A Zero-cost Approach to Detect Recycled SoC Chips Using Embedded SRAM

Zimu Guo, Md. Tauhidur Rahman, Mark M. Tehranipoor and **Domenic Forte**
ECE Department, University of Florida

Motivations

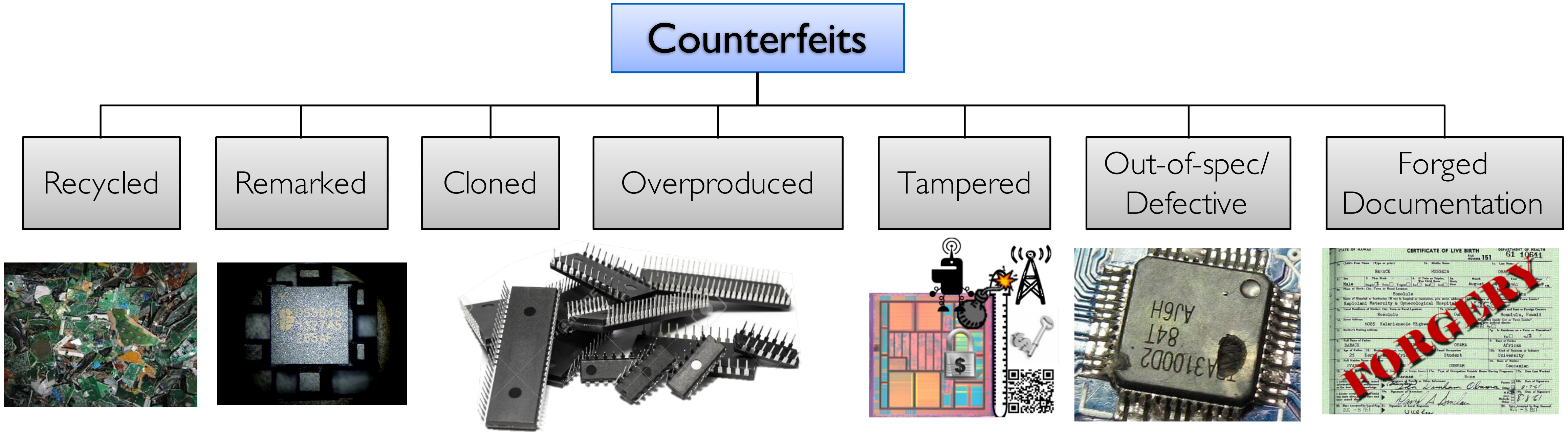
Impact of counterfeit ICs.

- The Government and Industry Data Exchange Program (GIDEP) has seen a **six-fold increase** in reported counterfeit ICs since 2006.
- Information Handling Services Inc. (IHS) have pointed out that reports of counterfeit parts have increased by **25% every year** since 2001.
- Counterfeits result in substantial economic losses to the electronics industry, reportedly as high as **hundreds of billions**.
- Counterfeit parts decrease the overall **system reliability**.
- Manufactories **lose reputation**.

Current difficulties

- No one-size-fits-all solutions.
- Detection requires additional circuitries.

Counterfeits types and countermeasures



Counterfeits

Recycled

Remarked

Cloned

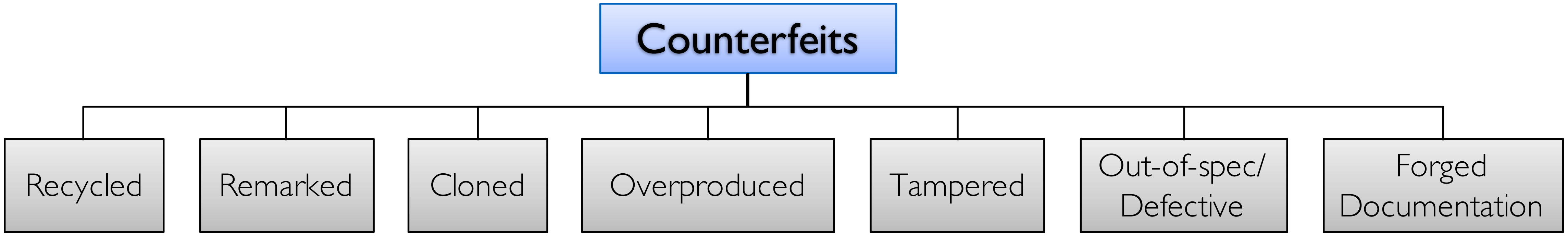
Overproduced

Tampered

Out-of-spec/ Defective

Forged Documentation

Counterfeits types and countermeasures


Counterfeits

Recycled

Remarked

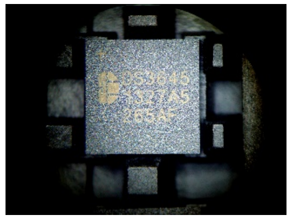
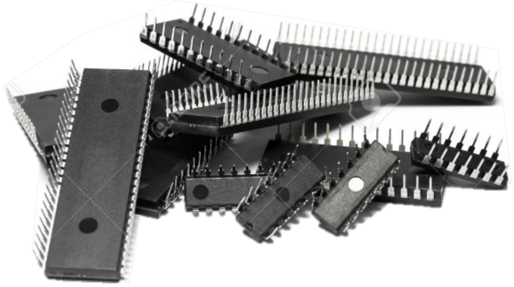
Cloned

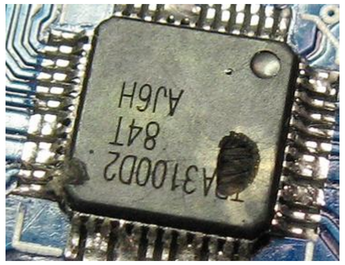
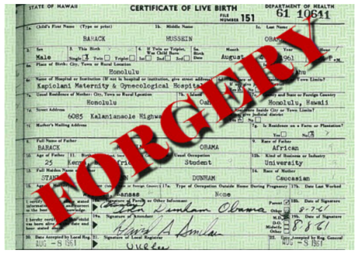
Overproduced

Tampered

Out-of-spec/ Defective

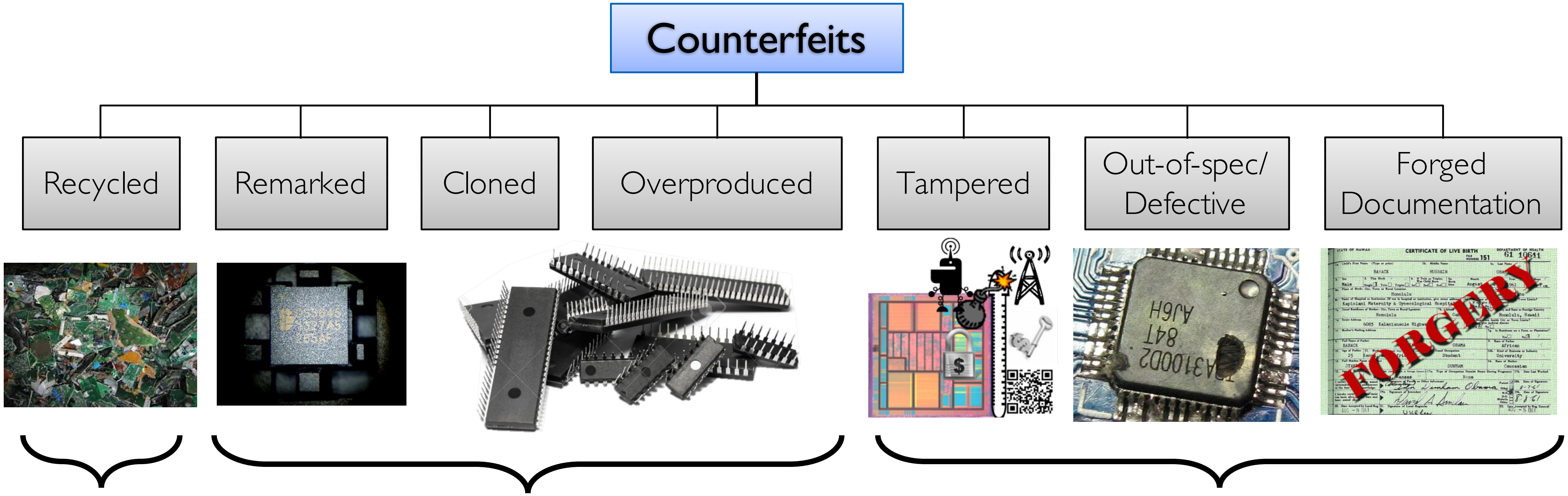
Forged Documentation

Detected by the techniques such as secure split-test (SST), electronic circuit ID (ECID), etc.

Counterfeits types and countermeasures

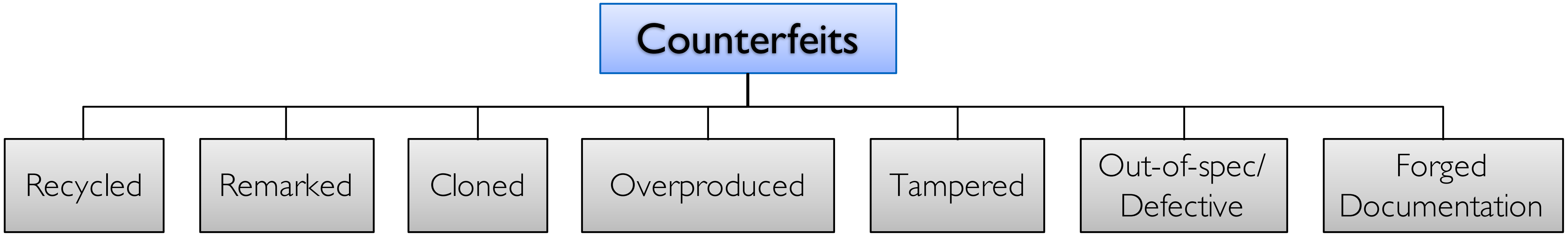


Detected by CDIR sensors

Detected by PUF

Detected by the techniques such as secure split-test (SST), electronic circuit ID (ECID), etc.

Counterfeits types and countermeasures



Counterfeits

Recycled

Remarked

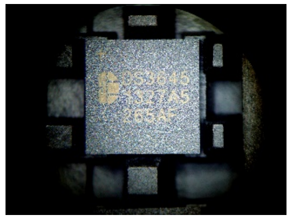
Cloned

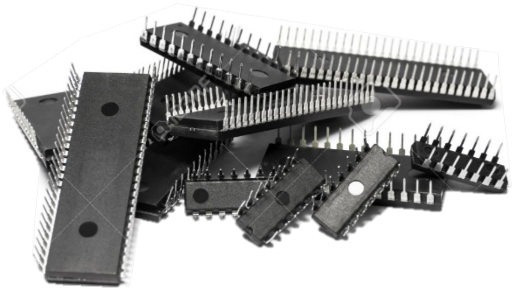
Overproduced

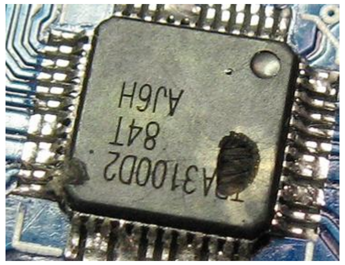
Tampered

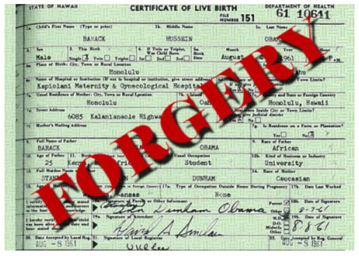
Out-of-spec/ Defective

Forged Documentation









Detected by CDIR sensors

Detected by PUF

Detected by the techniques such as secure split-test (SST), electronic circuit ID (ECID), etc.

Detected by SRAM PUF and Our approach

Major contributions

Recycled IC detection

- First SRAM based approach
- Zero-cost

Aging-sensitive SRAM bit selection algorithm

- Based on SRAM power-up readings
- Under room temperature and high temperature

Parameter analysis

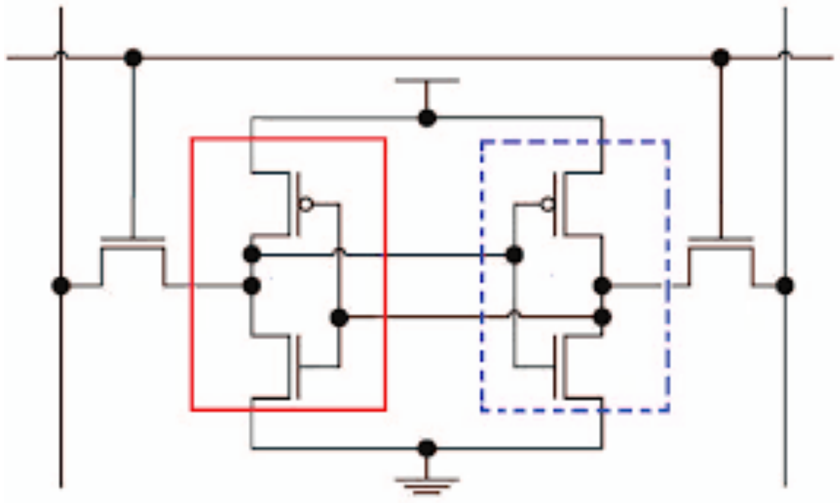
- ID length, threshold, etc.
- Low equal error rate

Measurements evaluation

- Four embedded SRAMs
- More than 10GB real data

SRAM Background

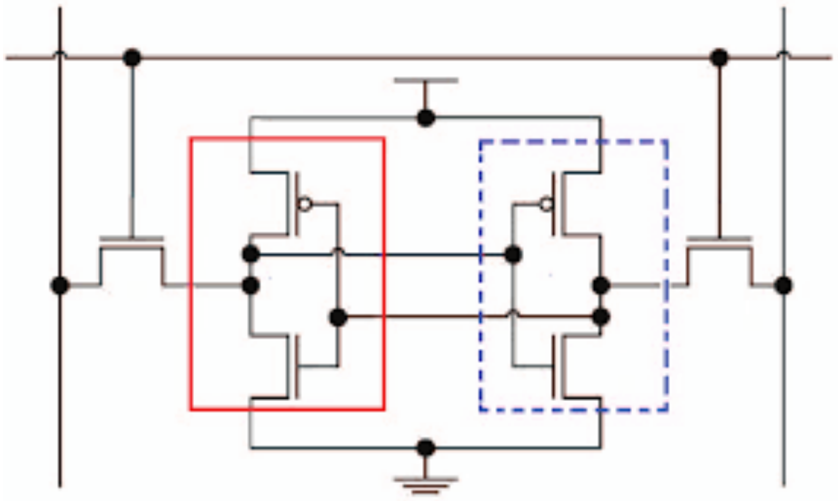
- **Structure:** popular 6-T SRAM (a)



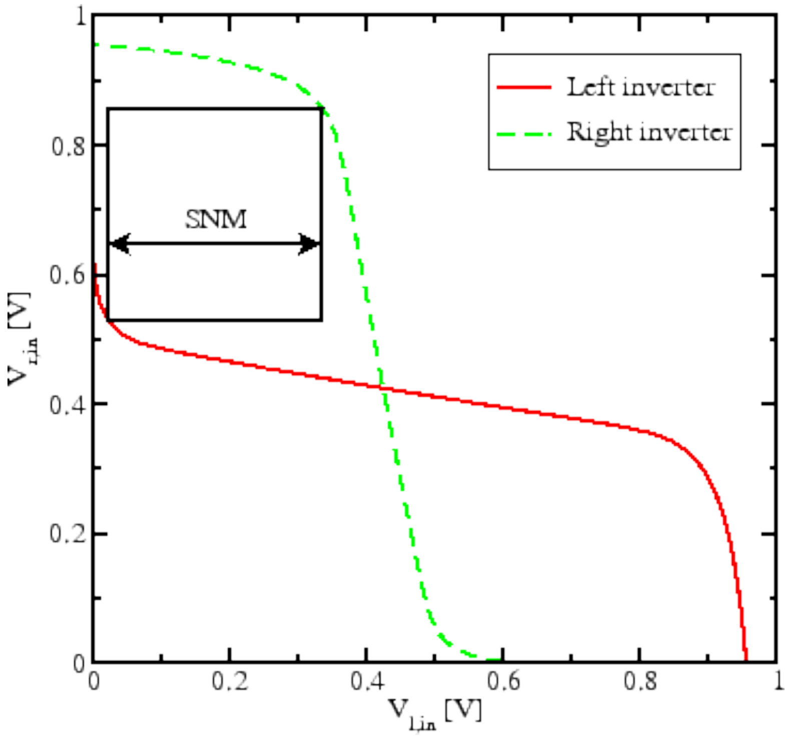
(a) 6Ts COMS SRAM Cell

SRAM Background

- **Structure:** popular 6-T SRAM (a)
- **Start-up behavior of SRAM cells varies due to process variations:**
  - Non-skewed cells: candidates for *SRAM TRNG*
  - Fully-skewed cells: candidates for *SRAM PUF*
  - Partially-skewed cells: candidates for SRAM ***Counterfeit detection***.



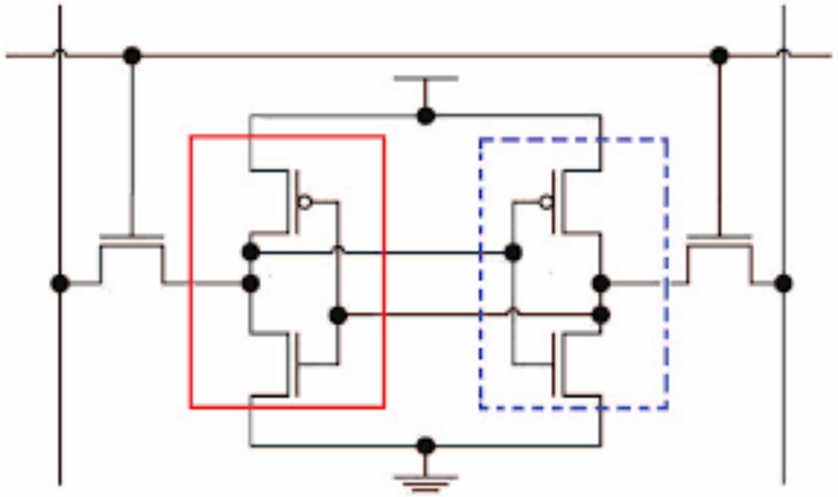
(a) 6Ts COMS SRAM Cell



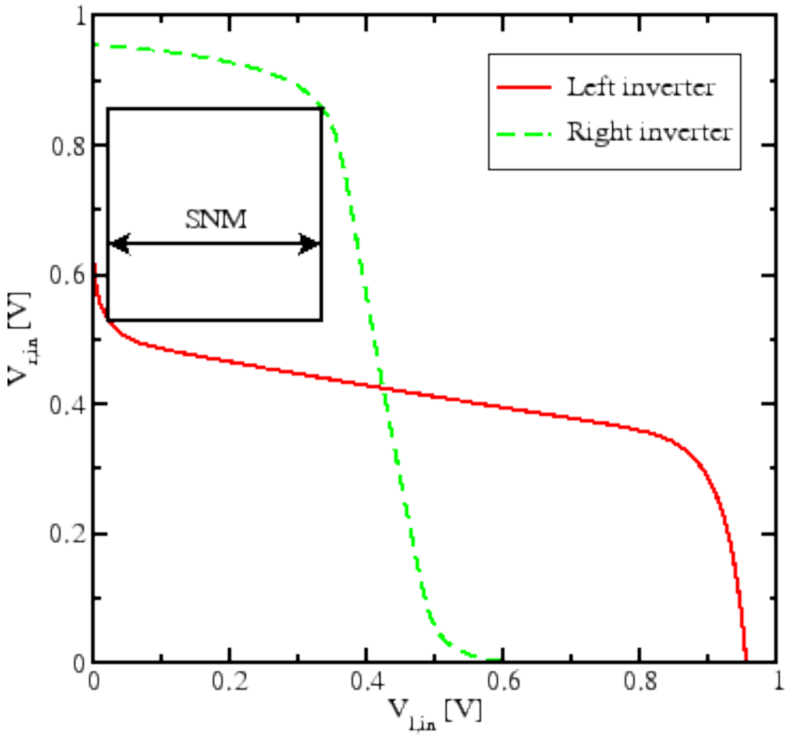
(b) VTCs of an SRAM Cell

SRAM Background

- **Structure:** popular 6-T SRAM (a)
- **Start-up behavior of SRAM cells varies due to process variations:**
  - Non-skewed cells: candidates for *SRAM TRNG*
  - Fully-skewed cells: candidates for *SRAM PUF*
  - Partially-skewed cells: candidates for SRAM ***Counterfeit detection***.
- **SRAM aging:**
  - Hot carrier injection (HCI)
  - Bias temperature instability (BTI)
  - Aging effects on partially-skewed cells: change the start-up values.



(a) 6Ts COMS SRAM Cell



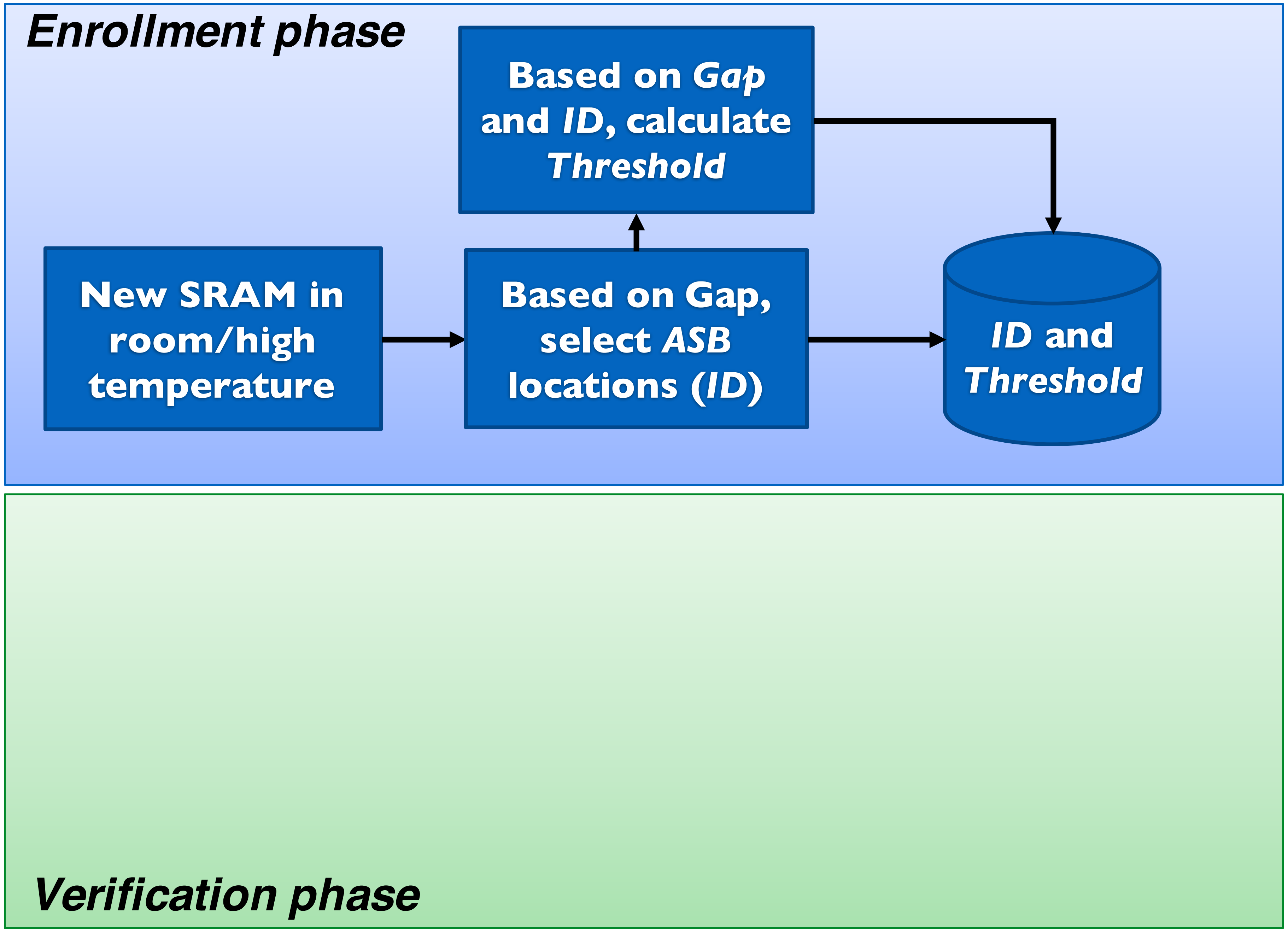
(b) VTCs of an SRAM Cell

Proposed methodology

Enrollment phase

Verification phase

Proposed methodology



Enrollment phase

New SRAM in room/high temperature

Based on Gap, select *ASB* locations (*ID*)

Based on *Gap* and *ID*, calculate *Threshold*

ID and *Threshold*

Verification phase

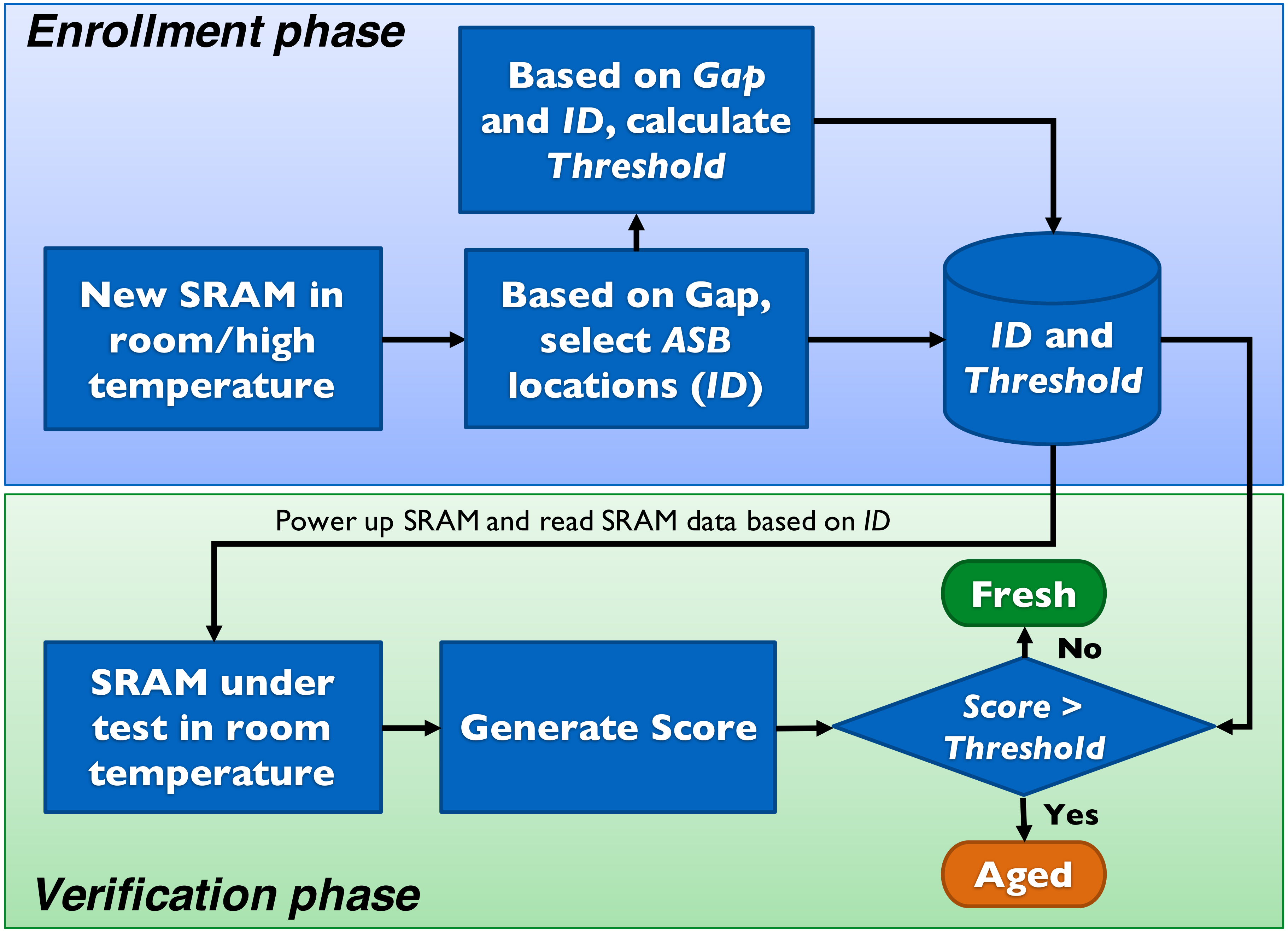
ASBs: **A**geing-**S**ensitive SRAM **B**its (*partially-skewed cells*).

Gap: Designer-defined parameter.

ID: ASB locations.

Threshold: a value used to determined recycled IC.

Proposed methodology


Enrollment phase
Based on *Gap* and *ID*, calculate *Threshold*
New SRAM in room/high temperature
Based on Gap, select *ASB* locations (*ID*)
ID and *Threshold*
Power up SRAM and read SRAM data based on *ID*
Fresh
No
SRAM under test in room temperature
Generate Score
Score > *Threshold*
Yes
Aged
Verification phase

ASBs: **A**geing-**S**ensitive SRAM **B**its (*partially-skewed cells*).

Gap: Designer-defined parameter.

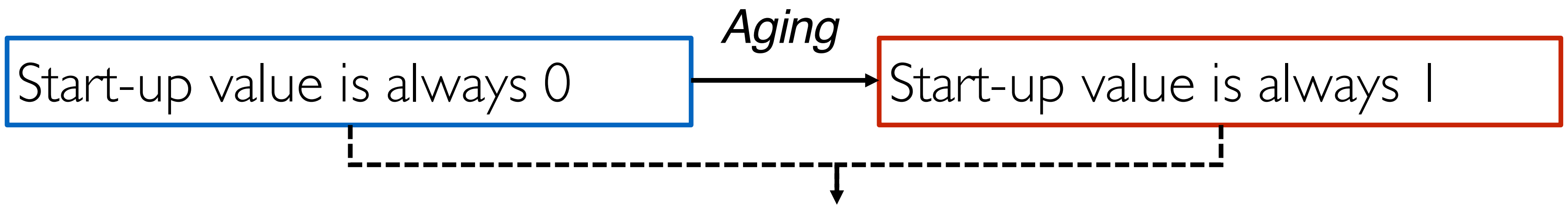
ID: ASB locations.

Threshold: a value used to determined recycled IC.

Score: a value generated by SRAM under test.

ASB qualification

- **Ideal case: a SRAM cell's**



Start-up value is always 0

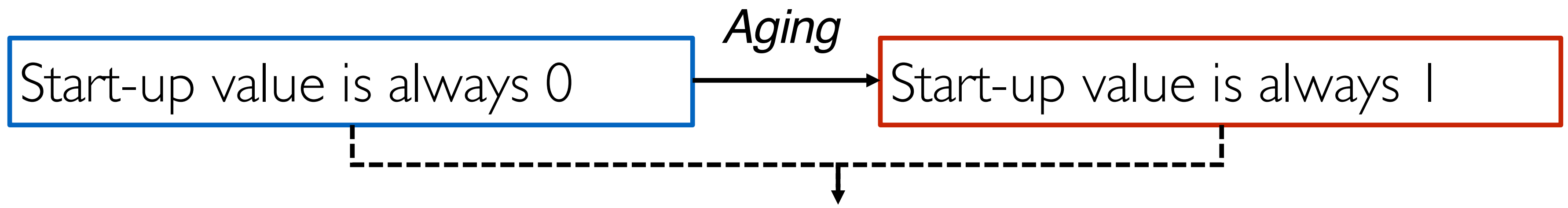
Aging

Start-up value is always 1

Probability of 0 changes by **100%** after aging

ASB qualification

- **Ideal case: a SRAM cell's**



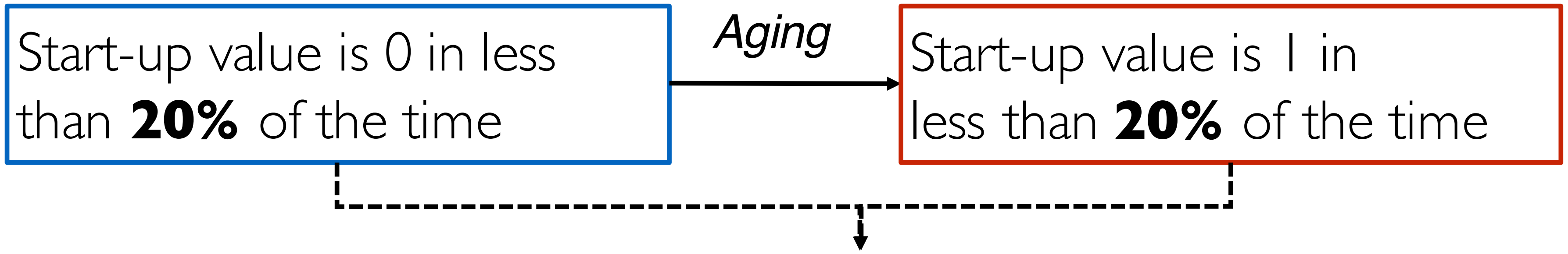
Start-up value is always 0

Aging

Start-up value is always 1

Probability of 0 changes by **100%** after aging

- **More general case: a SRAM cell's**



Start-up value is 0 in less than **20%** of the time

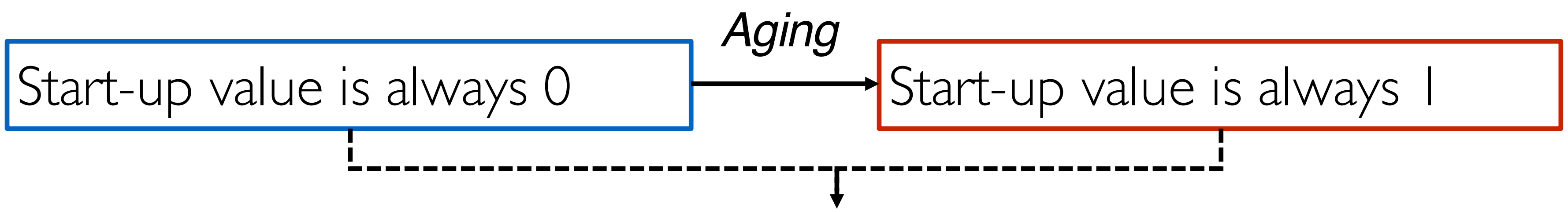
Aging

Start-up value is 1 in less than **20%** of the time

Probability of 0 changes by **60%** after aging

ASB qualification

- **Ideal case: a SRAM cell's**



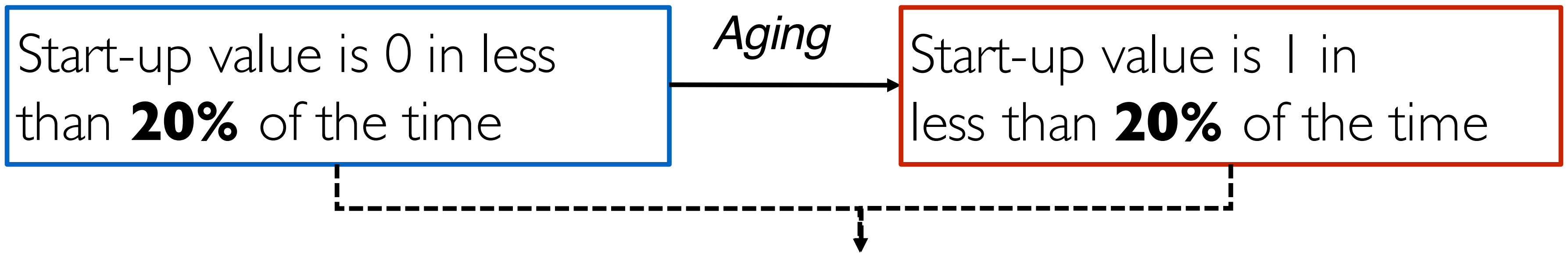
Start-up value is always 0

Aging

Start-up value is always 1

Probability of 0 changes by **100%** after aging

- **More general case: a SRAM cell's**



Start-up value is 0 in less than **20%** of the time

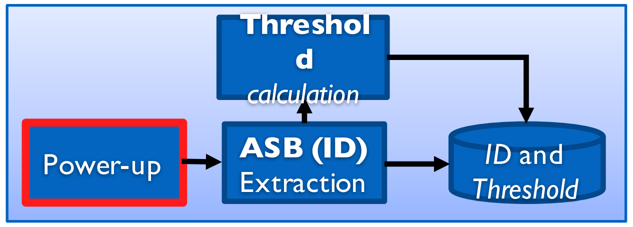
Aging

Start-up value is 1 in less than **20%** of the time

Probability of 0 changes by **60%** after aging

- **Gap**
  - A value ranging from 0 to 1 representing this *probability change*.

Extracting ASB locations

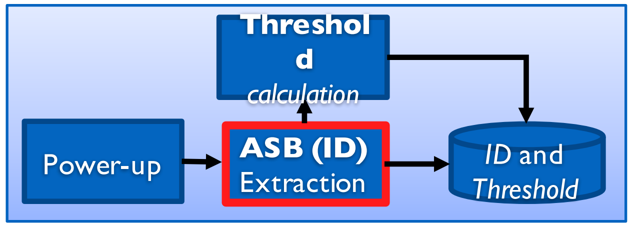


Power up the SRAM for enrollment

New SRAM

“Aged” SRAM

Extracting ASB locations

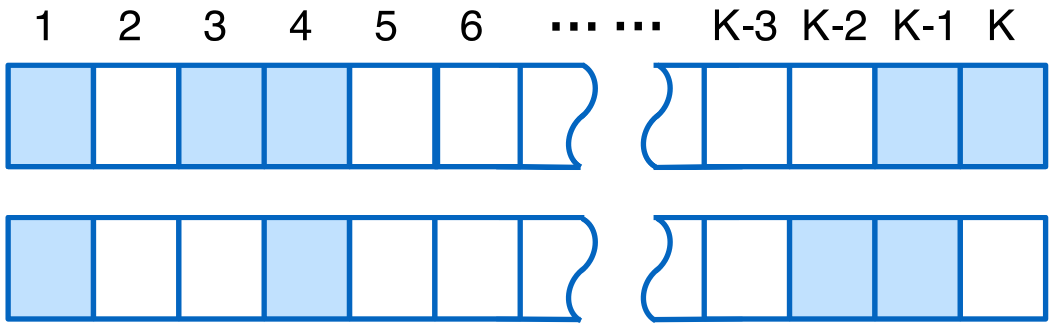


ID is calculated with respect to **Gap** g

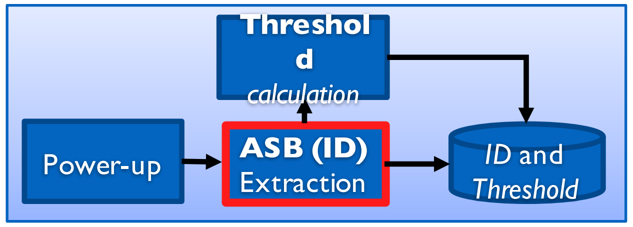
Bit locations (whole SRAM, K bits)

New SRAM ($P_{0|RT}(k) \le \frac{1-g}{2}$)

“Aged” SRAM ($P_{0|PC}(k) > \frac{1+g}{2}$)



Extracting ASB locations

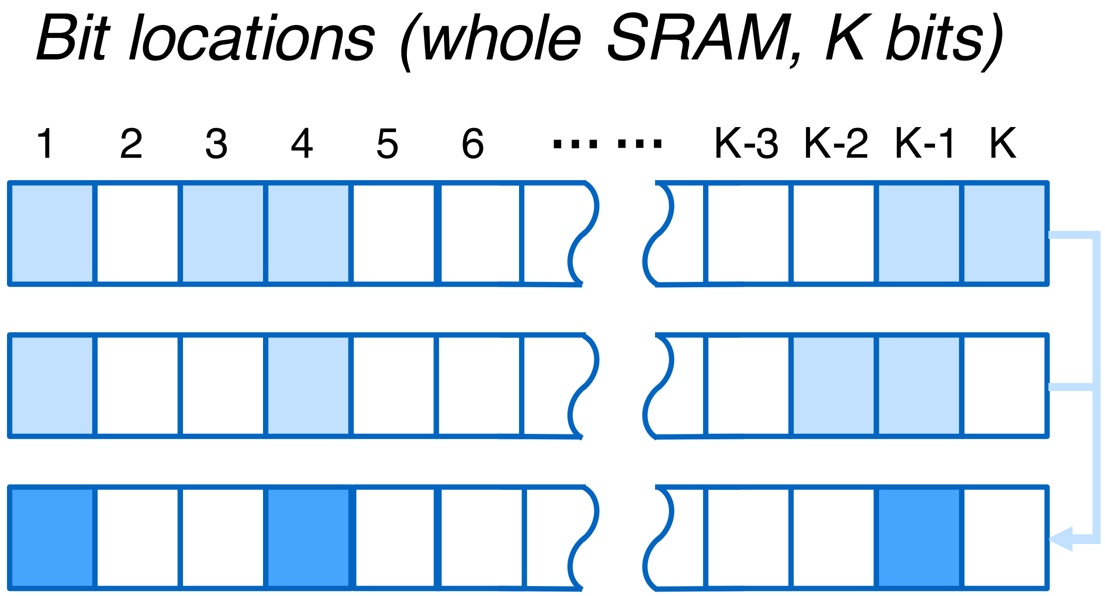


ID is calculated with respect to **Gap** g

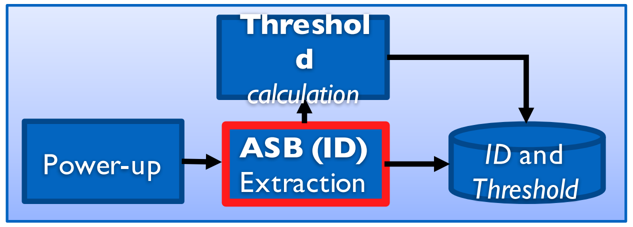
New SRAM ($P_{0|RT}(k) \leq \frac{1-g}{2}$)

“Aged” SRAM ($P_{0|PC}(k) > \frac{1+g}{2}$)

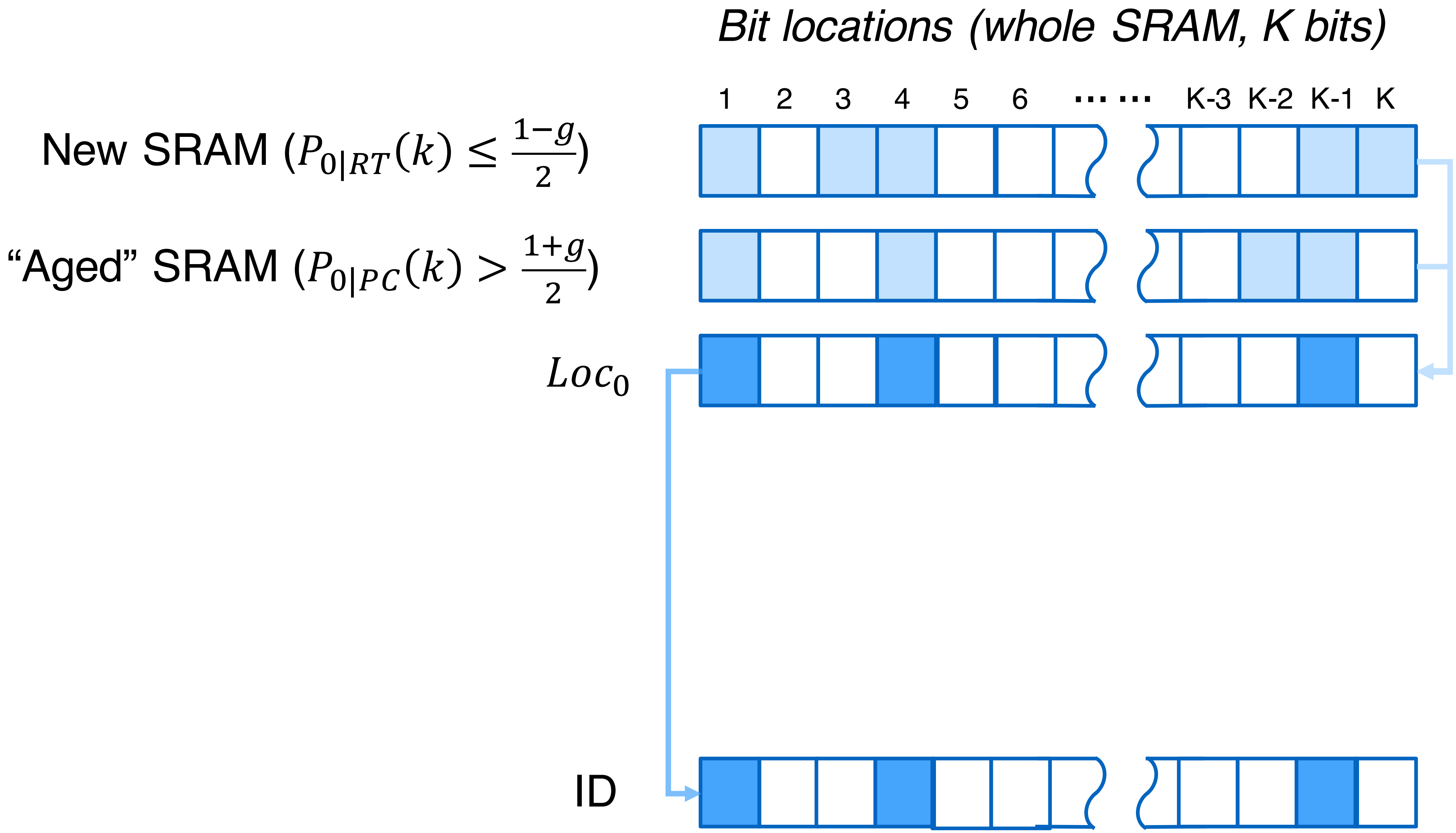
Loc_0



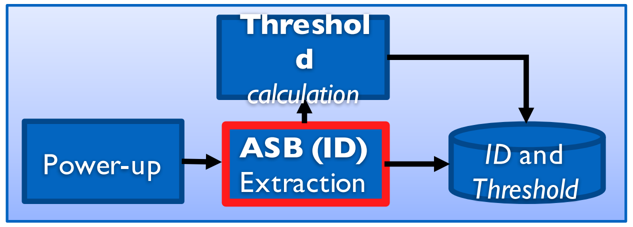
Extracting ASB locations



ID is calculated with respect to **Gap** g

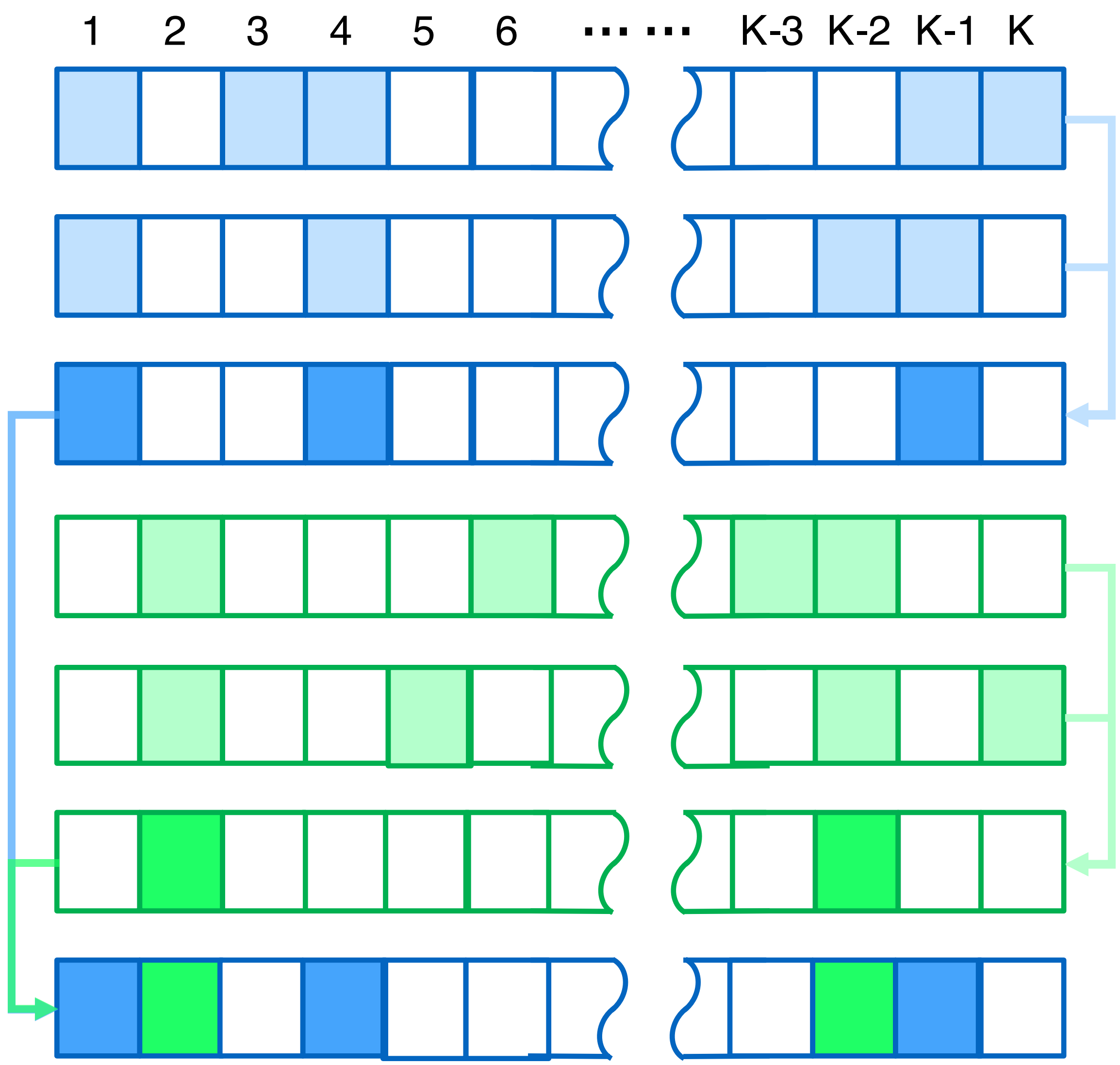

Bit locations (whole SRAM, K bits)
1
2
3
4
5
6
⋯⋯
K-3
K-2
K-1
K
New SRAM ($P_{0|RT}(k) \leq \frac{1-g}{2}$)
"Aged" SRAM ($P_{0|PC}(k) > \frac{1+g}{2}$)
Loc_0
ID

Extracting ASB locations



ID is calculated with respect to **Gap** g

Bit locations (whole SRAM, K bits)



New SRAM ($P_{0|RT}(k) \le \frac{1-g}{2}$)

"Aged" SRAM ($P_{0|PC}(k) > \frac{1+g}{2}$)

Loc_0

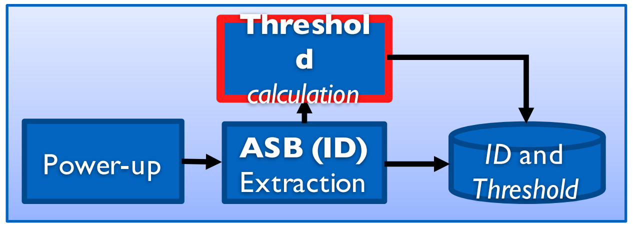
New SRAM ($P_{1|RT}(k) \le \frac{1-g}{2}$)

"Aged" SRAM ($P_{1|PC}(k) > \frac{1+g}{2}$)

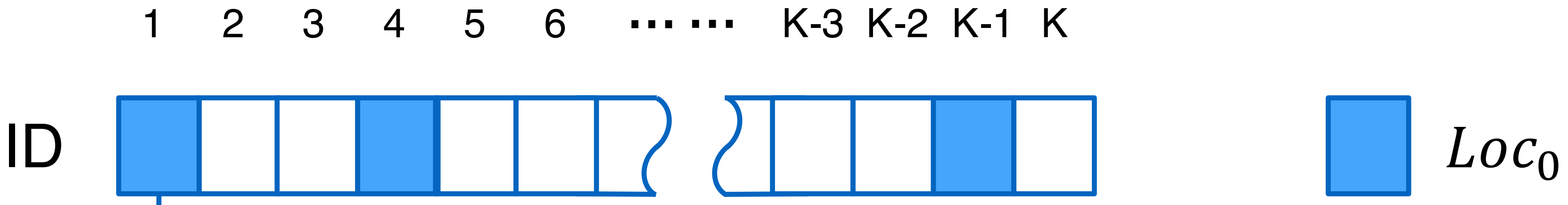
Loc_1

ID

Threshold calculation

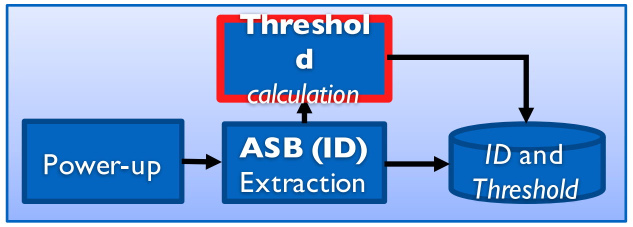


Bit locations (whole SRAM, K bits)

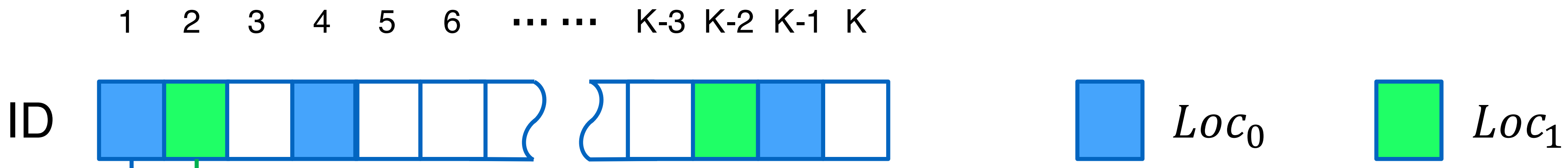


Before aging: $P_{0|RT}(k) \leq \frac{1-g}{2}$ ➔expected number of ‘0’s < $|Loc_0| \times \frac{1-g}{2}$

Threshold calculation



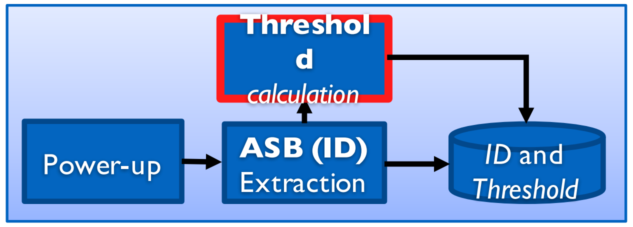
Bit locations (whole SRAM, K bits)

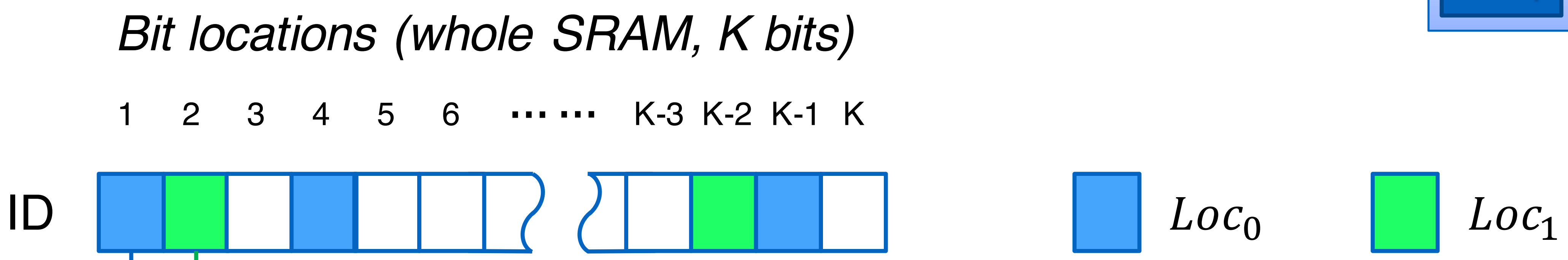


Before aging: $P_{0|RT}(k) \leq \frac{1-g}{2}$ ➔expected number of ‘0’s $< |Loc_0| \times \frac{1-g}{2}$

Before aging: $P_{1|RT}(k) \leq \frac{1-g}{2}$ ➔expected number of ‘1’s $< |Loc_1| \times \frac{1-g}{2}$

Threshold calculation



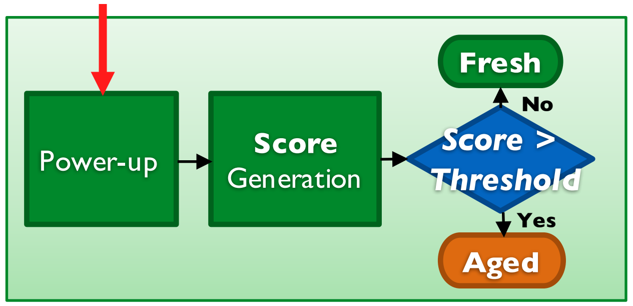

Bit locations (whole SRAM, K bits)
1 2 3 4 5 6 ⋯ ⋯ K-3 K-2 K-1 K
ID
Loc_0
Loc_1

Before aging: $P_{0|RT}(k) \leq \frac{1-g}{2}$ ➔expected number of ‘0’s $< |Loc_0| \times \frac{1-g}{2}$

Before aging: $P_{1|RT}(k) \leq \frac{1-g}{2}$ ➔expected number of ‘1’s $< |Loc_1| \times \frac{1-g}{2}$

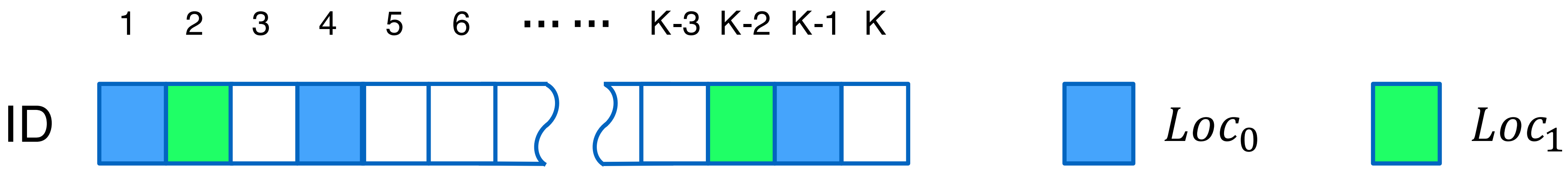
Threshold: $\mathrm{t} = |Loc_0| \times \frac{1-g}{2} + |Loc_1| \times \frac{1-g}{2}$

Score generation

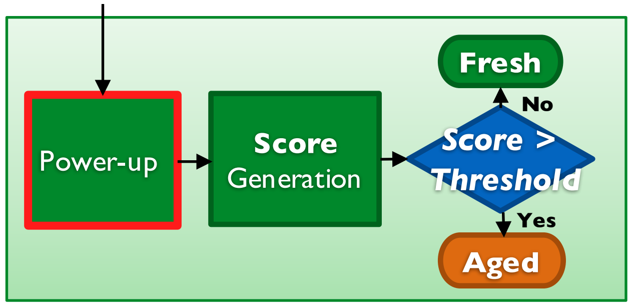


- ***Step 1***: Load **ID** (consists of two independent parts Loc_0 and Loc_1).

Bit locations (whole SRAM, K bits)

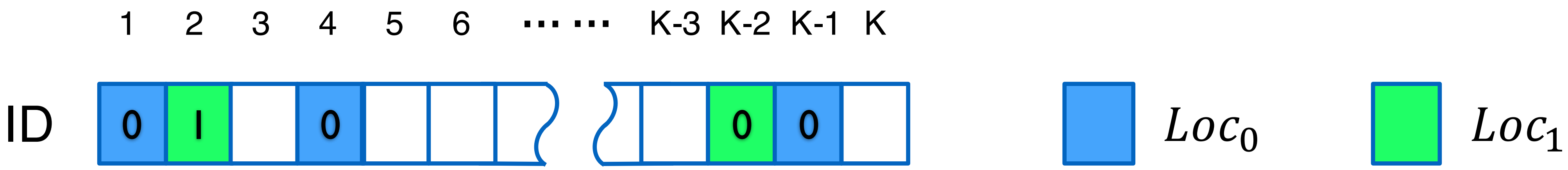


Score generation

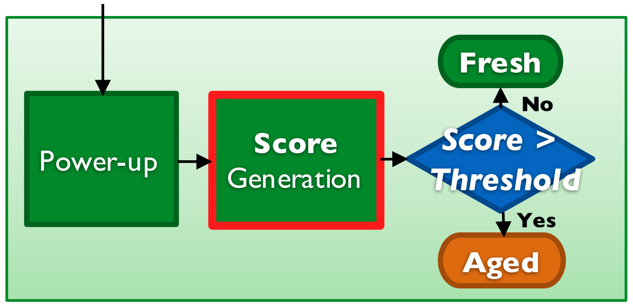


- ***Step 1***: Load **ID** (consists of two independent parts Loc_0 and Loc_1).
- ***Step 2***: Power up SRAM and read the value specified by **ID**.

Bit locations (whole SRAM, K bits)

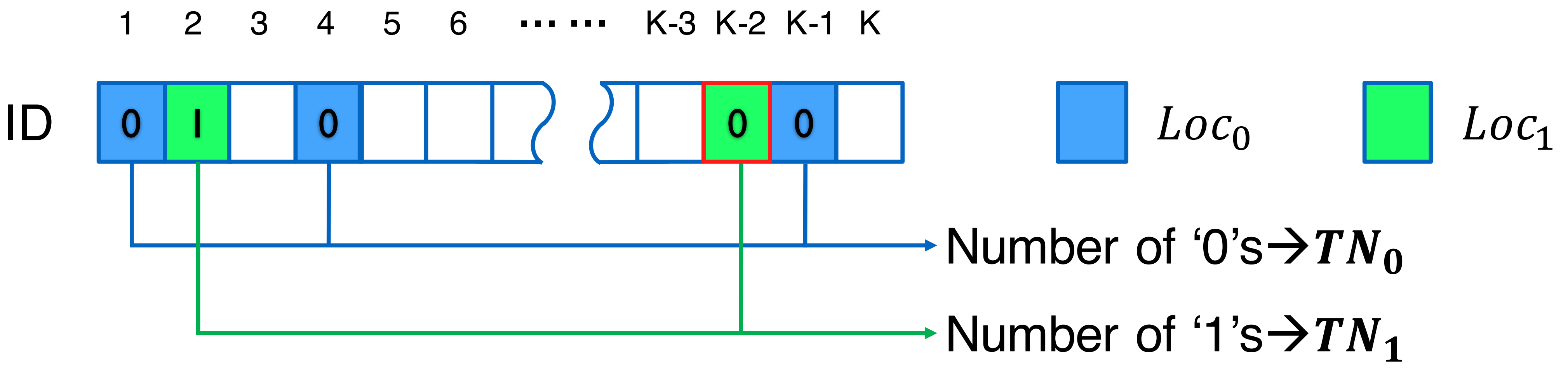


Score generation

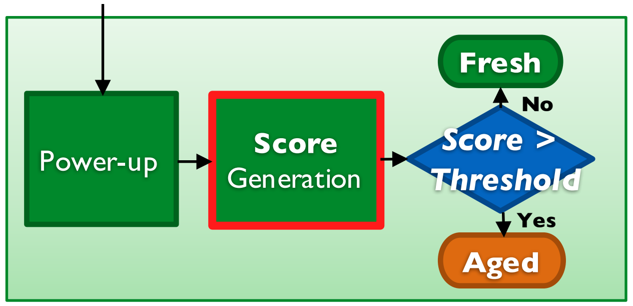


- ***Step 1***: Load **ID** (consists of two independent parts Loc_0 and Loc_1).
- ***Step 2***: Power up SRAM and read the value specified by **ID**.
- ***Step 3***: Count ‘0’/‘1’s among the bits specified by Loc_0/Loc_1 $(\boldsymbol{TN_0}/\boldsymbol{TN_1})$.

Bit locations (whole SRAM, K bits)

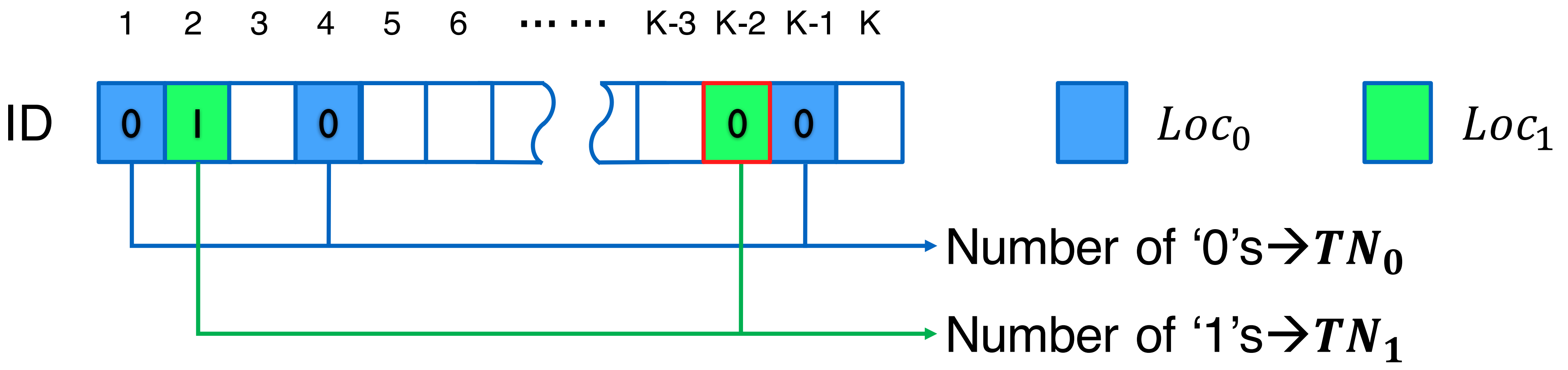

1
2
3
4
5
6
……
K-3
K-2
K-1
K
ID
0
I
0
0
0
Loc_0
Loc_1
Number of ‘0’s→$\boldsymbol{TN_0}$
Number of ‘1’s→$\boldsymbol{TN_1}$

Score generation

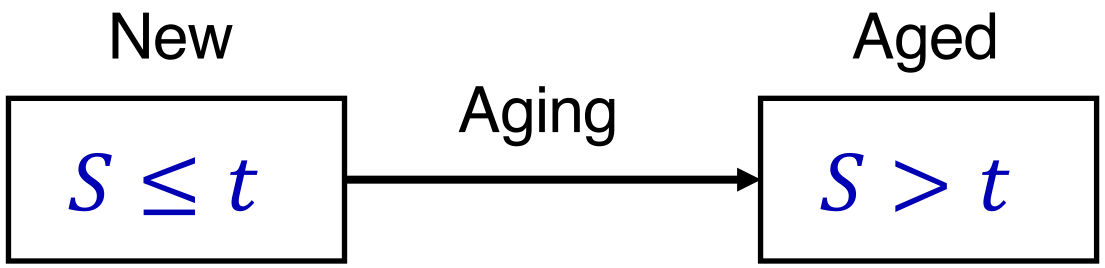


- ***Step 1***: Load **ID** (consists of two independent parts Loc_0 and Loc_1).
- ***Step 2***: Power up SRAM and read the value specified by **ID**.
- ***Step 3***: Count ‘0’/‘1’s among the bits specified by Loc_0/Loc_1 ($\boldsymbol{TN_0}/\boldsymbol{TN_1}$).

Bit locations (whole SRAM, K bits)


1 2 3 4 5 6 ⋯⋯ K-3 K-2 K-1 K
ID
0
1
0
0
0
Loc_0
Loc_1
Number of ‘0’s→$\boldsymbol{TN_0}$
Number of ‘1’s→$\boldsymbol{TN_1}$

- **Score** ($S = TN_0 + TN_1$)

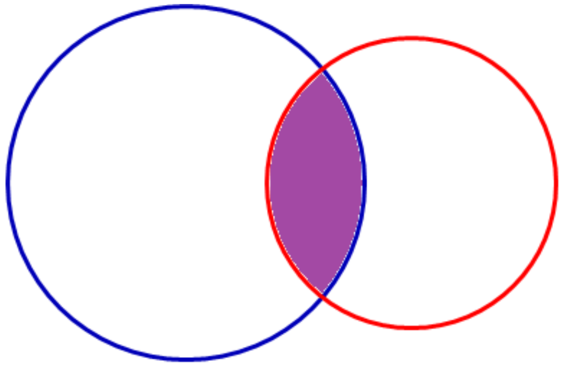


Prediction with proper testing conditions

Predicted ID extracted from

- New SRAM → New SRAM in room temperature
- "Aged" SRAM → New SRAM in High/Low temperature

$\{\mathbf{1}, 4, 5, \mathbf{12}, 15, \mathbf{26}, 60, \mathbf{78}, \ldots\}$

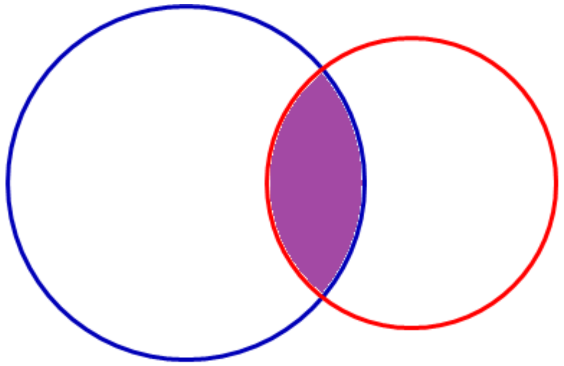


Prediction with proper testing conditions

Predicted ID extracted from

- New SRAM → New SRAM in room temperature
- "Aged" SRAM → New SRAM in High/Low temperature

$\{\mathbf{1}, 4,5, \mathbf{12}, 15, \mathbf{26}, 60, \mathbf{78}, \ldots\}$



True ID extracted from

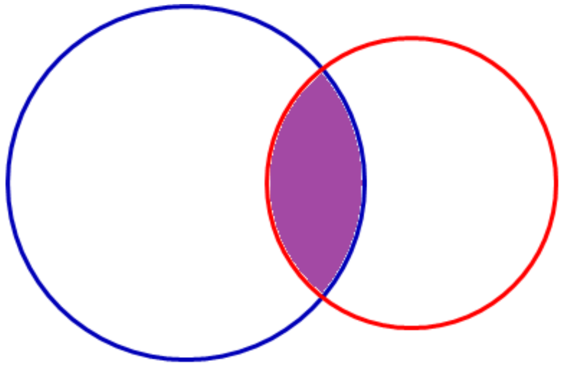
- New SRAM → New SRAM in room temperature
- "Aged" SRAM → Aged SRAM in room temperature

$\{\mathbf{1}, 3,6, \mathbf{12}, \mathbf{26}, 27,31,59, \mathbf{78}, \ldots\}$

Prediction with proper testing conditions

Predicted ID extracted from
- New SRAM → New SRAM in room temperature
- "Aged" SRAM → New SRAM in High/Low temperature

$\{\mathbf{1},4{,}5,\mathbf{12},15,\mathbf{26},60,\mathbf{78},\ldots\}$



Overlapped locations
$\{1{,}12{,}26{,}78,\ldots\}$

True ID extracted from
- New SRAM → New SRAM in room temperature
- "Aged" SRAM → Aged SRAM in room temperature

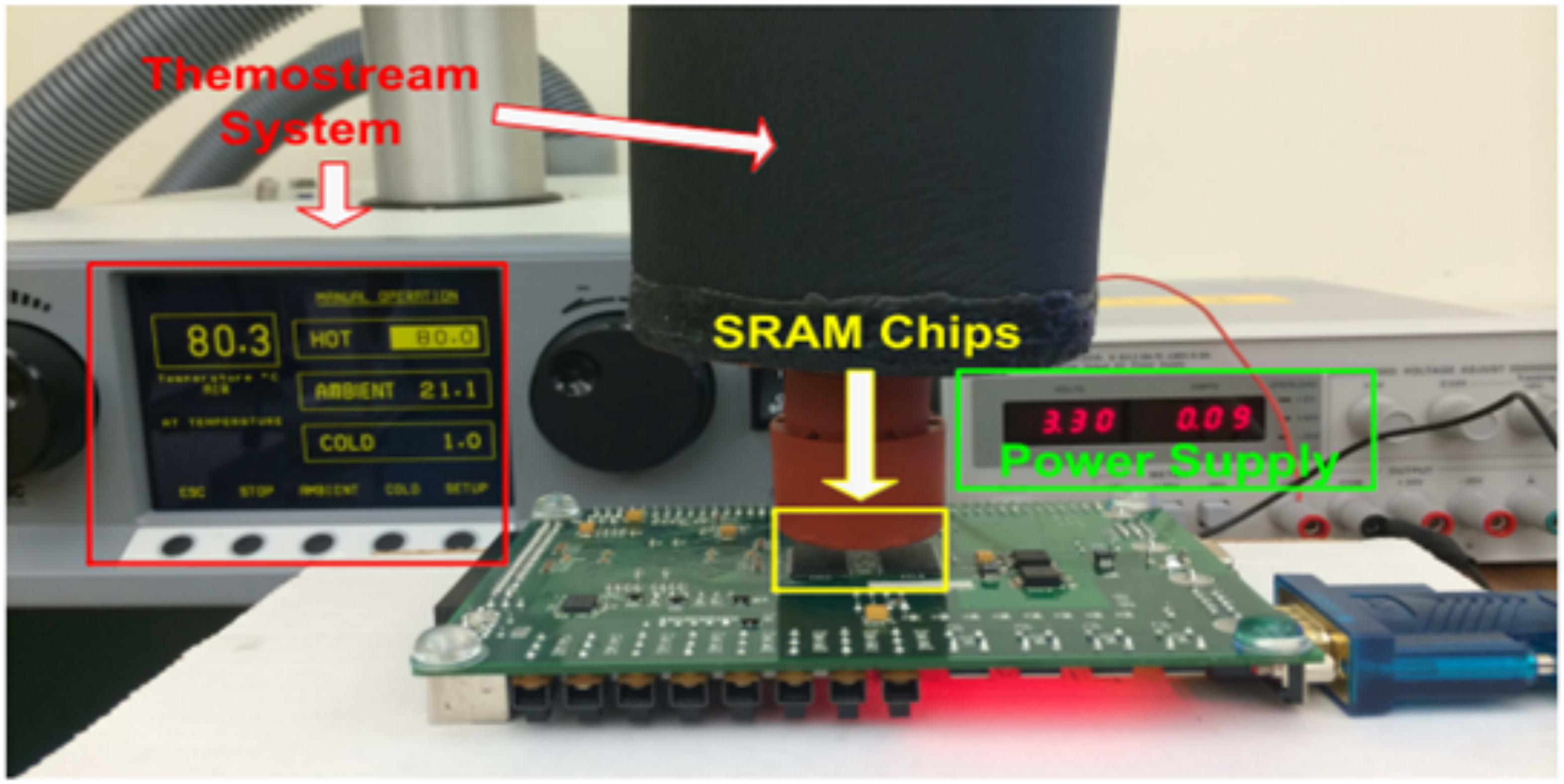
$\{\mathbf{1},3{,}6,\mathbf{12},\mathbf{26},27{,}31{,}59,\mathbf{78},\ldots\}$

$\frac{\lvert\text{Overlapped locations}\rvert}{\lvert\text{Predicted ID}\rvert}$	Gap values					
	0.5	0.6	0.7	0.8	0.9	1
High temperature	18%	17%	14%	9%	14%	25%
Low temperature	12%	9%	7%	8%	7%	20%

Experimental results

Experiment Setup

- Platforms: 4 Spartan-3 FPGAs with 2 MB on-board SRAM
- Temperature corners: Low 0°C, Room 20°C, High 80°C.
- Voltage corners: 3.0V, 3.3V and 3.6V.
- 10 trials for each testing corner.
- Aging duration: 5 hours accelerated aging.



Experimental results

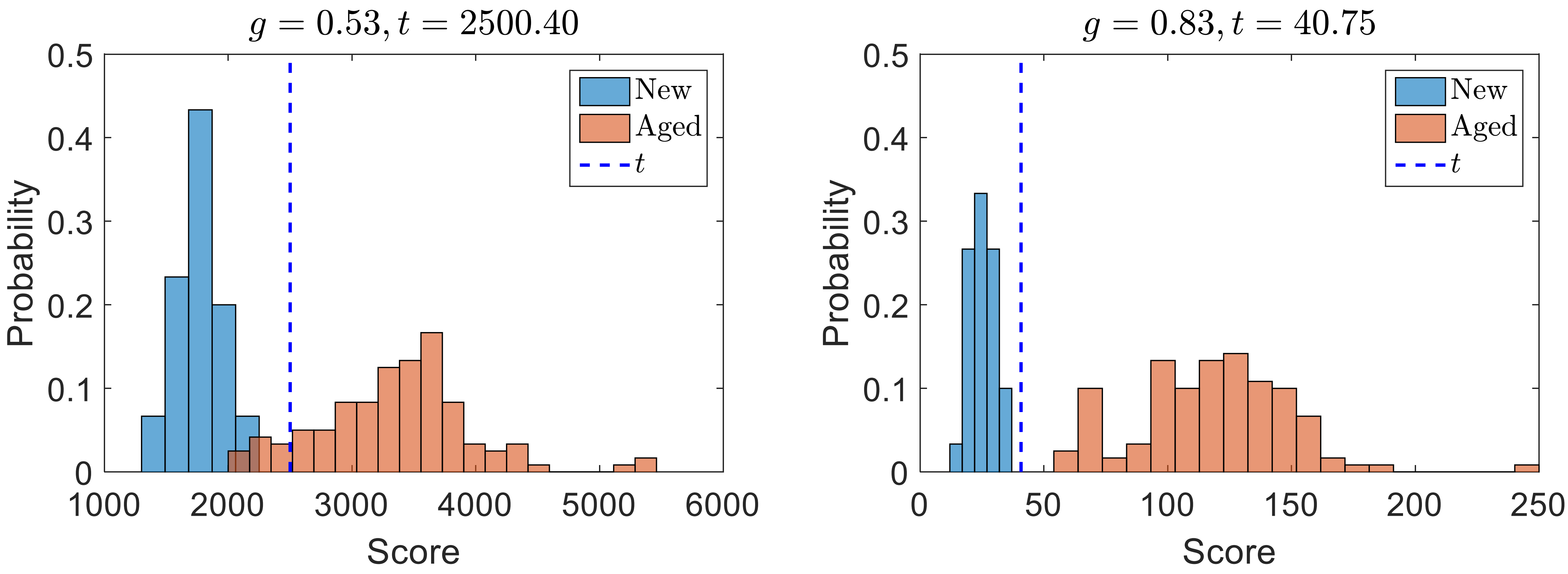
Experiment Setup

- Platforms: 4 Spartan-3 FPGAs with 2 MB on-board SRAM
- Temperature corners: Low 0°C, Room 20°C, High 80°C.
- Voltage corners: 3.0V, 3.3V and 3.6V.
- 10 trials for each testing corner.
- Aging duration: 5 hours accelerated aging.

Metrics

- False Accept Rate ($\boldsymbol{FAR}$)
  - $FAR = \frac{\text{The number of trials which detect the } \textbf{aged} \text{ SRAM as } \textbf{new}}{\text{Total numbr of trails}}$
- False Reject Rate ($\boldsymbol{FRR}$)
  - $FRR = \frac{\text{The number of trials which detect the } \textbf{new} \text{ SRAM as } \boldsymbol{aged}}{\text{Total numbr of trails}}$
- Equal Error Rate ($\boldsymbol{EER}$)
  - $EER = \frac{FAR+FRR}{2}$
- **ID length**

Effect of different Gap values



$g = 0.53, t = 2500.40$

(a)

$g = 0.83, t = 40.75$

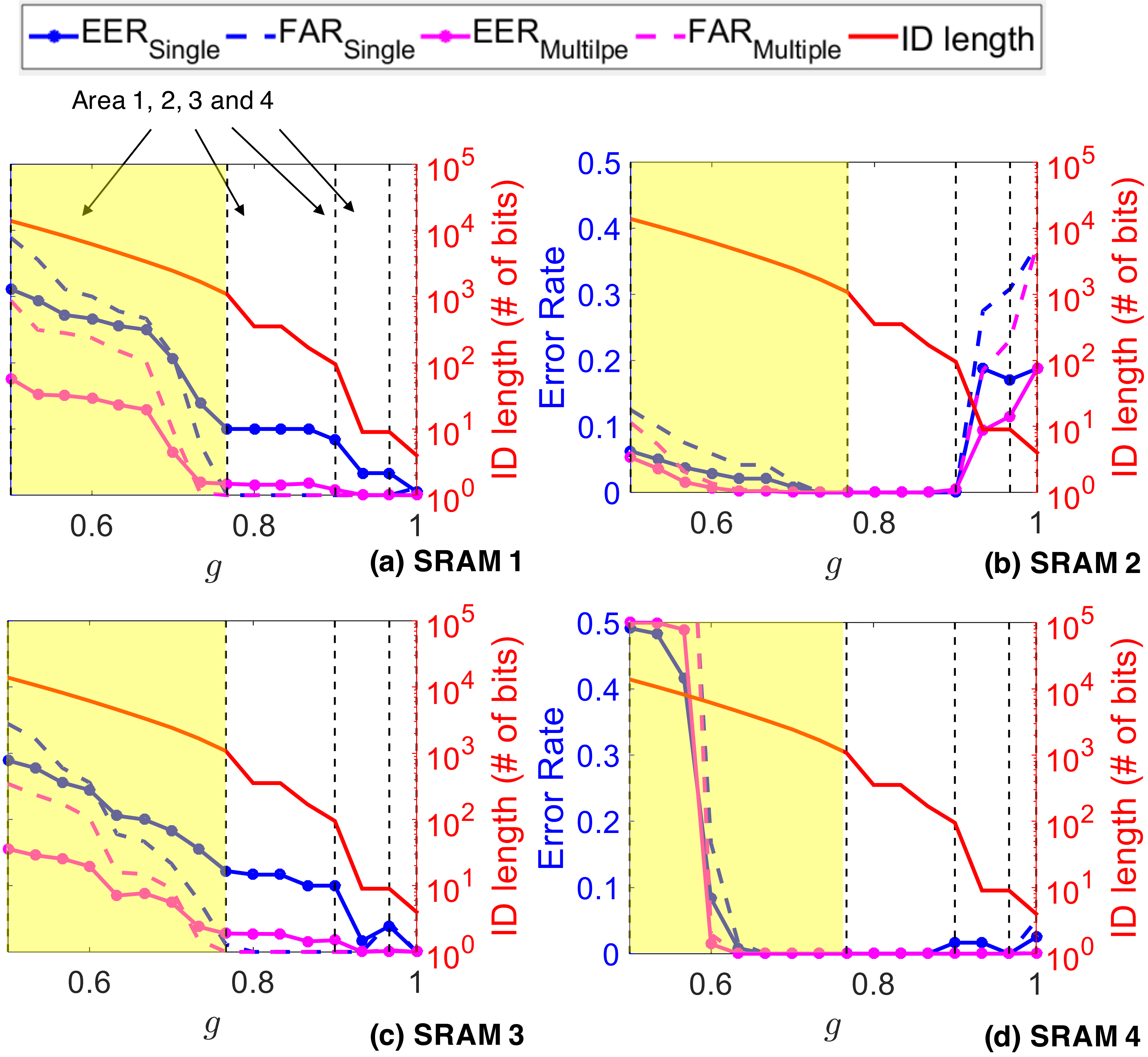
(b)

Score distributions on different Gap values

Experimental results

Area 1: Large error rates due to a small gap values. New and Aged SRAM scores heavily overlap.

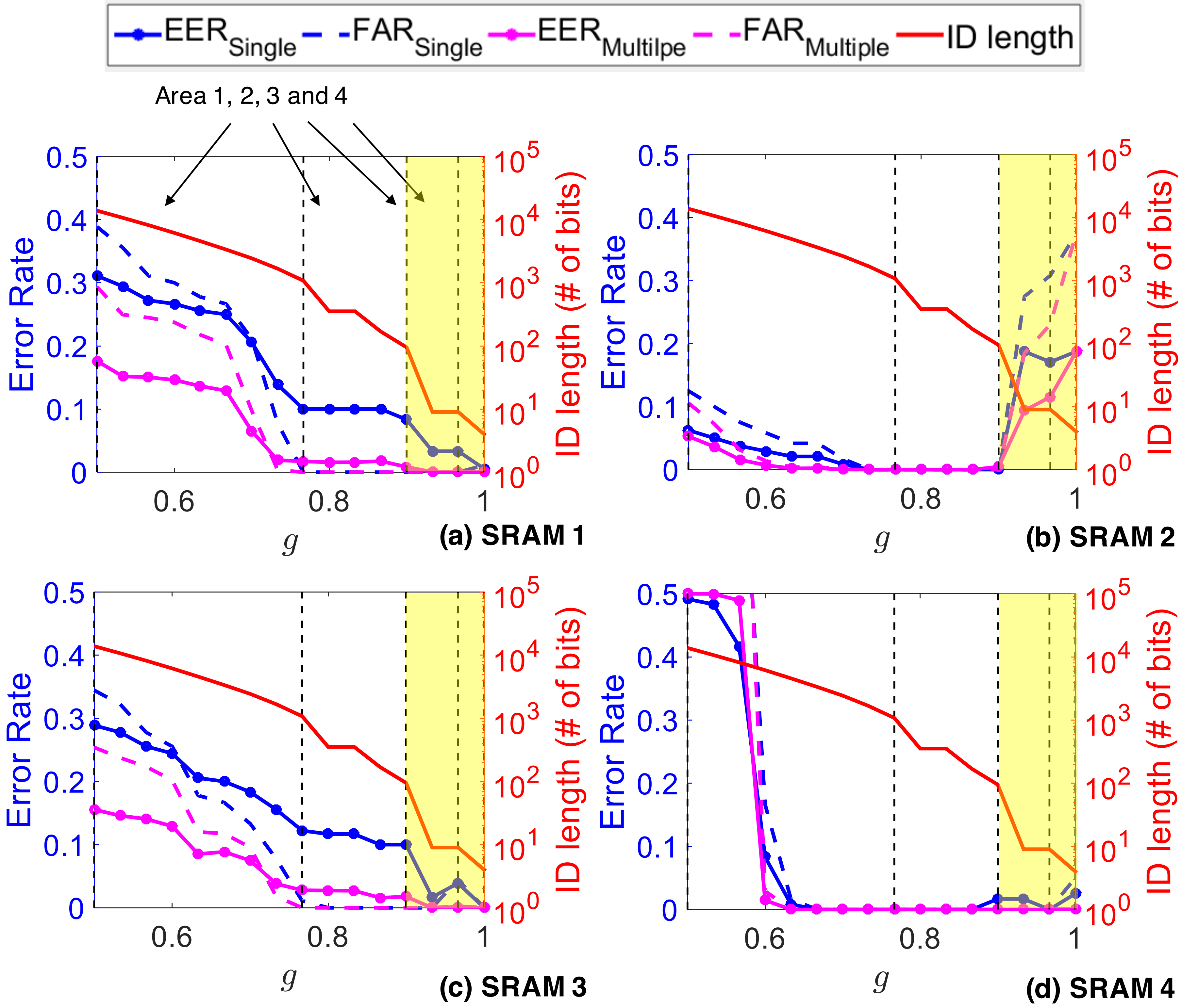
SRAM #	EER	FAR
1	0.21	0.25
2	0.05	0.05
3	0.15	0.20
4	0.25	0.25



Experimental results

Area 3 and **4**: Large gap values result in short IDs. One bit error leads to a large total error rate.

SRAM #	EER	FAR
1	0.00	0.00
2	0.14	0.28
3	0.00	0.00
4	0.00	0.00



(a) SRAM 1

(b) SRAM 2

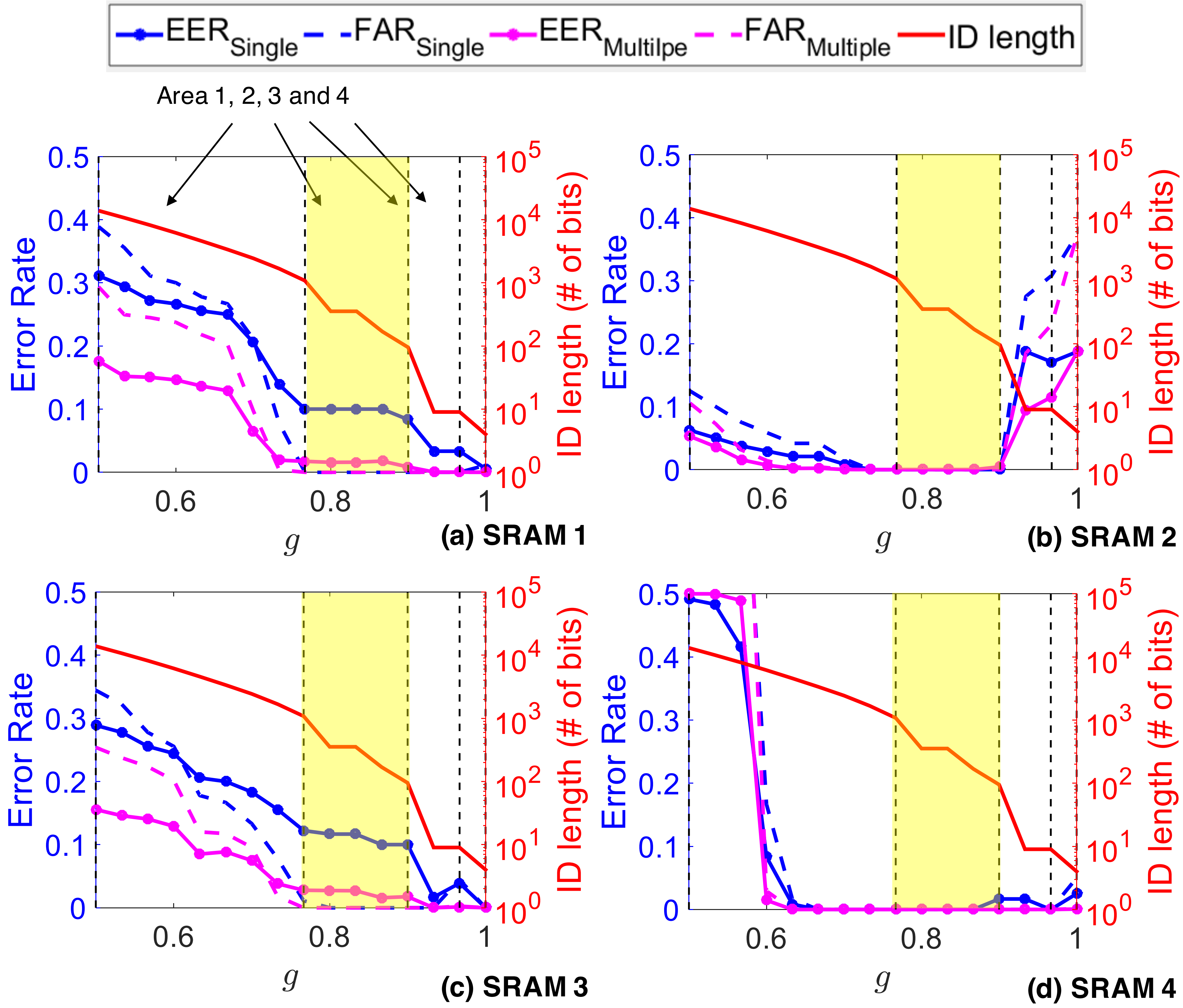
(c) SRAM 3

(d) SRAM 4

Experimental results

Area 2: Good operation range with respect to robustness and accuracy.

SRAM #	EER	FAR
1	0.01	0.00
2	0.00	0.00
3	0.03	0.00
4	0.00	0.00



Conclusion and future work

Conclusion

- Recycled ICs detection with no hardware overhead.
- Acceptable overall accuracy (**more than 97%**).
- Strict detection performance (**100% detection of aged SRAMs**).

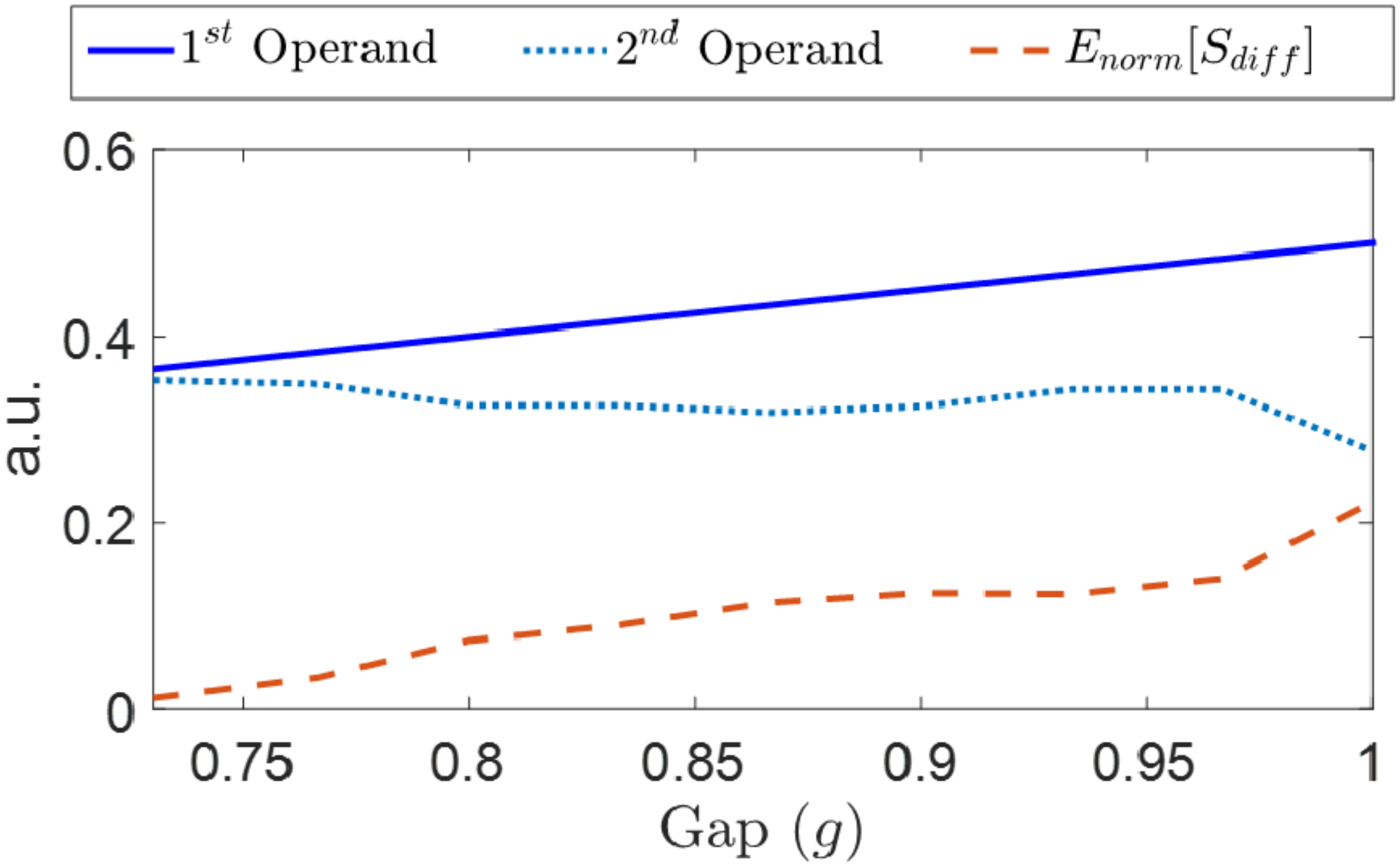
Future work

- Test on more SRAMs.
- Apply shorter aging time.
- Increasing the trials during the enrollment phase.
- Apply reinforced aging.

Questions?

Backup slides

Prediction accuracy estimation



$$E[S_{diff}] = E[S_{aged}] - E[S_{new}]$$

Expected score difference incr eases as Gap increasing