Permission to Use Conditions

1. Permission is granted to copy and distribute this slide set for educational purposes only, provided that the complete bibliographic citation and following credit line is included: “Hardware Security Slides by F. Gebali. ©2024. Gebali”.
2. Permission is granted to alter and distribute this material provided that the following credit line is included: “Adapted from Hardware Security Slides by F. Gebali. ©2024. Gebali"
3. This material may not be copied or distributed for commercial purposes without express written permission of the copyright holder.

ECE 448/548 Cyber-System Security

DRAM PUF

F. Gebali

EOW 433

Office Phone: 250-721-6509

`https://ece.engr.uvic.ca/~fayez/`

Outline

1 Intro

2 DRAM

3 Setup

4 Model

5 DRAM PUF

6 SNR

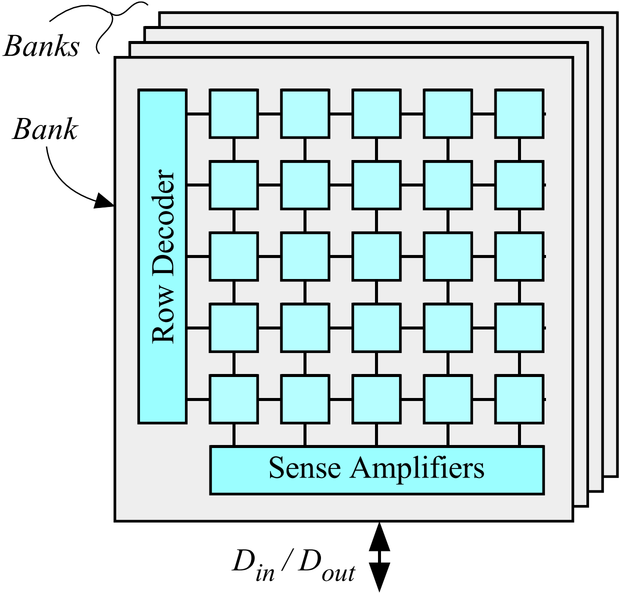
Introduction

DRAM PUFs

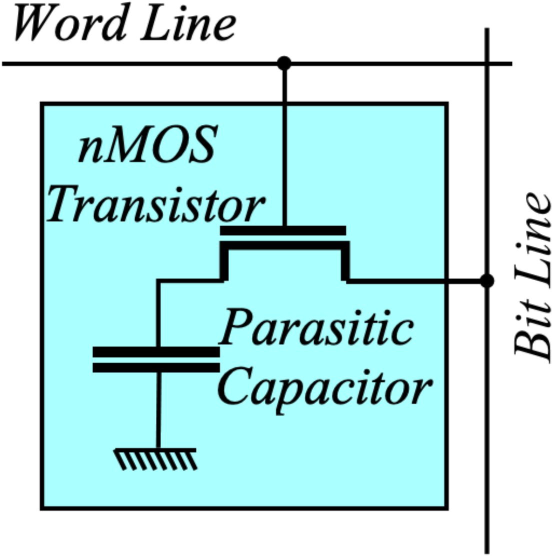
1. DRAM is present in many ICs including IoT devices
2. Using DRAM as a PUF relies on one of two things:
   1. Retention-based DRAM PUF (cell leakage)
   2. Row hammer-based DRAM PUF
3. The response of a DRAM PUF is noisy due to static and dynamic noise sources
4. DRAM PUF response has low entropy and not suitable for generating cryptographic key by itself
5. The DRAM response is very much time-dependent due to leakage

DRAM Architecture

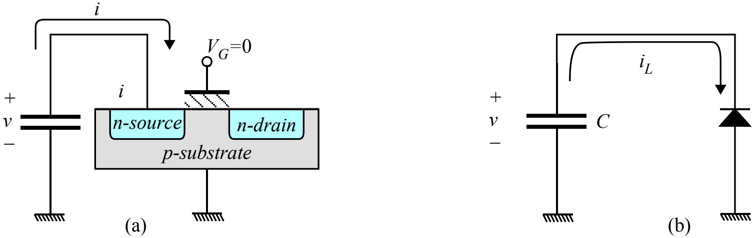
Basic DRAM Structure



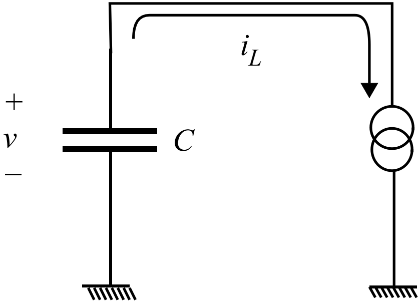
Basic DRAM Cell Structure



DRAM Cell Charge Leakage Model

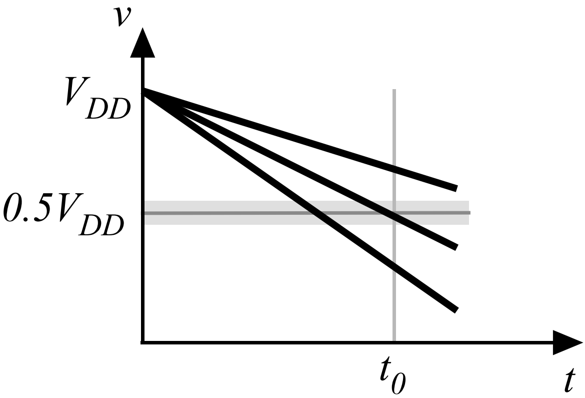


Charge Leakage Equivalent Circuit Model



$$v(t) = V_{DD} - \frac{I_L}{C} \times t$$

Cell Voltage Decay



1. Need to determine t_0
2. Need to design a timing trigger circuit

Setting Up Sampling Strategy

Setting Up Sampling Strategy

1. It is very important to know the correct time t_0 to sample the bit lines of a give word.

2. One approach is to design a timing circuit to sample bit lines at time t_0

3. Another approach is to select a certain reference bit line to sample the voltage value and trigger when this bit line reached the value $0.5V_{DD}$.

4. At any rate, we need to be aware of effects of aging, temperature, supply voltage fluctuations, etc.

DRAM PUF Statistical Model

DRAM PUF Statistical Model

There are two random processes at play here: static and dynamic noise sources.

1. Random process variations (RPV)
2. Random CMOS transistor noise
3. These factors give the device unique, albeit noisy, ID or biometric
4. RPV is static (slowly-varying) and unique to each bit
5. CMOS transistor noise is dynamic and common to all devices

Effect of Random Variations

Digital value of a cell after precharge depends on analog effects:

1. Choice of t_0 and v_r
2. Transistor threshold voltages (V_{th})
3. area of nMOS transistor
4. Parasitic capacitive capacitance
5. Sensitivity of the sense amplifier
6. Parasitic capacitances of the bit lines

Cell Value Probabilities

1. Assume a is probability that a cell has value 1 after sampling trigger
2. Assume $b = 1 - a$ is probability that a cell has value 0 after reset
3. Ideally the sampling v_r and t_0 are chosen so we have

$$a_i = b_i = 0.5$$

RPV as a Biased Gaussian Distribution

$$f_{A_p}(a) = \frac{1}{\sigma_p\sqrt{2\pi}} e^{-(a_p - a_i)^2/2\sigma_p^2}$$

a is our random variable due to RPV with value

$$a_p = G(a_i, \sigma_p)$$

CMOS Noise as a Gaussian Distribution

$$f_N(n) = \frac{1}{\sigma_n\sqrt{2\pi}} e^{-n^2/2\sigma_n^2}$$

n is our random variable due to CMOS noise with value

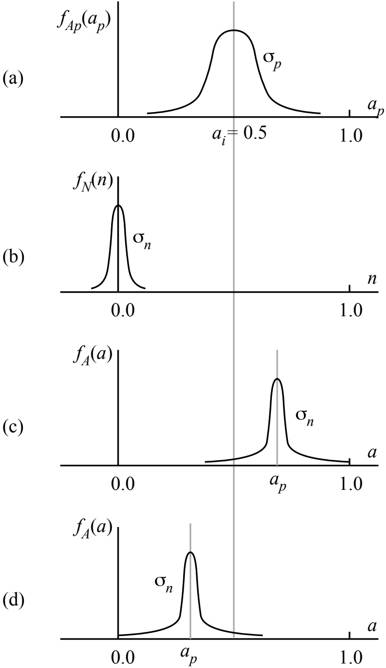
$$n = G(0, \sigma_n)$$

Combining RPV & CMOS Noise

$$f_A(a) = \frac{1}{\sigma_n\sqrt{2\pi}} e^{-(a-a_p)^2/2\sigma_n^2}$$

a is our random variable due to RPV & CMOS noise with value

$$a = G(a_p, \sigma_n)$$


(a)
$f_{Ap}(a_p)$
σ_p
a_p
0.0
$a_i = 0.5$
1.0
(b)
$f_N(n)$
σ_n
n
0.0
1.0
(c)
$f_A(a)$
σ_n
a
0.0
a_p
1.0
(d)
$f_A(a)$
σ_n
a
0.0
a_p
1.0

DRAM PUF Response

Ideal Sampling

Under ideal sampling we would have our reference voltage given by:

$$\frac{V_{DD}}{2} = V_{DD} - \frac{I_0}{C_0} \times t_0$$

where I_0 and C_0 are the ideal values without RPV or noise. In other words we can write

$$t_0 = \frac{V_{DD}}{2} \times \frac{C_0}{I_0}$$

Decay Model in Presence of Noise

We can write actual values of I_L and C as:

$$I_L = I_0(1 + \alpha_p + \alpha_n) \qquad C = C_0(1 + \beta_p + \beta_n)$$

1. α_p and α_n are the effects on leakage current due to RPV and CMOS noise.

2. Similar definitions for β_p and β_n

Decay Voltage Model

At ideal sampling time, we can write $v(t_0)$ in the form

$$\begin{aligned} v(t = t_0) &= V_{DD} - \frac{I_L}{C} \times \frac{V_{DD}}{2} \times \frac{C_0}{I_0} \\ &= V_{DD} - \frac{V_{DD}}{2} \times \frac{1 + \alpha_p + \alpha_n}{1 + \beta_p + \beta_n} \end{aligned}$$

In absence of any noise, $v(t_0) = V_{DD}/2$, as expected.

Signal-to-Noise Ratio (SNR) for DRAM PUF

Signal-to-Noise Ratio (SNR) for DRAM PUF

1. When $a_p = a_i$ the SRAM cell value has equal probability of being 1 or 0 and this value totally depends on the effects of CMOS noise ($\Longrightarrow$ low SNR).
2. $a_i < a_p \leq 1$ the SRAM cell value is biased to be 1 with little effects from CMOS noise especially when $a_p \rightarrow 1$.
3. $0 \leq a_p < a_i$ the SRAM cell value is biased to be 0 with little effects from CMOS noise especially when $a_p \rightarrow 0$.

SNR Definition

$$SNR = 10\log\left[\frac{(a_p - a_i)^2 + \sigma_n^2}{\sigma_n^2}\right]$$

Minimum SNR: $a_p = 0.5$

$$\begin{aligned} SNR_{min} &= 10 \log \left(\frac{\sigma_n^2}{\sigma_n^2} \right) \\ &= 0 \end{aligned}$$

Maximum SNR: $a_p = 0$ or $a_p = 1$

$$SNR_{max} = 10 \log \left(\frac{a_i^2 + \sigma_n^2}{\sigma_n^2} \right)$$