1D-5

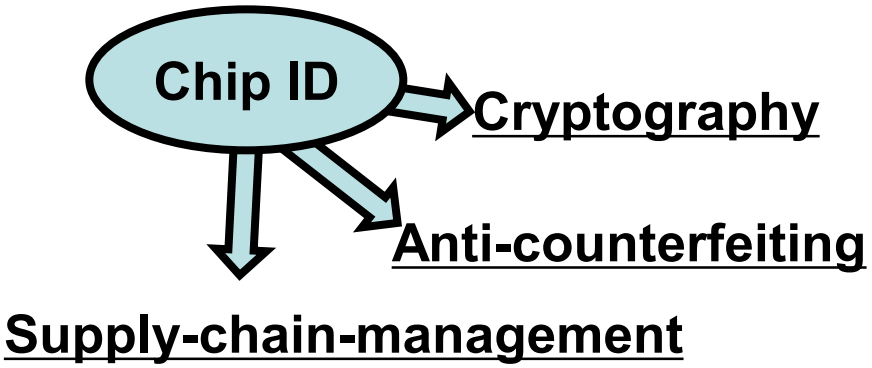
A Physical Unclonable Function Chip Exploiting Load Transistors' Variation in SRAM Bitcells

Shunsuke Okumura[1], Shusuke Yoshimoto[1],
Hiroshi Kawaguchi[1],
and Masahiko Yoshimoto[1,2].

[1]Kobe University
[2]JST, CREST

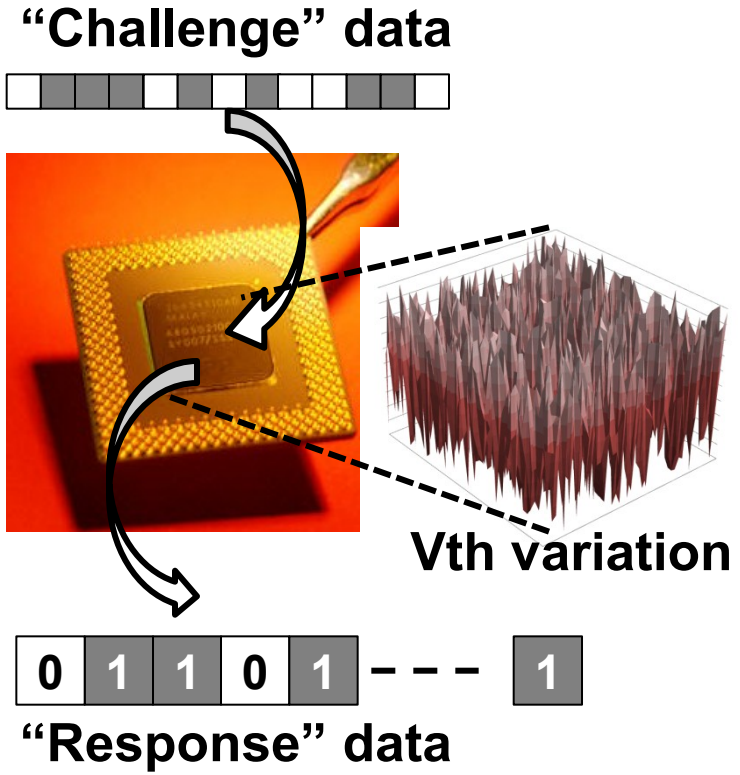
Jan. 23th, 2013, ASP-DAC

Backgraoud



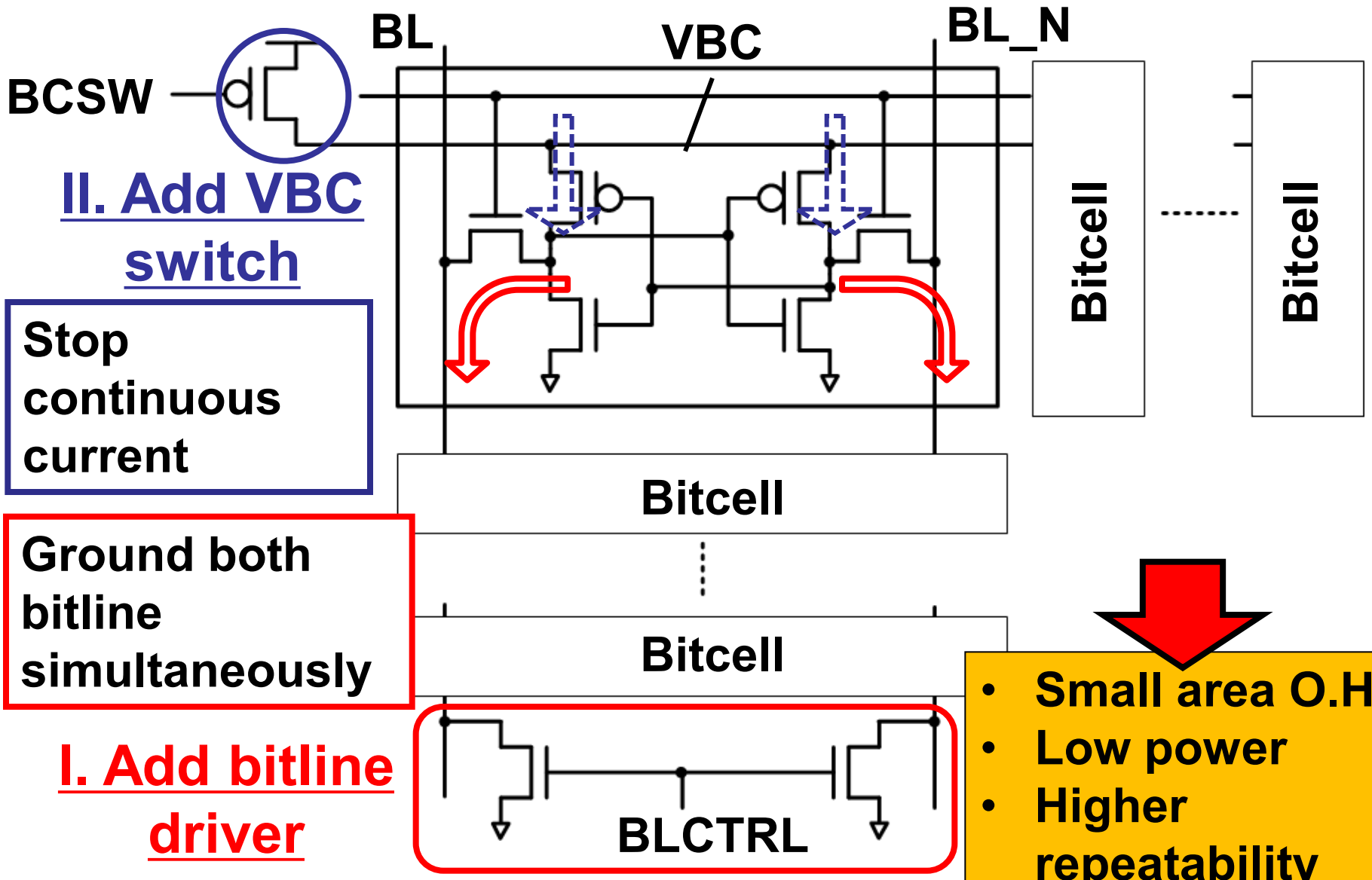
To prevent illegal replication of chip ID

Physical Unclonable Function (PUF) is applied to chip ID.

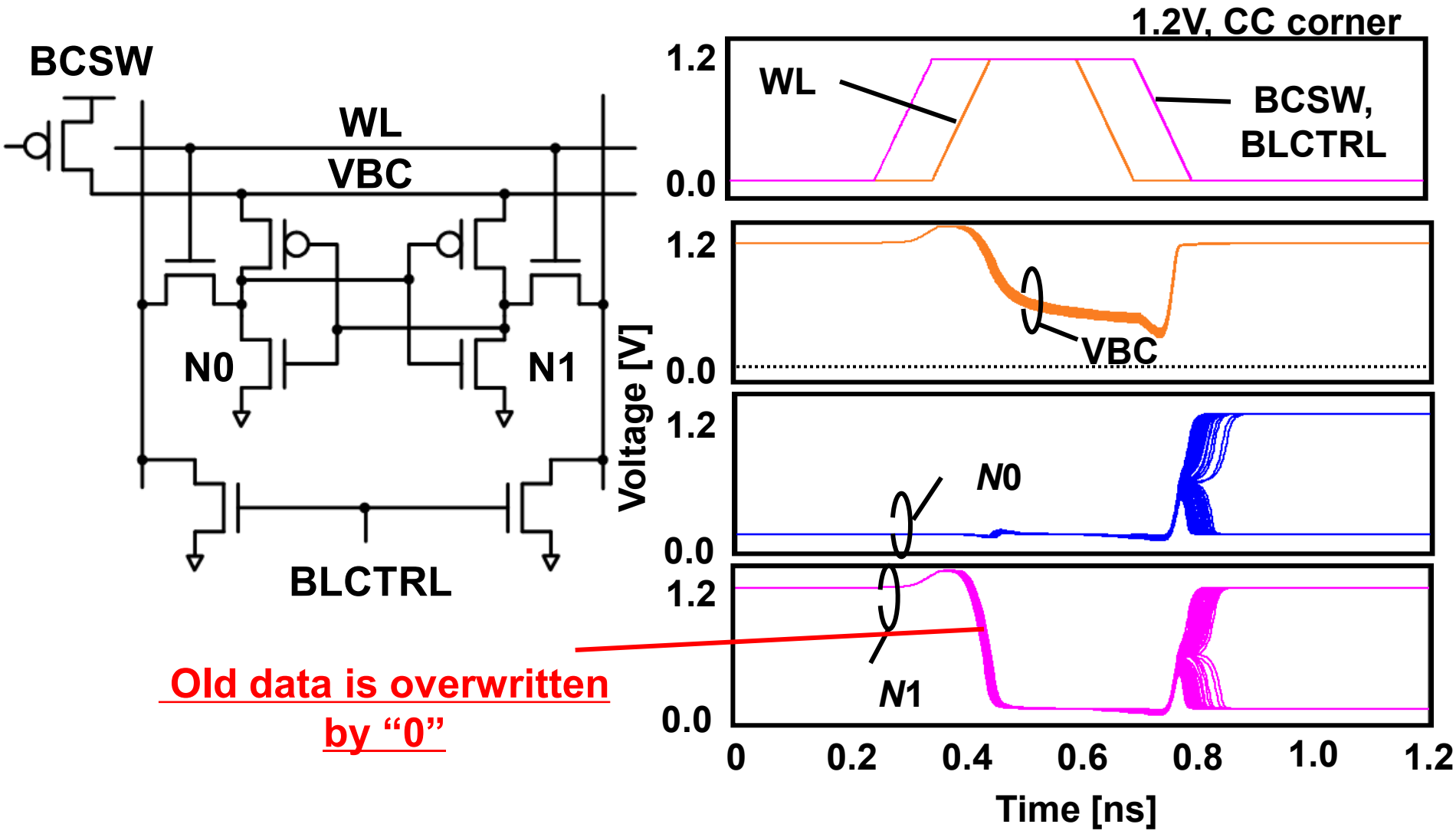


PUF needs
- Repeatability
- Randomness
- Low power

Proposed ID generation Scheme



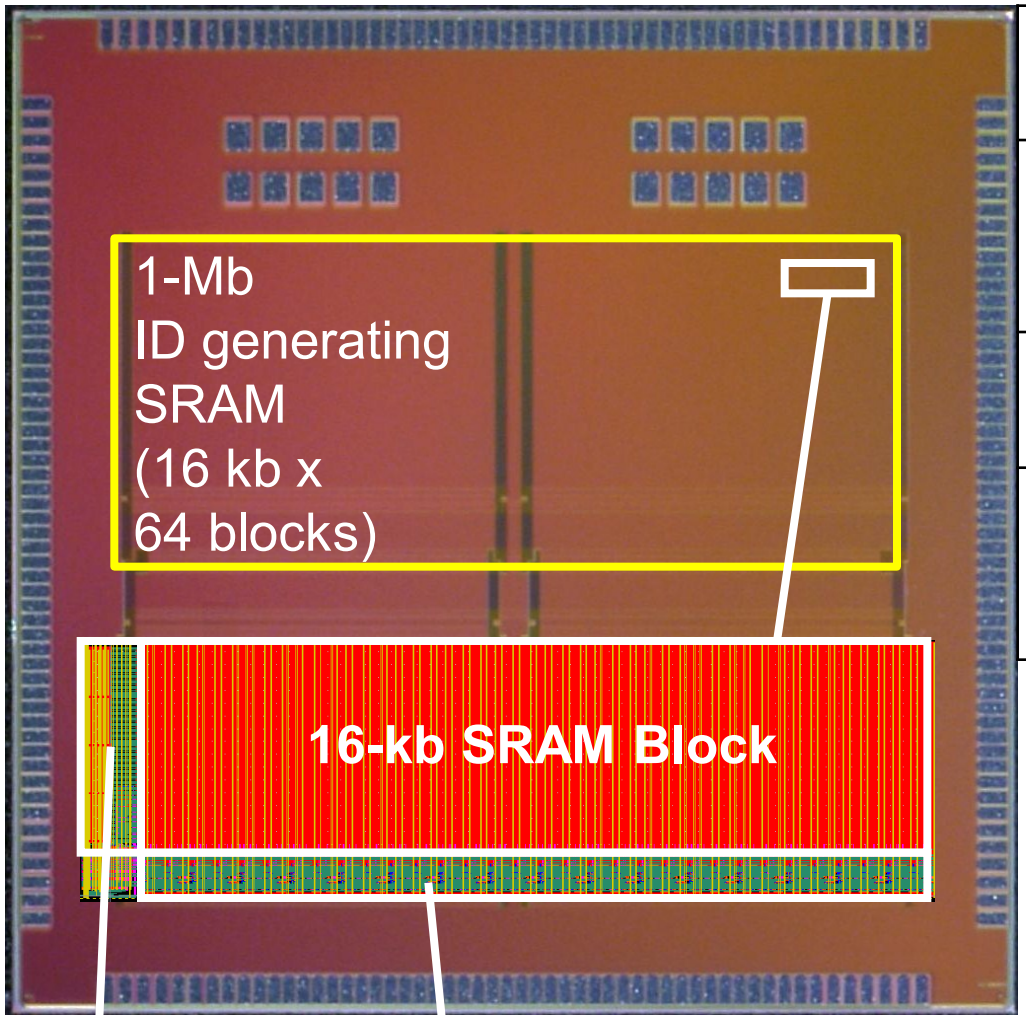
Simulation waveforms



Old data is overwritten by "0"

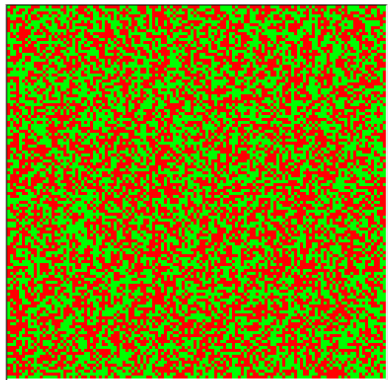
Bitcells store unique values depending on the variation.

Test chip



X decoder Y decoder & I/O circuits

Technology	65-nm CMOS 12 metal layers
Area	4.82 mm^2 (1260 um x 3240 um)
SRAM organization	16-kb block x 64 (= 1 Mb)
Block configuration	128 rows x 8 columns x 16 bits/word



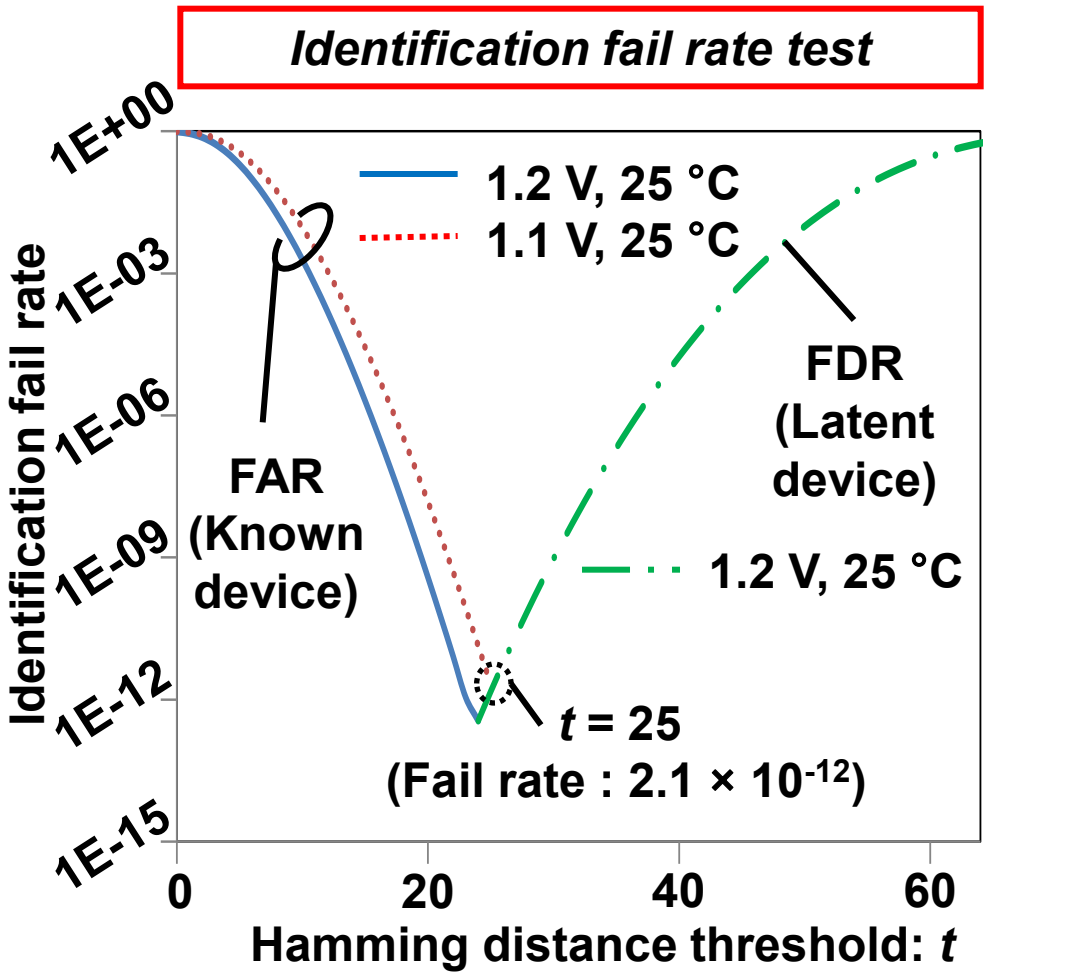
“0”
“1”

Generated chip ID (128 b x 128 rows)

Experimental results

- 12,288 sample ID
- Voltage fluctuation test
- Temperature fluctuation test
- Aging test

Repeatability and Identification fail rate are estimated.



Identification fail rate: 2.1×10^{-12}