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
SRAM PUF

F. Gebali

EOW 433

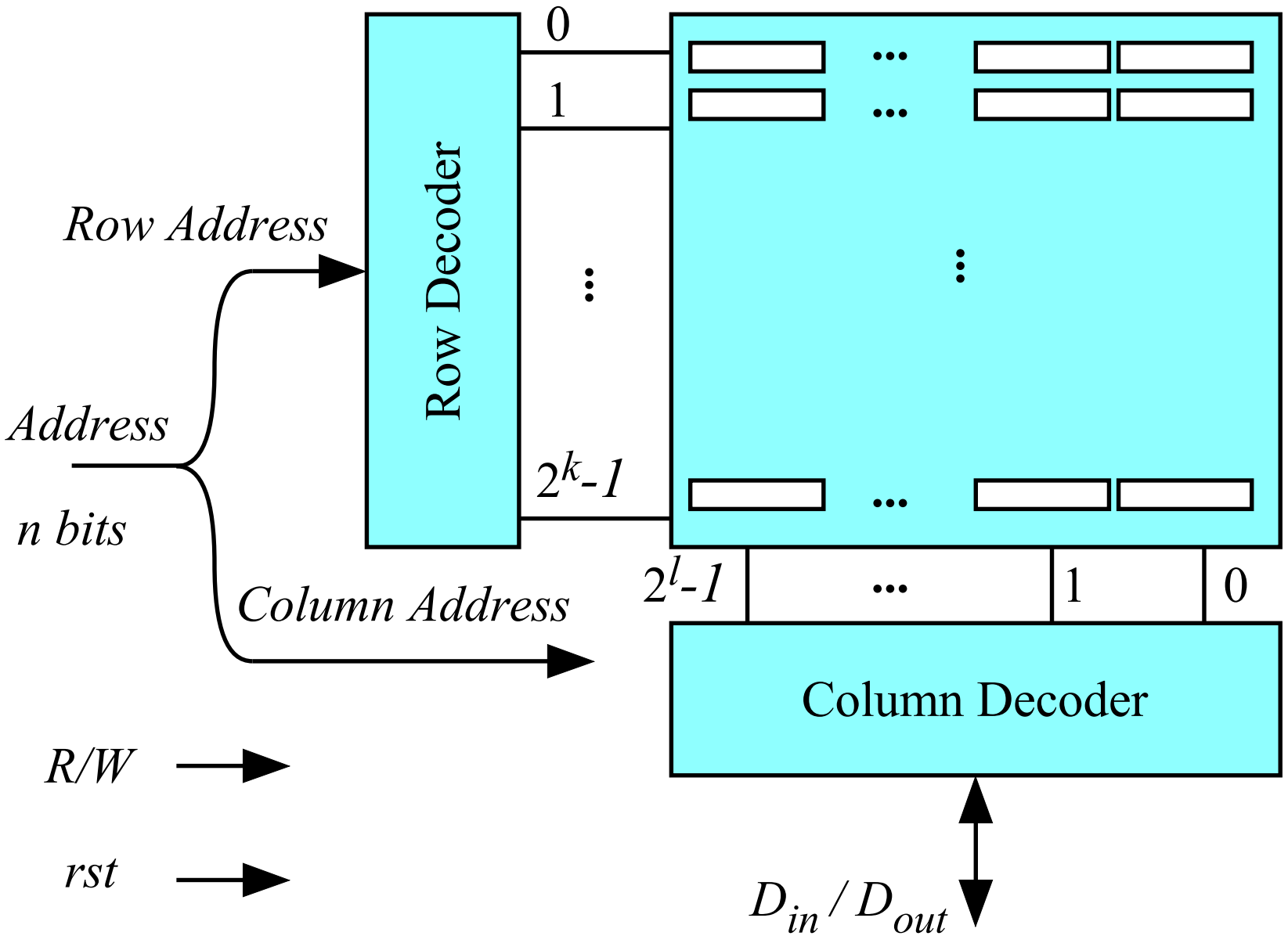
Office Phone: 250-721-6509

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

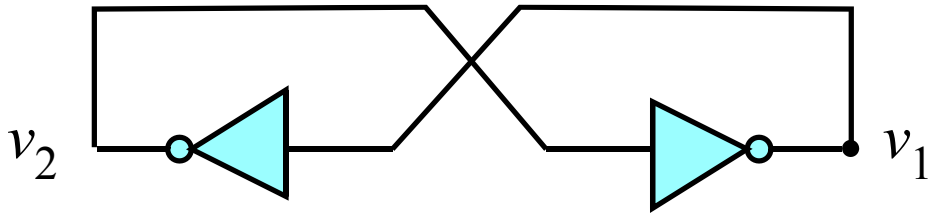
Outline

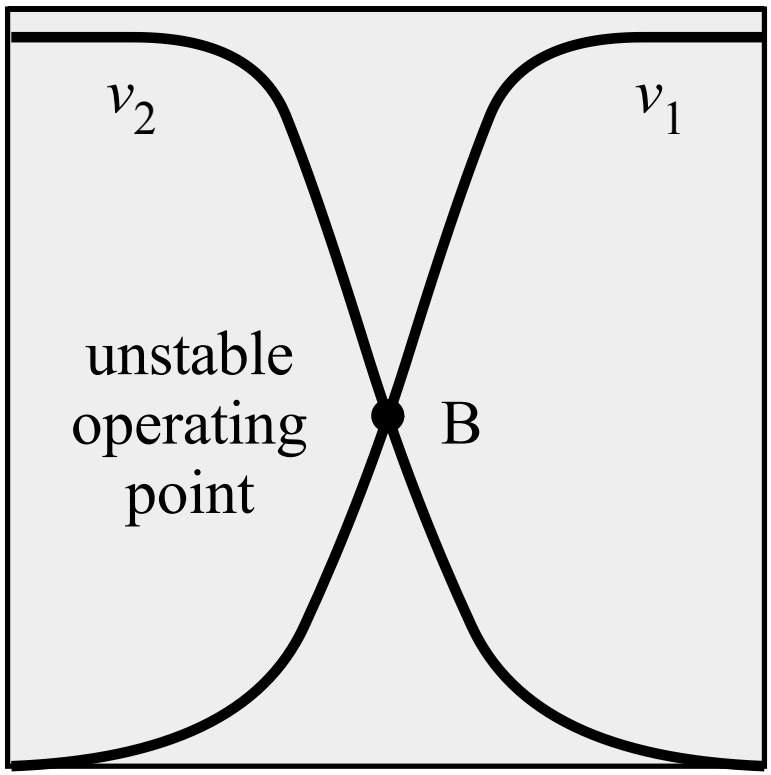
SRAM Architecture

Basic SRAM Structure

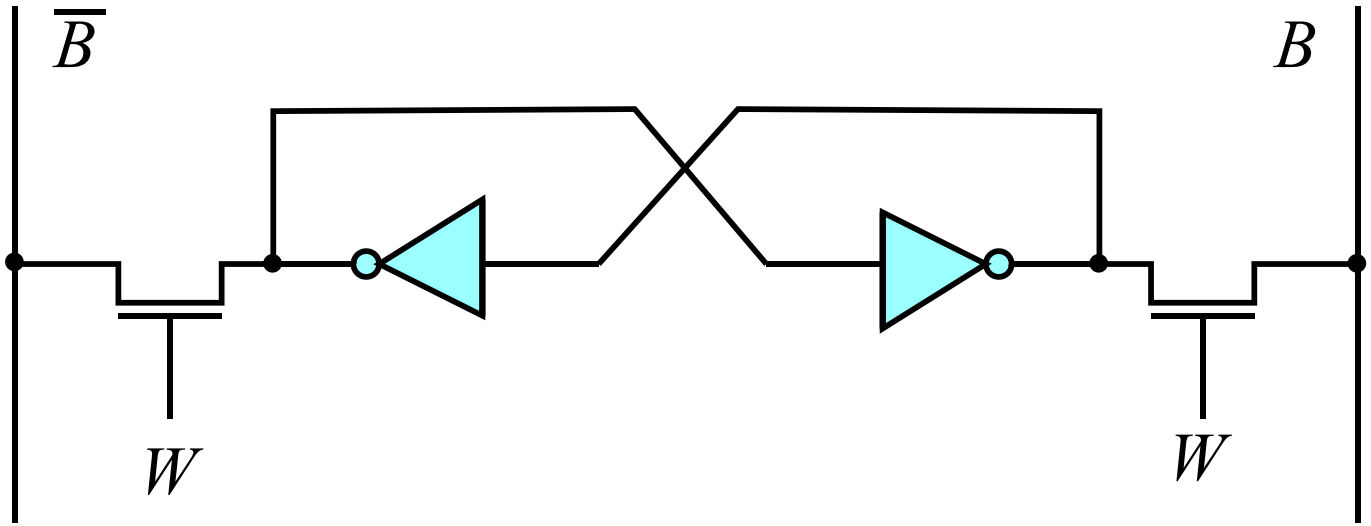


Two Cross-Coupled Inverters

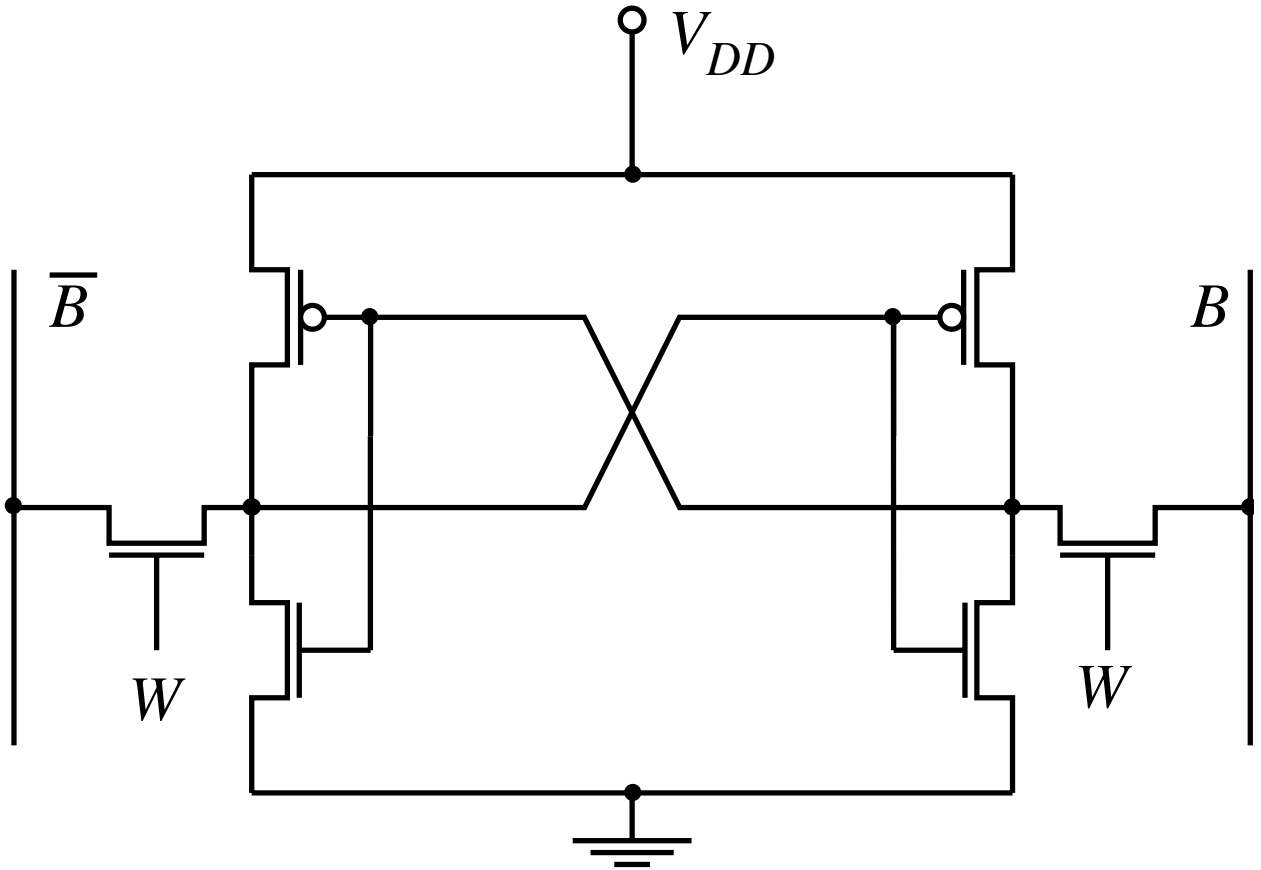




SRAM One-Bit Cell as Two Cross-Coupled Inverters



SRAM 6-Transistor Cell



SRAM PUF

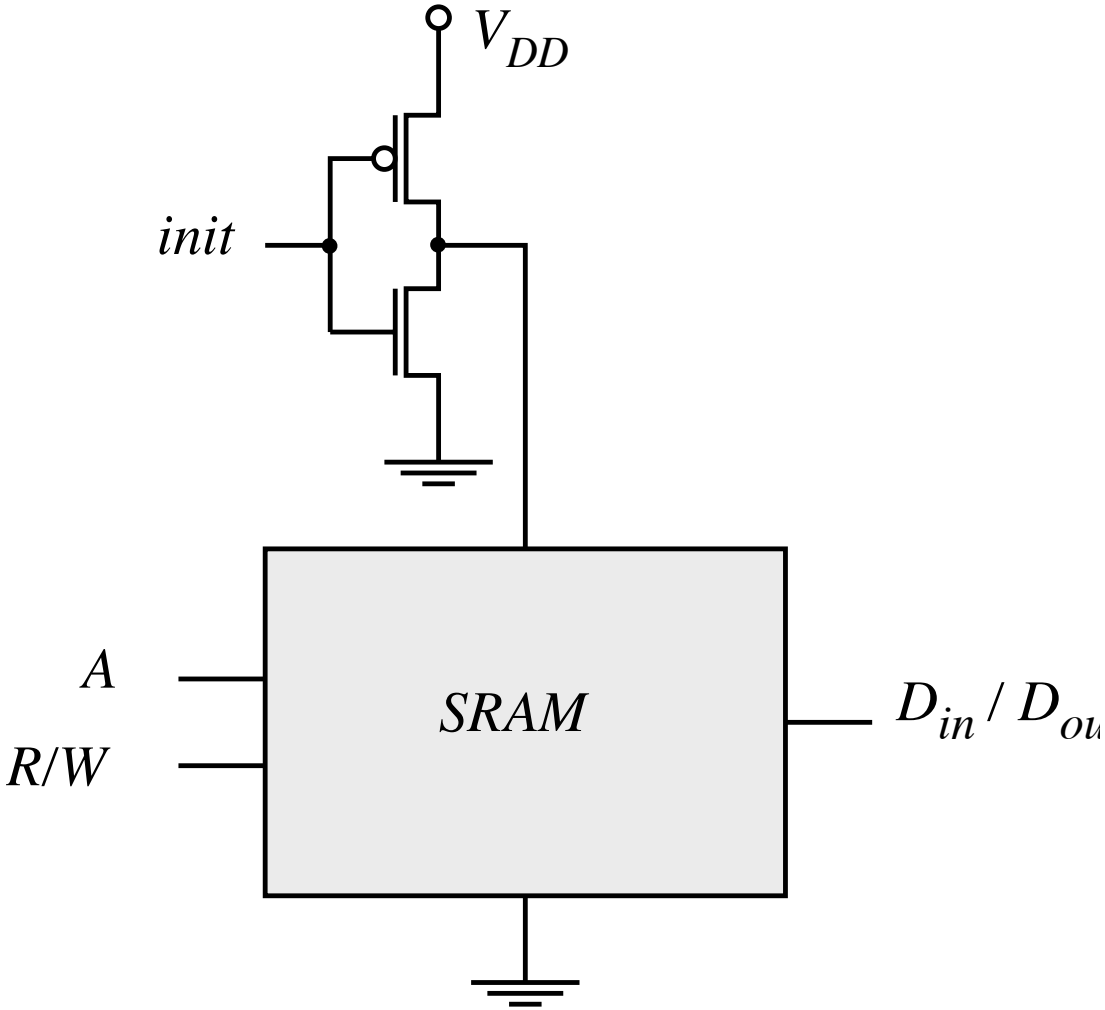
Advantages of SRAM PUF

1. SRAM based on CMOS technology do not require any extra processing steps which makes them practical to implement at no additional costs or delays [1].

2. Area is less than that required by identity stored in nonvolatile memory that need circuits for charge pump.

3. The identity can not be cloned or reverse-engineered. Else ID is destroyed.

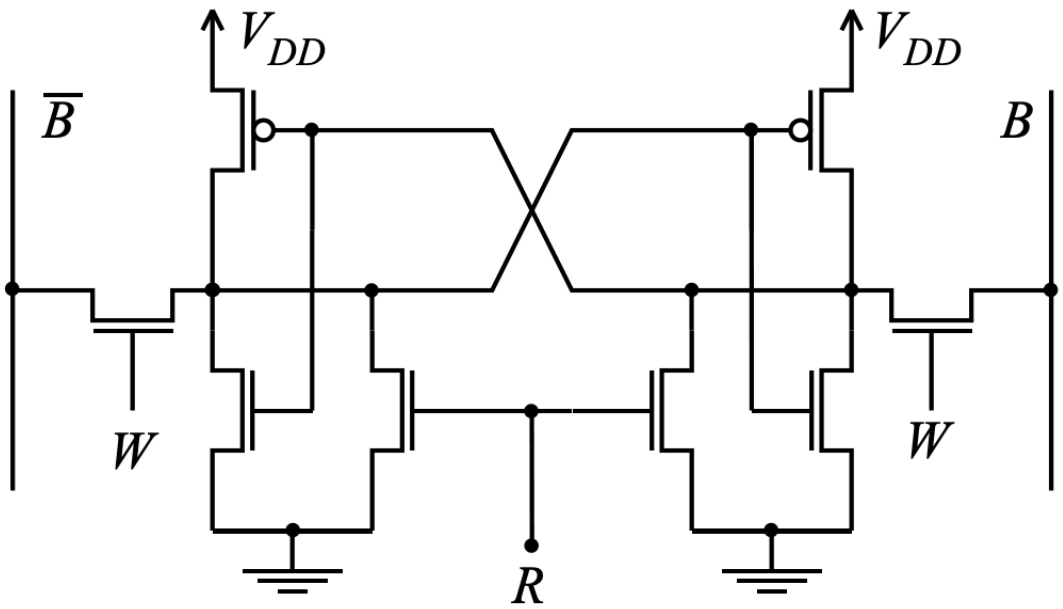
Resetting SRAM PUF: Gated Power Supply



SRAM PUF: Gated Power Supply Limitations

1. Area of inverter powering SRAM could be very large
2. Delay of inverter powering SRAM could be very large

SRAM PUF: Modified Reset Circuitry



1. $R \rightarrow 1$
2. Inverters inputs are 0 (unstable)
3. $R \rightarrow 0$

SRAM PUF Criteria

1. Many CRP must be established to prevent attackers from forging a valid response by observing past activities.
2. Number of bits of B must be "large enough" to be able to establish unique ID of each device.
3. Techniques needed to remove thermal noise from the PUF response.
4. Algorithms needed to extract a high-entropy stable and repeatable secret key from a noisy low-entropy response.

SRAM PUF Statistical Model

SRAM 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 reset depends on analog effects:

1. Transistor threshold voltages (V_{th})
2. Rise and fall times of the inverters
3. Parasitic capacitive loading of inverters
4. Transistor areas affecting speed and current drive ability

Cell Value Probabilities

1. Assume a is probability that a cell has value 1 after reset
2. Assume $b = 1 - a$ is probability that a cell has value 0 after reset
3. Ideally the cell structure is symmetric and 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_p 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

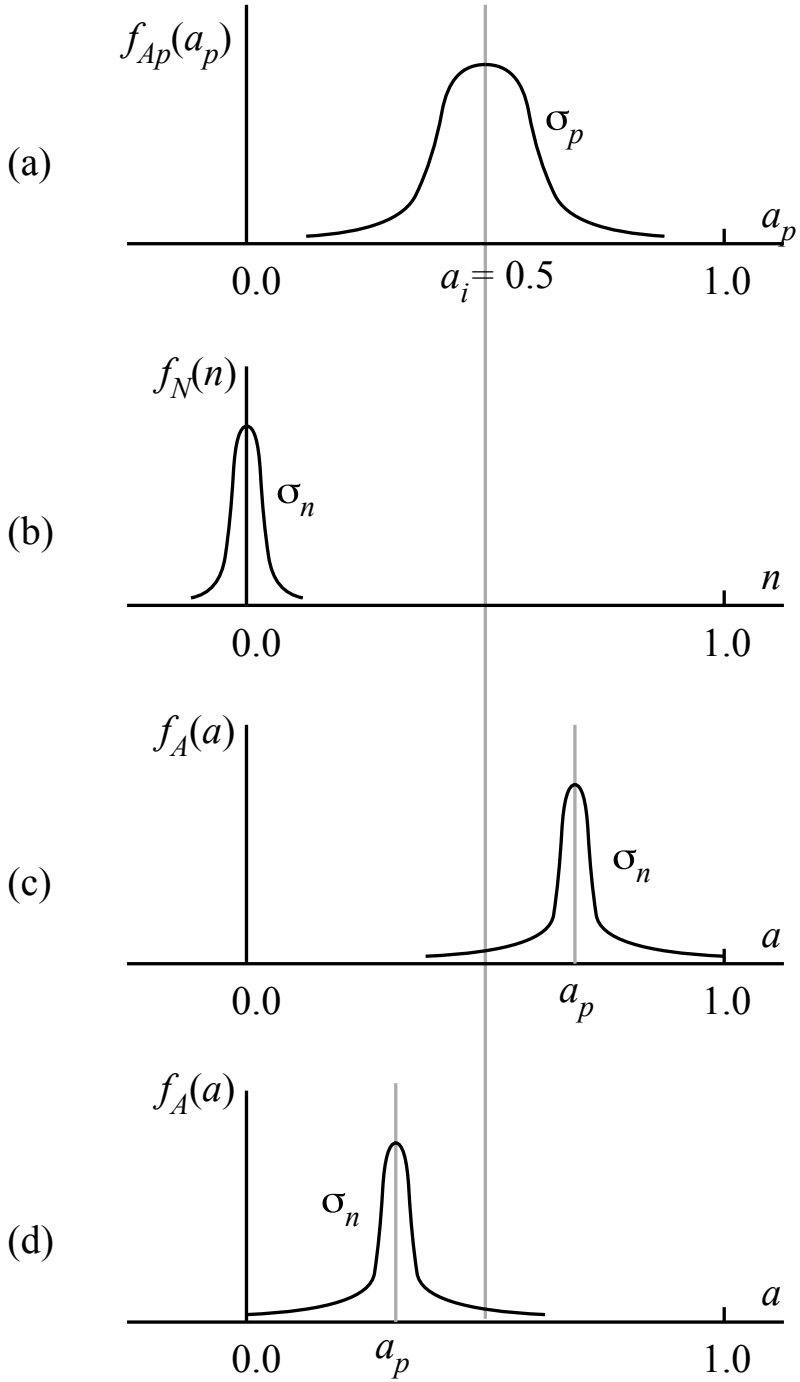
$$n = G(0, \sigma_n)$$

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

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



SRAM Bit Value After Reset

$$v(w,b) = \begin{cases} 0, & 0 \leq a_p(w,b) \leq a_i \\ 1, & a_i < a_p(w,b) \leq 1 \end{cases}$$

1. w is word address
2. b is bit location in a word

Signal-to-Noise Ratio (SNR) for SRAM 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 $a_p \to 1$.

3. $0 \leq a_p < a_i$ the SRAM cell value is biased to be 0 with little effects from CMOS noise especially when $a_p \to 0$.

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 $a_p = 1$

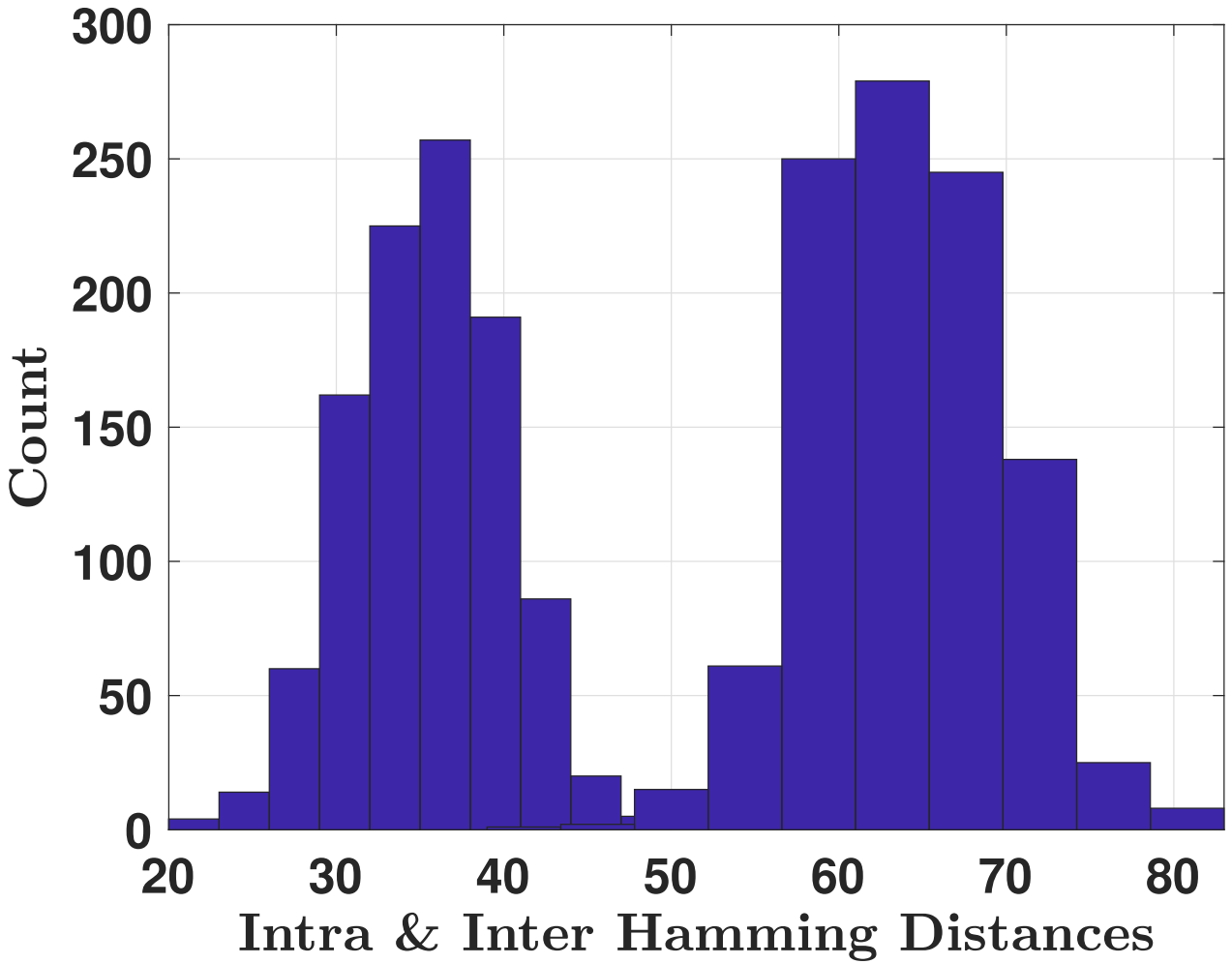
$$SNR_{max} = 10 \log \left[\frac{a_i^2 + \sigma_n^2}{\sigma_n^2} \right]$$

CRP Algorithms

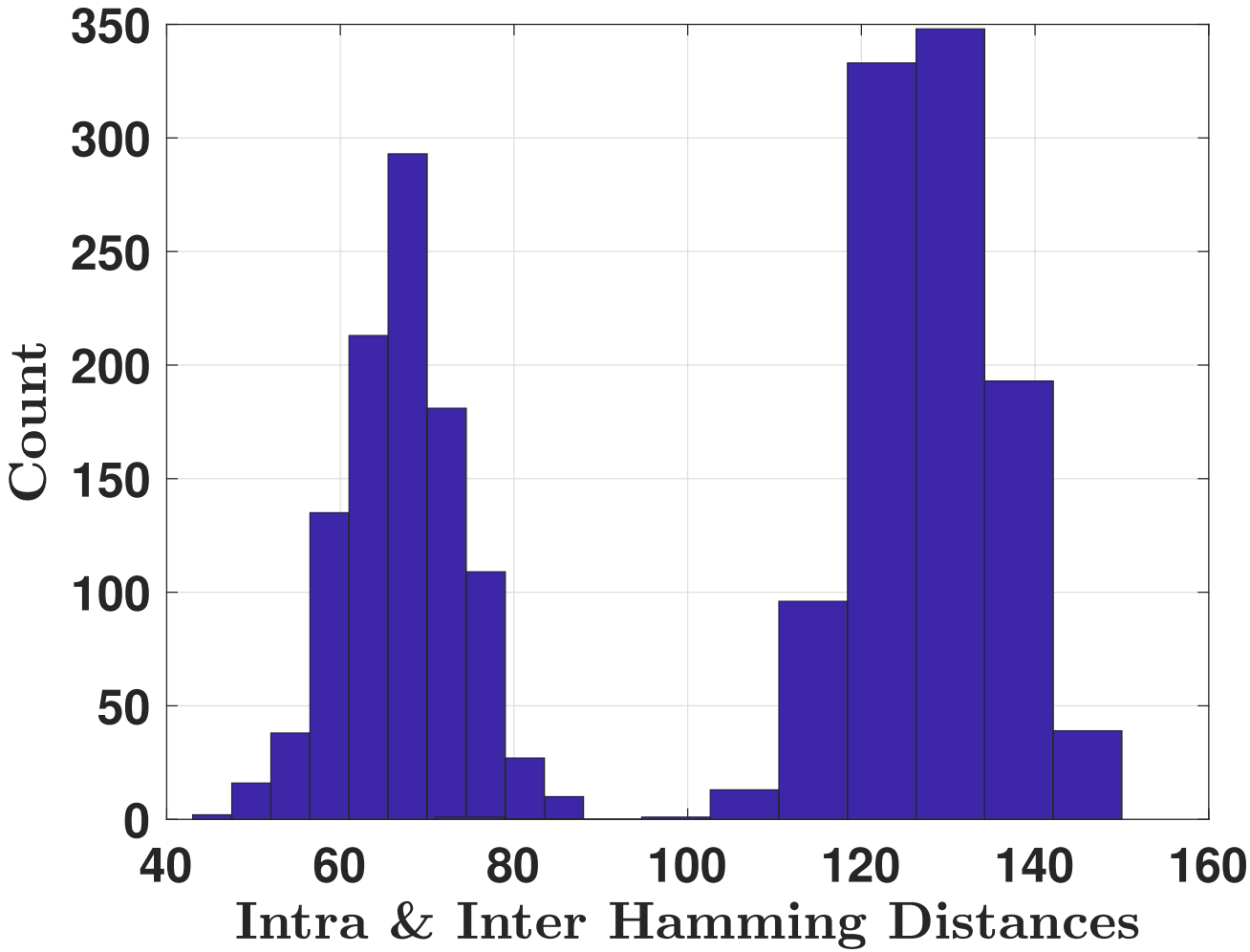
CRP Algorithms: Algorithm

Server	Channel	Client
#1. Select challeng (c)		
#2. Generate r, w, K, h	$\xrightarrow{(c,w)}$	#3. Use (c, w) to generate r_1', K, and h^*
#4. Verify $h^* = h$	$\xleftarrow{h^*}$	

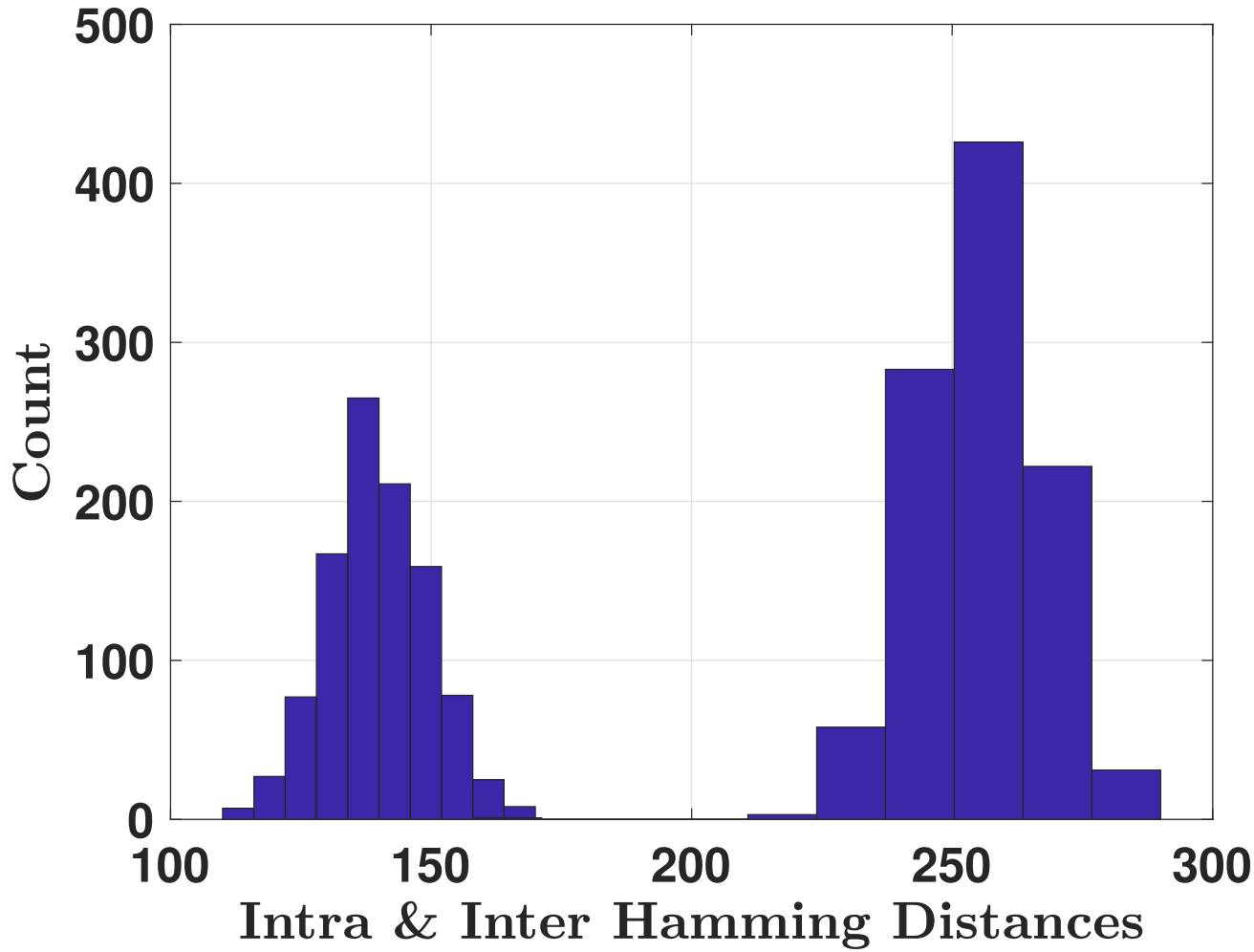
Simulation Case 1: $W = 1$K words, $B = 128$ bits, $N = 1024$ initialization operations and $SNR_{max} = 20$ dB



Simulation Case 2: $W = 1$K words, $B = 256$ bits, $N = 1024$ initialization operations and $SNR_{max} = 20$ dB



Simulation Case 2: $W = 1$K words, $B = 0.5$K bits, $N = 1024$ initialization operations and $SNR_{max} = 20$ dB



[1] D. E. Holcomb, W. P. Burleson, and K. Fu, “Power-up sram state as an identifying fingerprint and source of true random numbers,” *IEEE Transactions on Computers*, vol. 58, no. 9, Sep. 2009.