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

Ring Oscillator PUF

Dr. F. Gebali

Outline

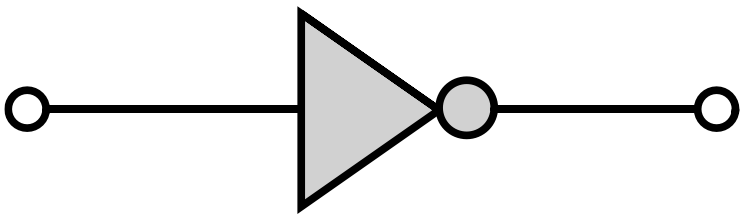
1 RO

2 Model

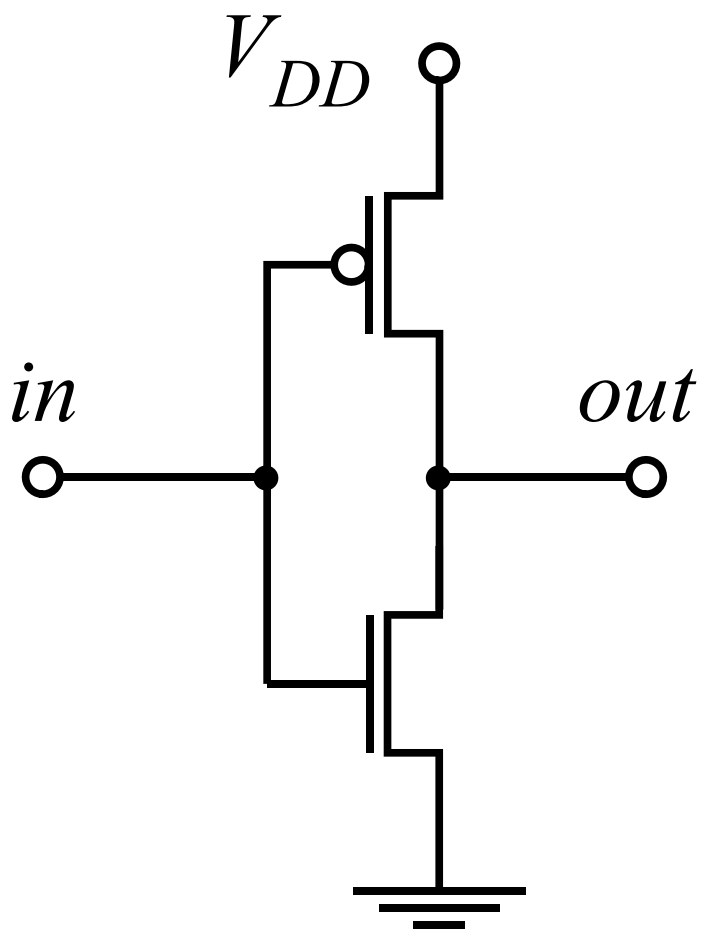
3 RO Sys

Ring Oscillator Architecture

Basic Inverter Structure

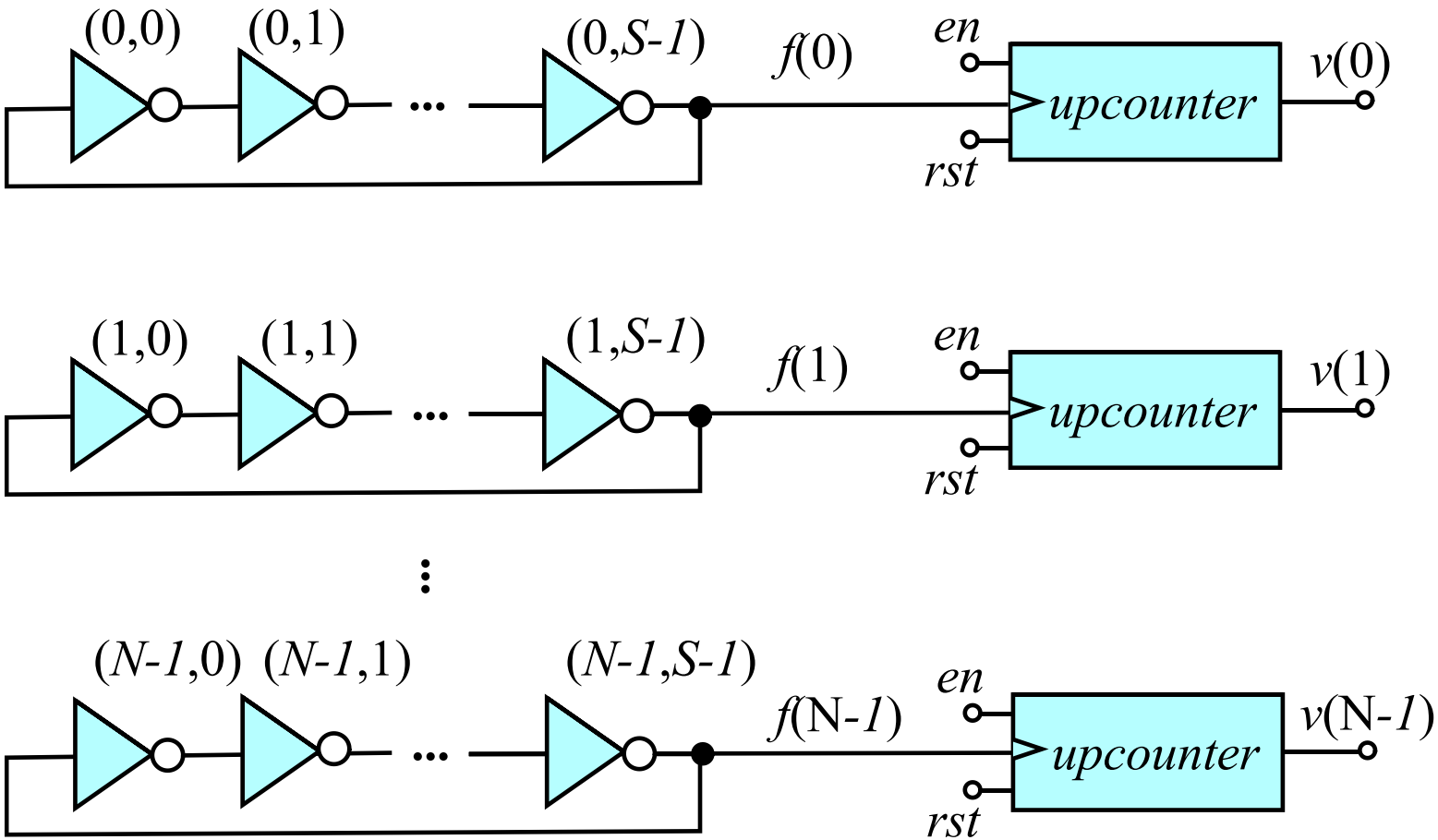


Circuit Symbol

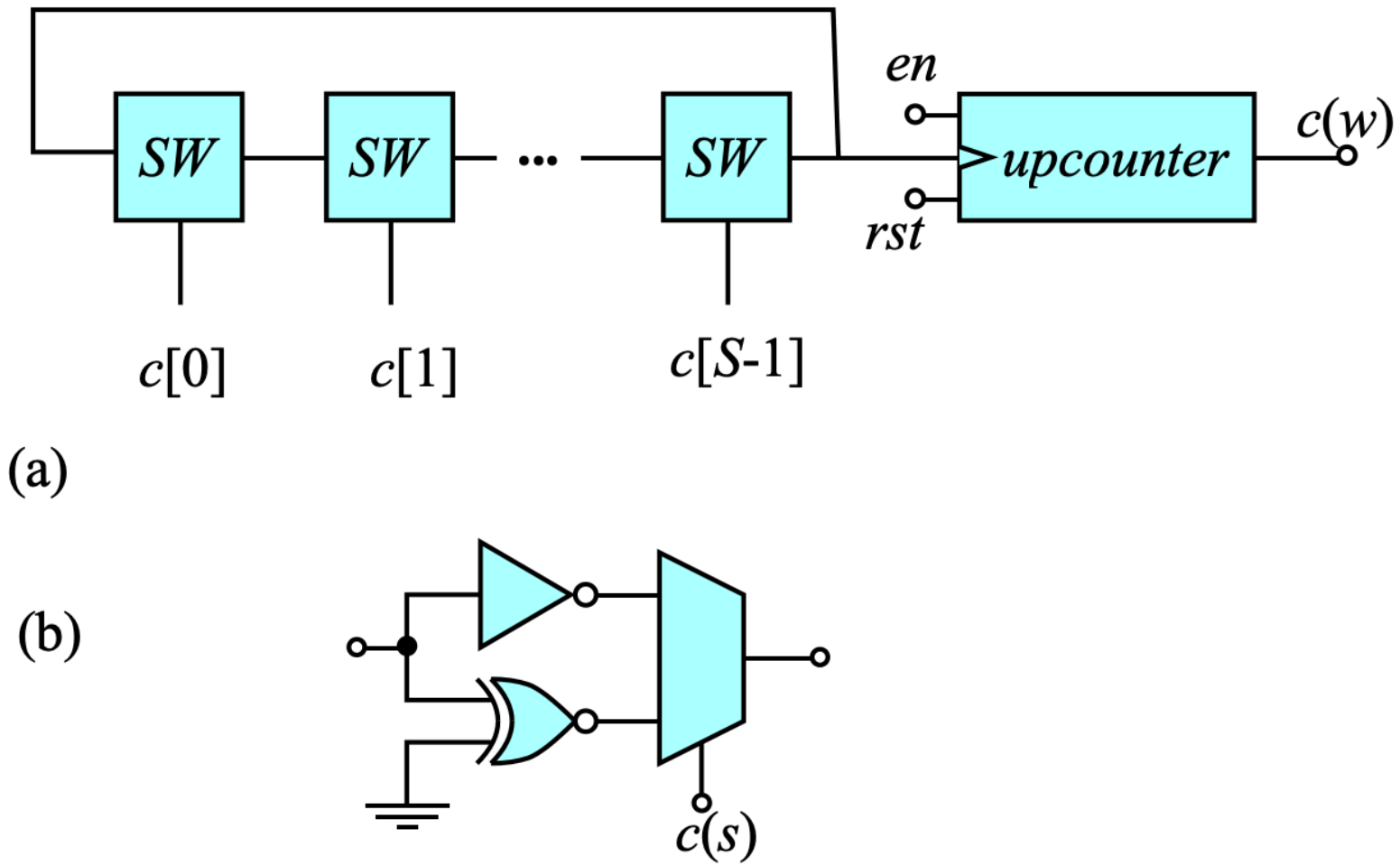


Circuit Diagram

Ring Oscillator PUF



Configurable Galois Ring Oscillator PUF



RO Oscillation Frequency

$$
\begin{aligned}
c &= \lfloor T_{obs}\, f \rfloor && \text{number of oscillations} \\
&= \left\lfloor \frac{T_{obs}}{2T} \right\rfloor \\
f &= \frac{1}{2T}\ \text{Hz} && \text{oscillation frequency} \\
T &= \sum_{s=0}^{S-1} \tau && \text{Total gate delay}
\end{aligned}
$$

RO Encoding

1. Choose a row to serve as reference counter c_r
2. Choose B other rows to obtain the B-bit response
3. For row i we quantize response bit b_i as

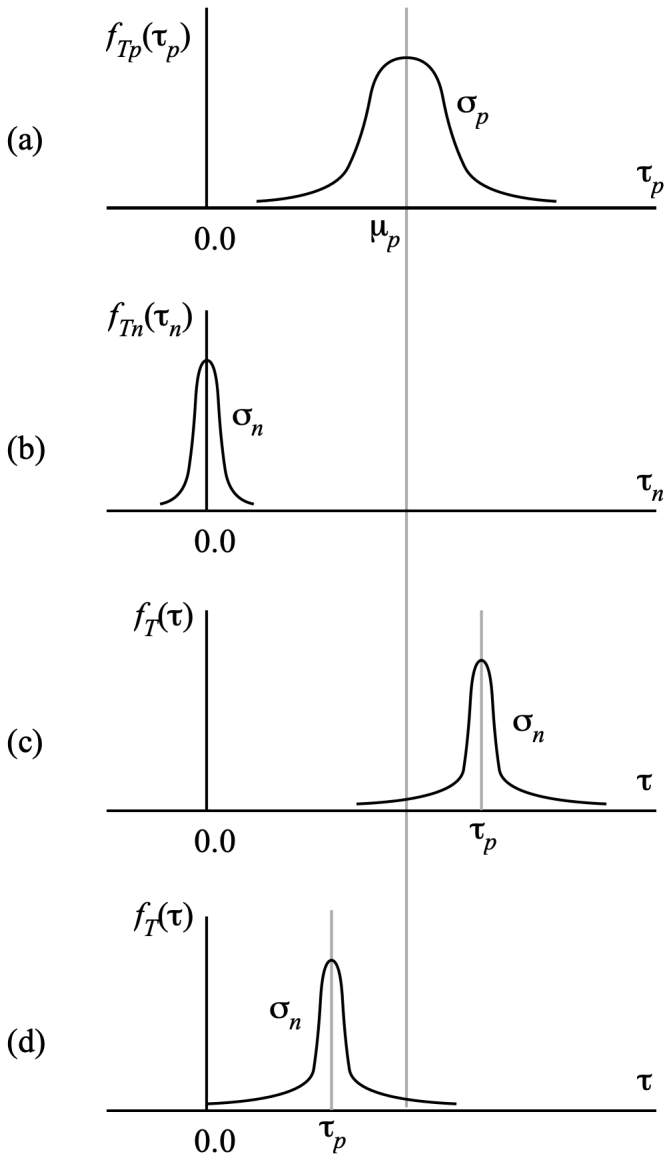
$$b_i = \begin{cases} 0 & \text{when} \quad c_i < c_r \\ 1 & \text{when} \quad c_i \geq c_r \end{cases}$$

Ring Oscillator PUF Statistical Model

Ring Oscillator PUF Statistical Model

1. Ideal delay of an inverter is τ_i
2. Two sources of noise affecting delay:
   1. Slowly-varying random process variations (RPV)
   2. Fast-varying random CMOS noise
3. CMOS noise is due to
   1. Thermal noise represented as an additive white Gaussian noise (AWGN) showing flat spectral distribution
   2. Shot noise due to charge carrier flow across semiconductor junctions showing flat spectral distribution
   3. Flicker noise due to charge trapping centres in the semiconductor bulk showing $1/f$ spectral distribution

RO Statistical Model



RO Authentication

Practical RO Authentication

	Hardware		Server		CA
1	Req (ID)	$\rightarrow$			
2			Req(ID)	$\rightarrow$	
3				$\leftarrow$	$\{c, r\}$
4			select c		
5			$w = \text{FEC}(r)$		
6			$h = \text{HASH}(r)$		
7		$\leftarrow$	$m = \{c,\ w\}$		
8	$r_1 = \text{PUF}(c)$				
9	$r_2 = \text{Decode}(r_1,\ w)$				
10	$h_2 = \text{HASH}(r_2)$	$\rightarrow$			
11			Compare h & h_2		

Numerical Results: $S = 7$ inverters, $\mu_p = 1$, $\sigma_p = 0.3$, $SNR_{max} = 30$ dB and $B = 128$ bits.