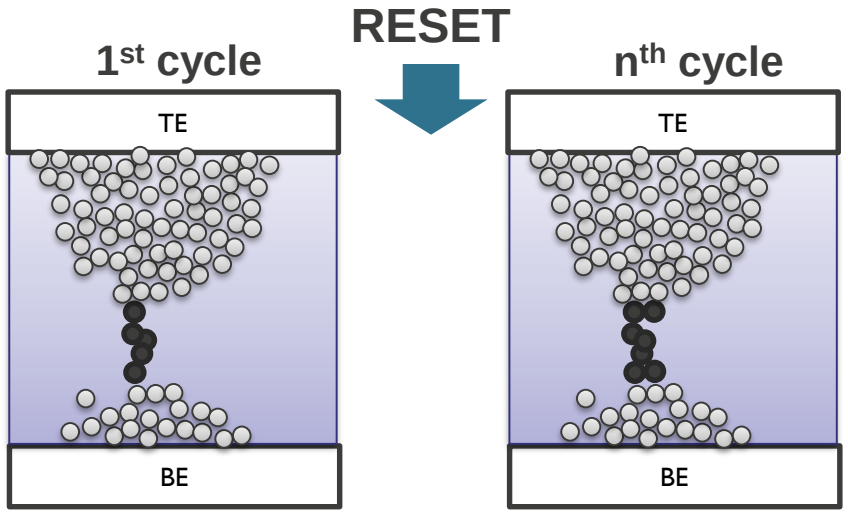


$R_0 \neq R_2$ and **$R_1 \neq R_3$**
under the same SET/RESET conditions

imec

COSIC

Is there sufficient config-to-config variation?

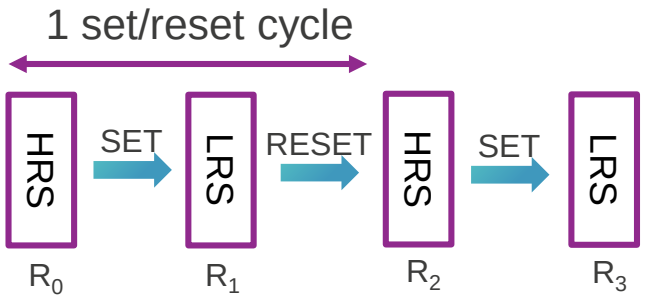


HRS

Less conductive vacancies → **higher R**

HRS

More conductive vacancies → **lower R**



$R_0 \neq R_2$ and **$R_1 \neq R_3$**
under the same SET/RESET conditions

Statistics and modeling

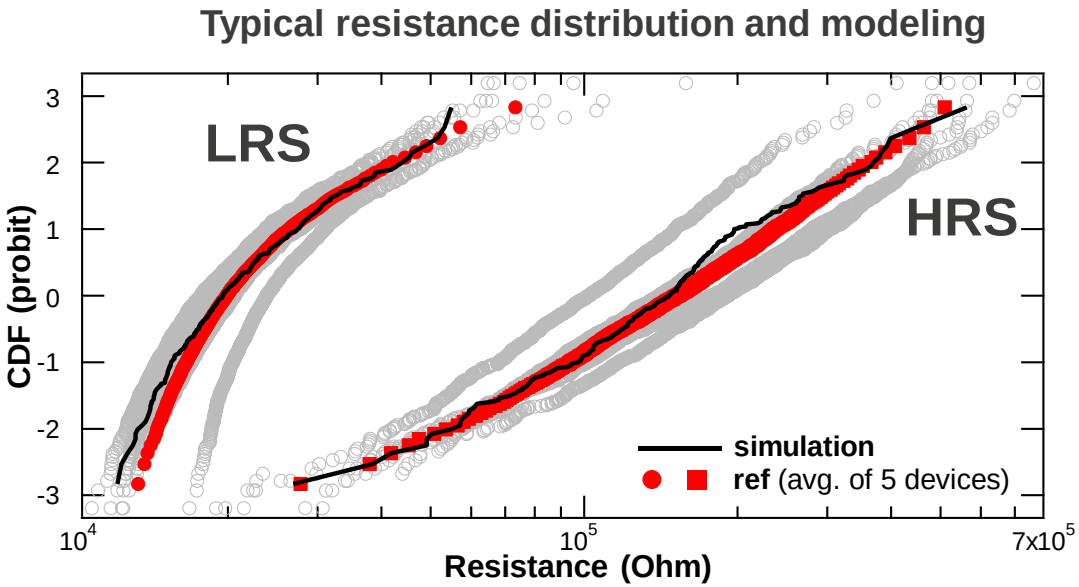
Randomness

analysis

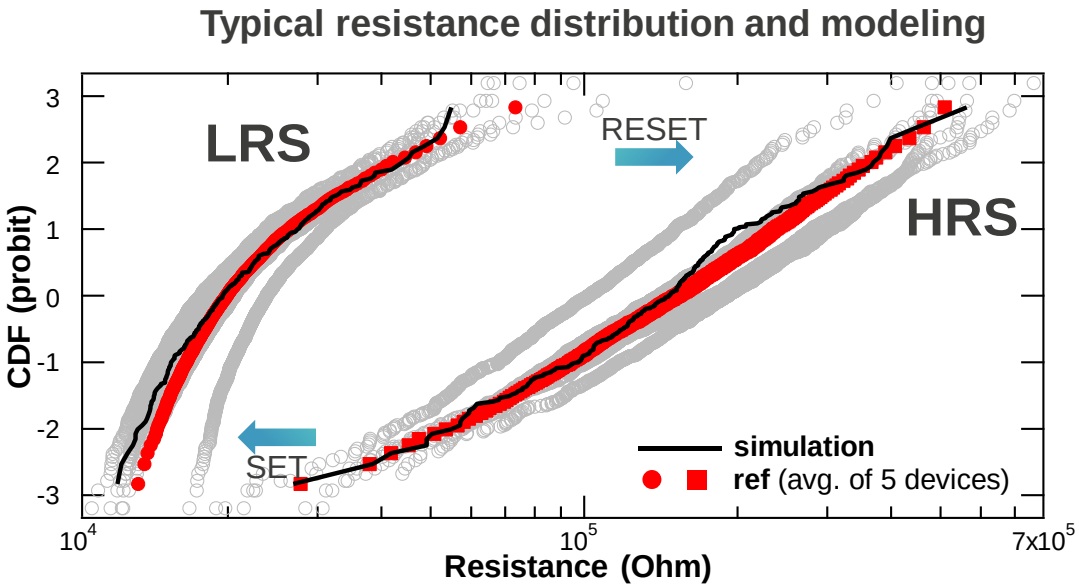
Outline

- Introduction
- RRAM PUF implementations
- Non-ideal reconfigurability
- Conclusion

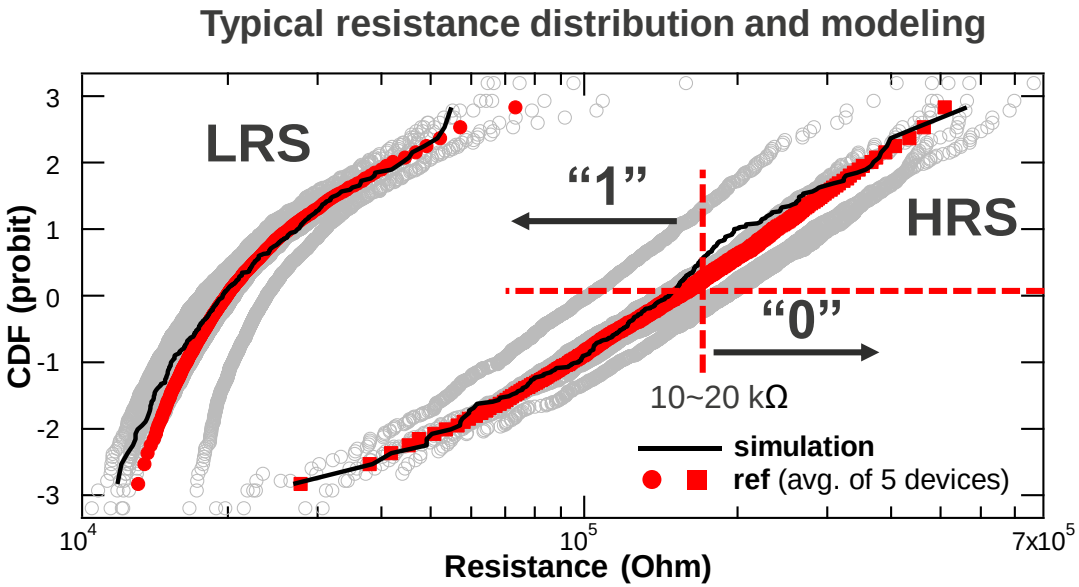
Resistance based RRAM PUF implementations

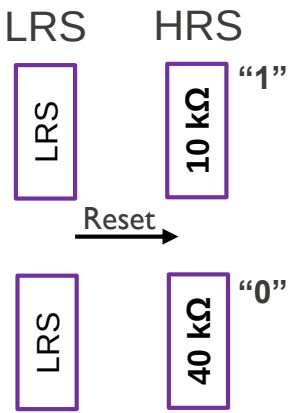


Resistance based RRAM PUF implementations



Resistance based RRAM PUF implementations

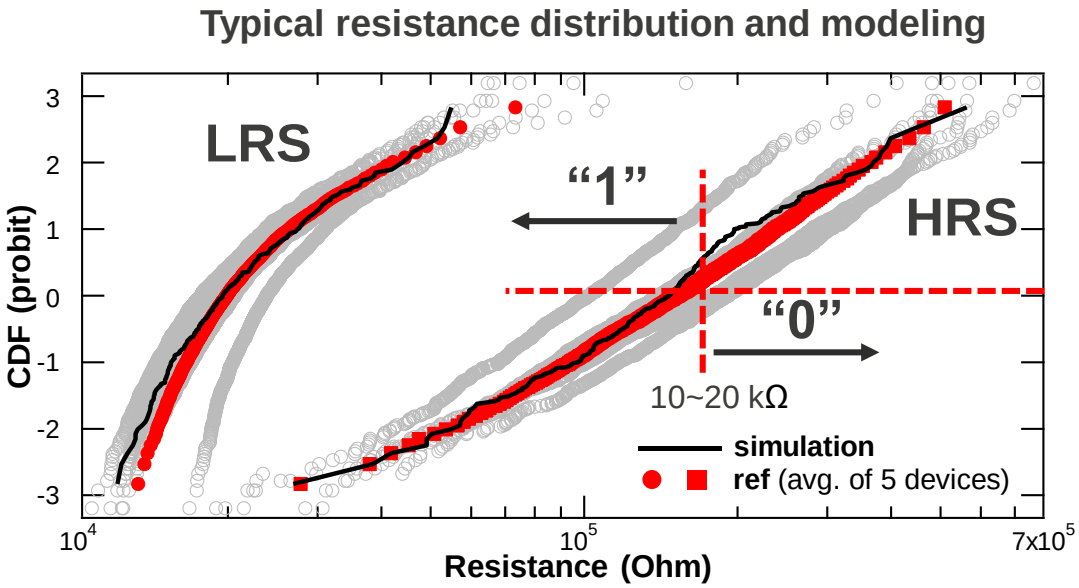


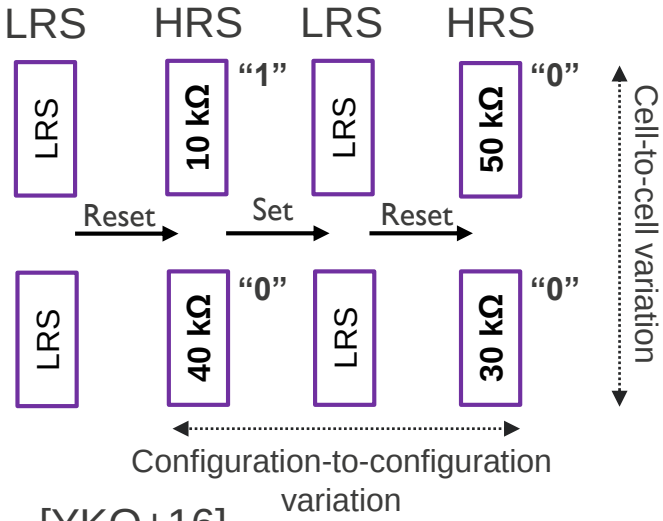


[YKO+16]

- "0" and "1" bits determined based on resistance threshold of LRS or HRS

Resistance based RRAM PUF implementations

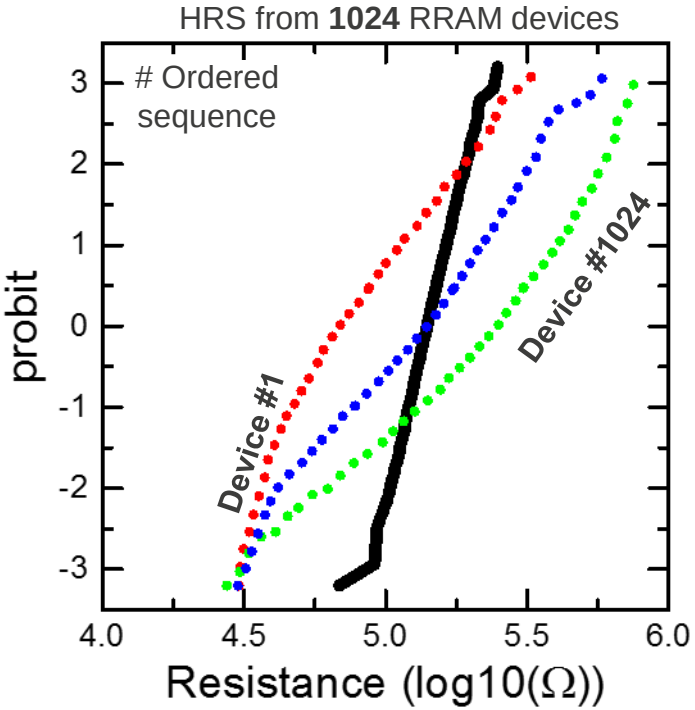




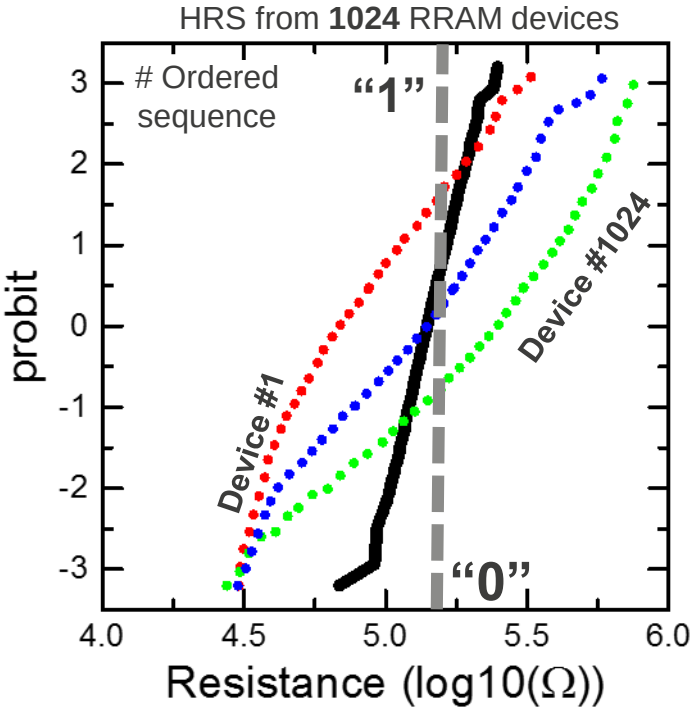
[YKO+16]

- "0" and "1" bits determined based on resistance threshold of LRS or HRS
- ***Reconfiguration*** **:** perform 1 set/reset cycle

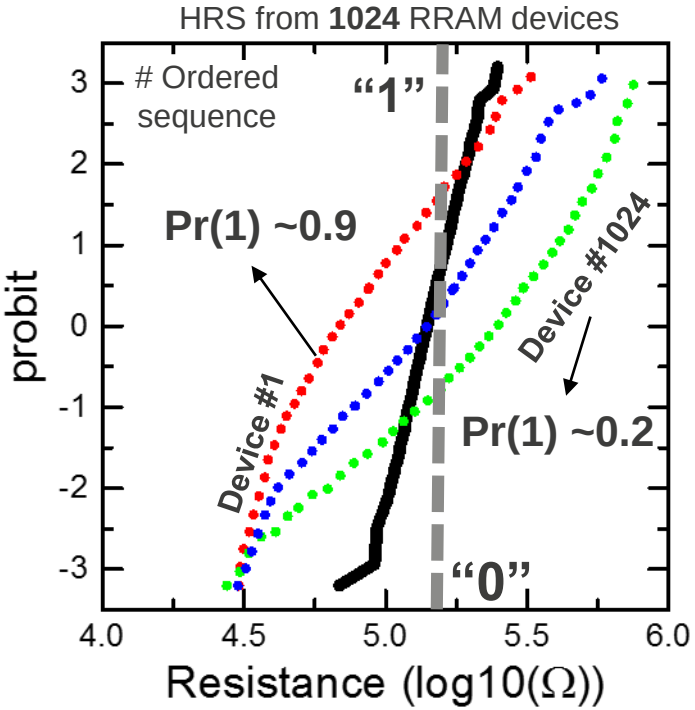
RRAMs are unique in practice



RRAMs are unique in practice

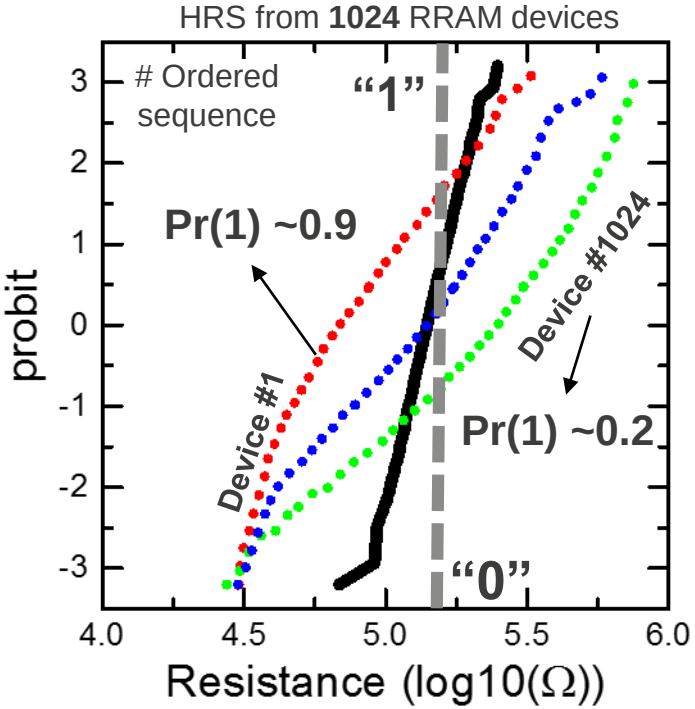


RRAMs are unique in practice

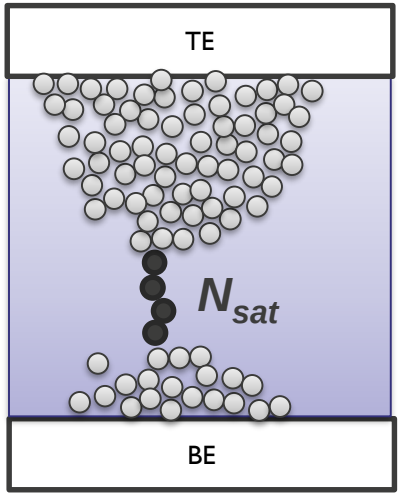


- **Device dependent bias exists**

RRAMs are unique in practice



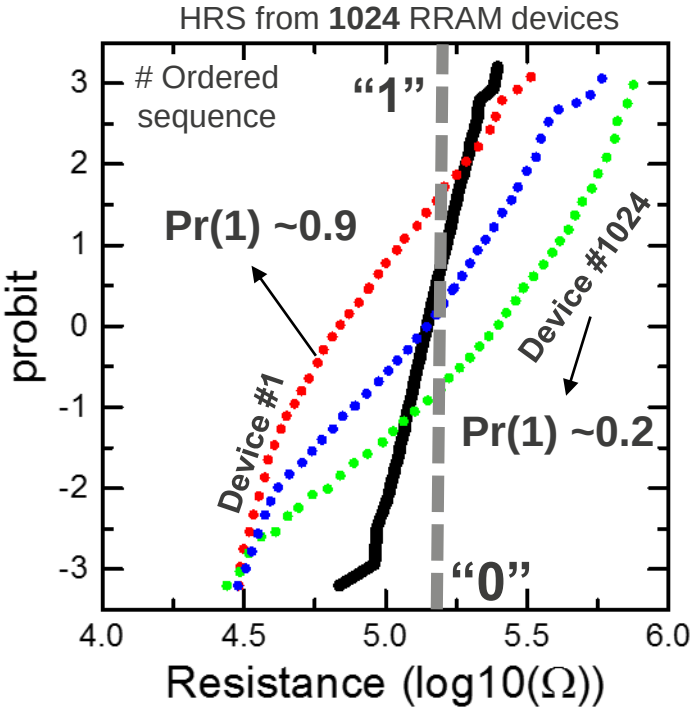
N_{sat} : minimum number of vacancies



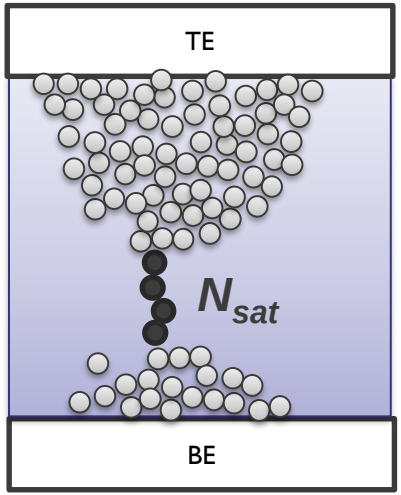
HRS

- **Device dependent bias exists**

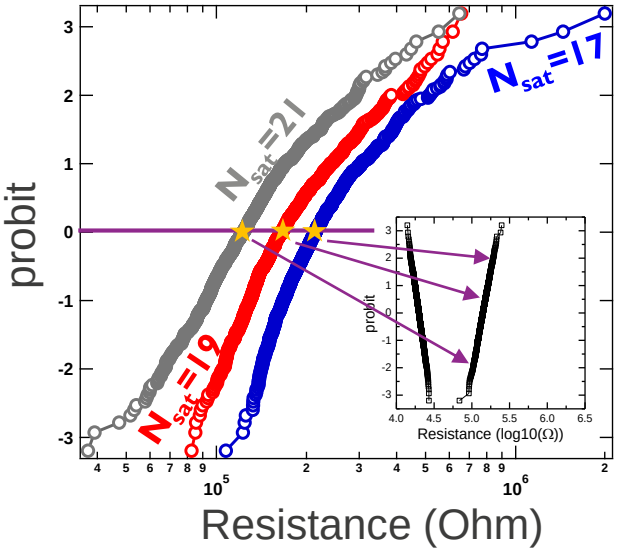
RRAMs are unique in practice



N_{sat} : minimum number of vacancies

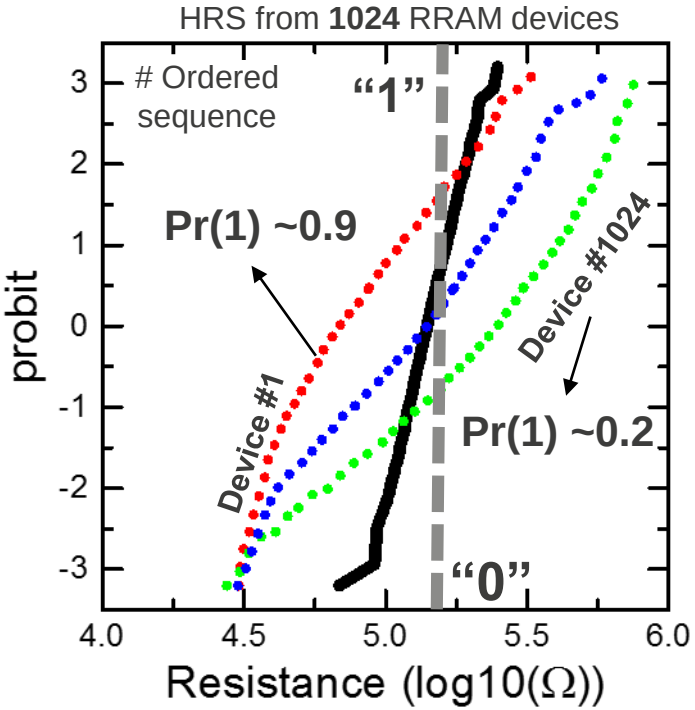


Reproduced

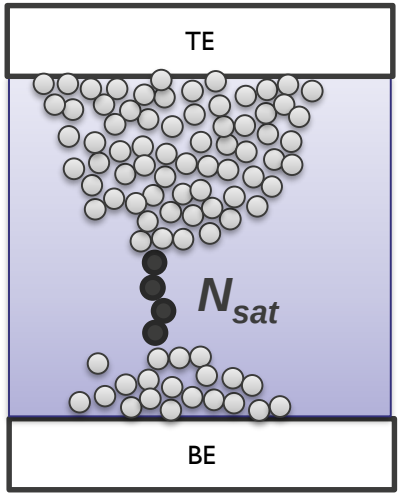


- **Device dependent bias exists**

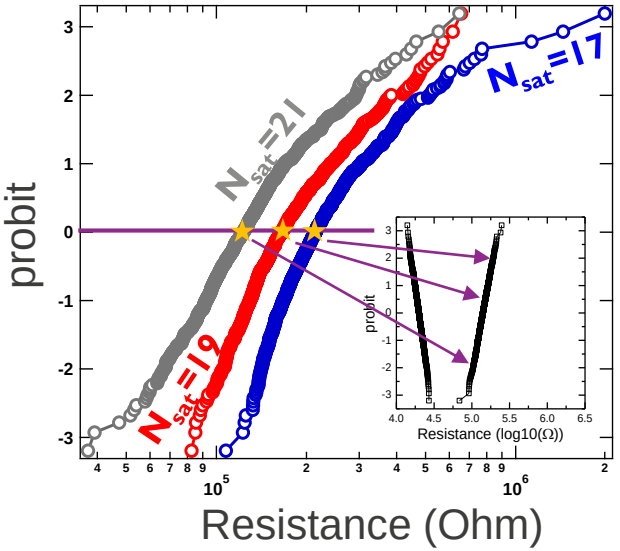
RRAMs are unique in practice



N_{sat} : minimum number of vacancies

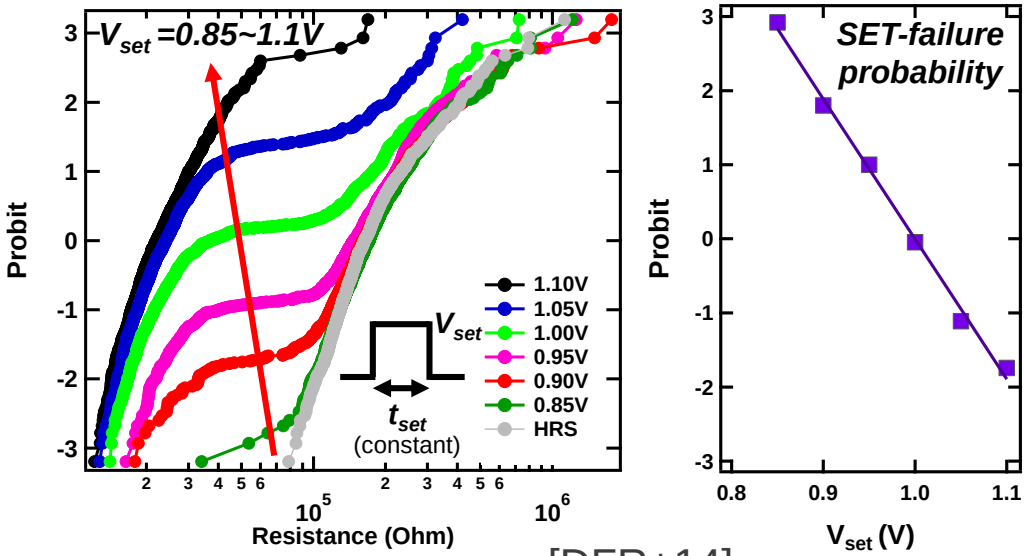


Reproduced



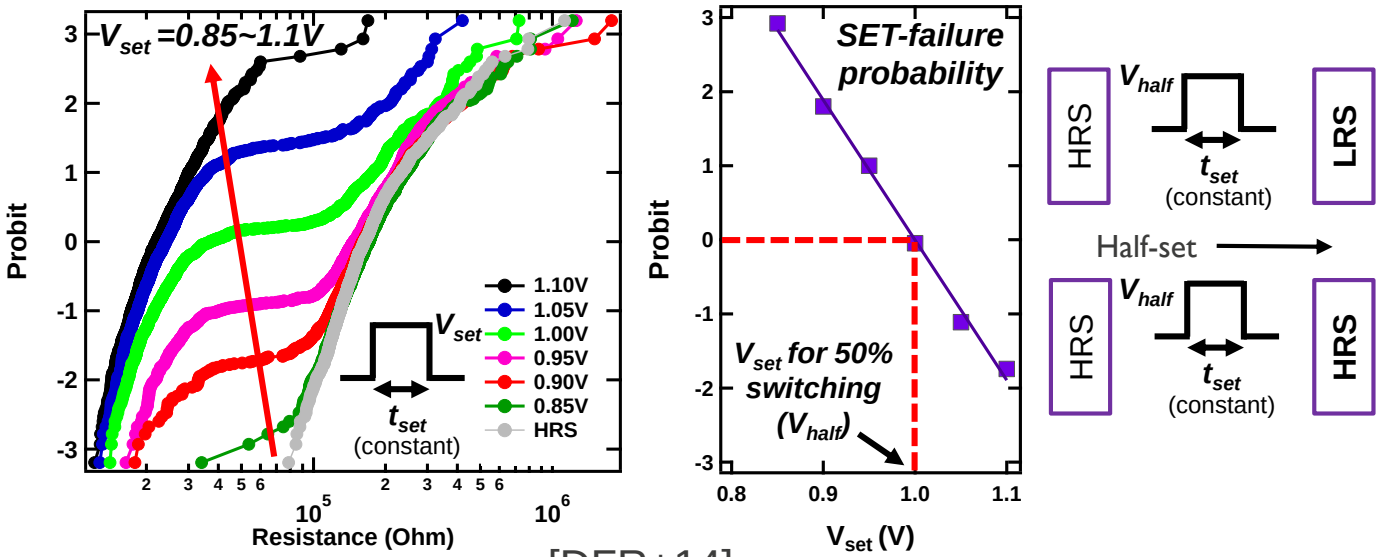
- **Device dependent bias exists**
- Usually overlooked since the distribution is narrower

Resistance splitting using *half-SET*



[DFR+14]

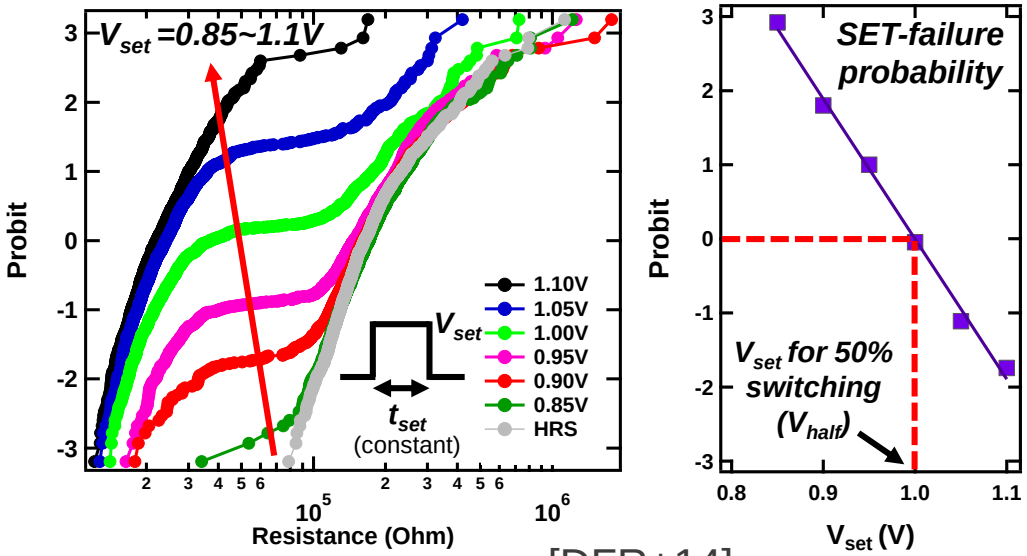
Resistance splitting using *half-SET*



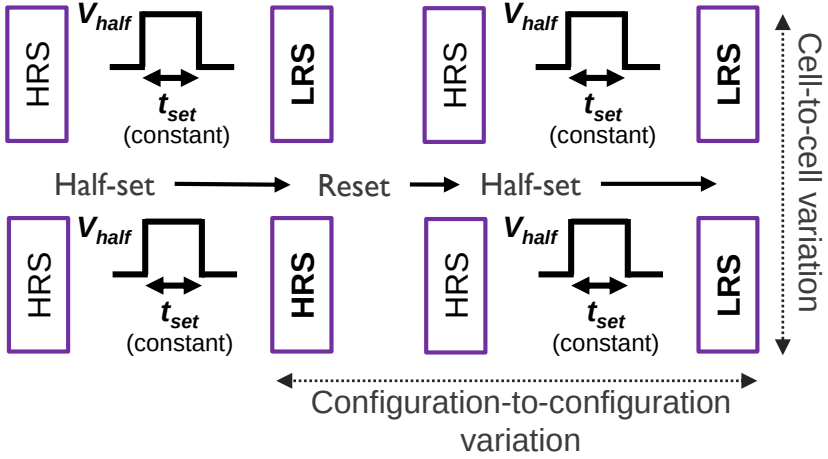
[DFR+14]

- HRS → “0” , LRS → “1”

Resistance splitting using *half-SET*



[DFR+14]

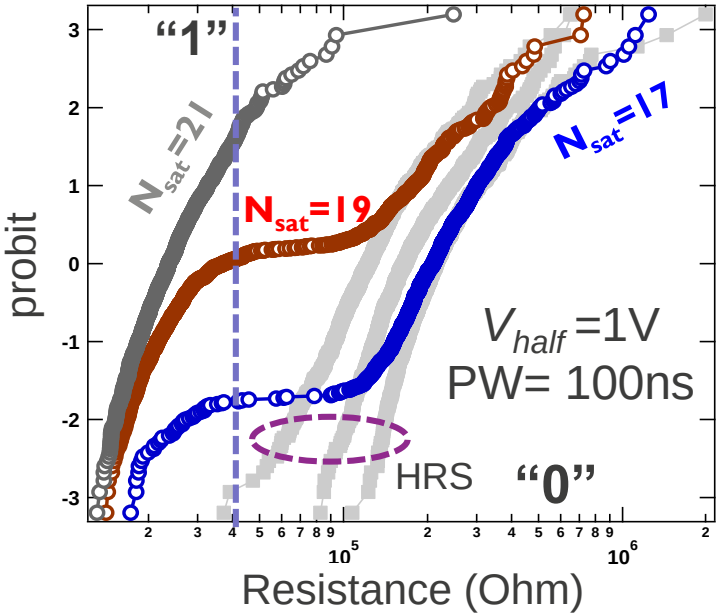


- HRS → "0" , LRS → "1"
- ***Reconfiguration:*** perform 1 reset and half-set cycle

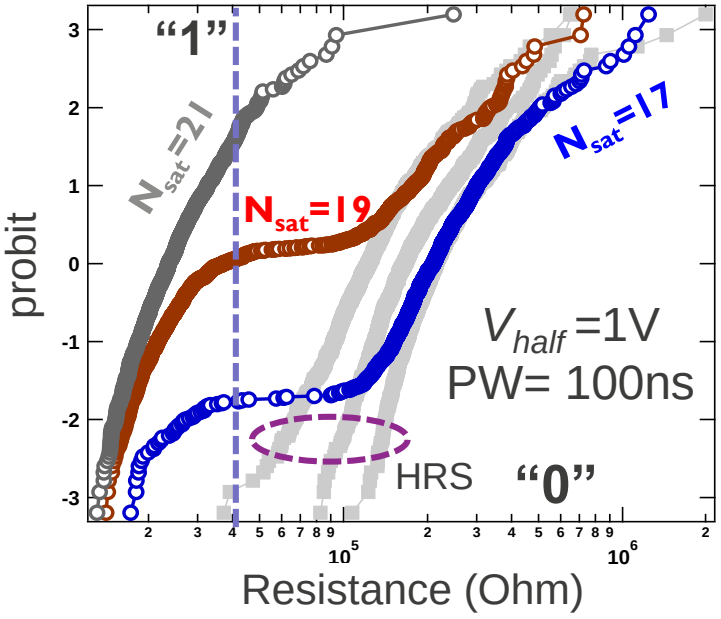
imec

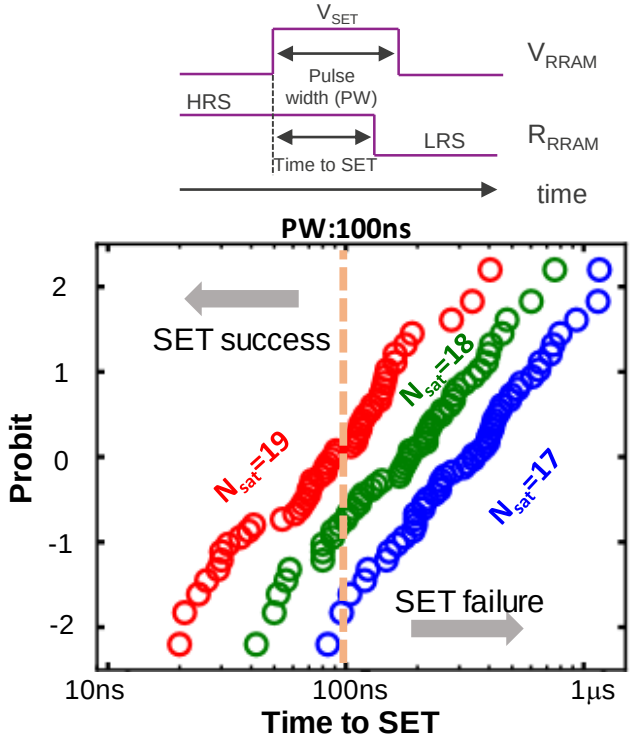
COSIC

Same problem exists for this method



Same problem exists for this method





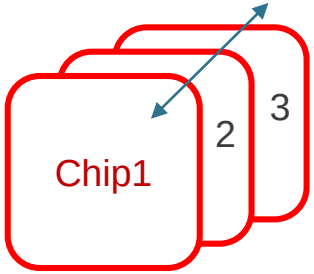
- Needs different time to SET different RRAMs

Outline

- Introduction
- RRAM PUF implementations
- Non-ideal reconfigurability
- Conclusion

Uniqueness between configurations is not ideal

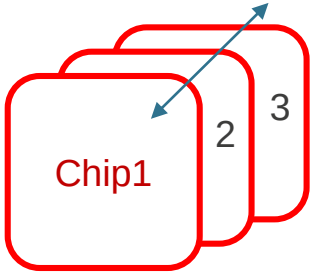
Inter-chip hamming distance



Ideally ~0.5 (normalized)

Uniqueness between configurations is not ideal

Inter-chip hamming distance



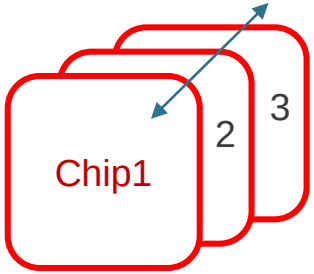
Ideally ~0.5 (normalized)

Inter-configuration hamming distance

- Target: as good as inter-chip HD

Uniqueness between configurations is not ideal

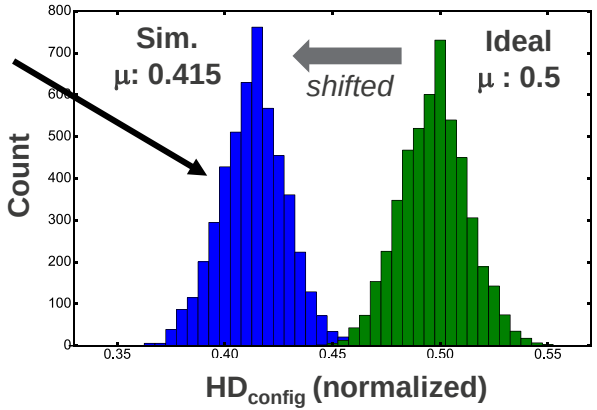
Inter-chip hamming distance



Ideally ~0.5 (normalized)

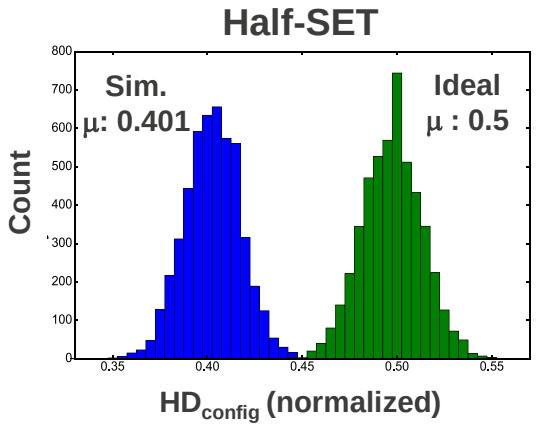
Inter-configuration hamming distance

RRAM PUF based on Resistance Threshold

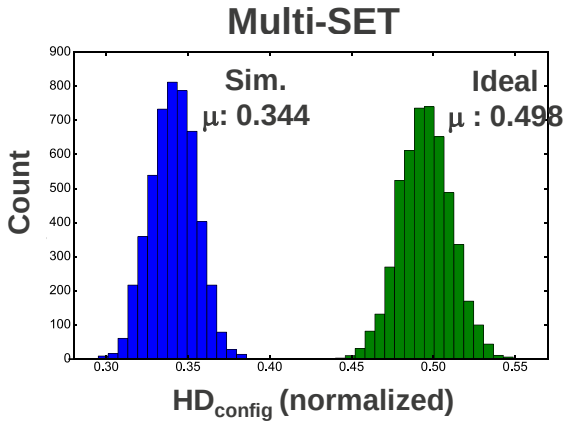


- Target: as good as inter-chip HD
- **Shifted HD_{config} shows the non-ideal reconfigurability**

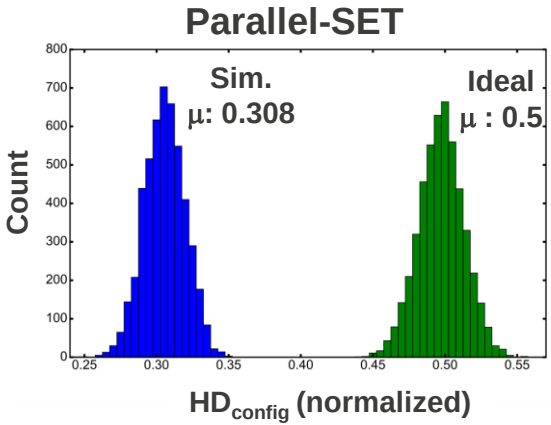
Non-ideal uniqueness of other implementations



[DFR+14]



[LHSB10]



[BAC+16]

- All implementations show clear uniqueness degradation between configurations
- Level of degradation varies for different PUF implementations

Outline

- Introduction
- RRAM PUF implementations
- Non-ideal reconfigurability
- Conclusion

Conclusion

- True reconfigurability is not achievable for RRAM PUFs
- The impact on uniqueness cannot be neglected

THANKS FOR YOUR ATTENTION!

imec
embracing a better life

COSIC