Physically “Unclonable” Functions or Physically hard for yoU to clone Functions PUFs Part III: SRAM

ECE 4156/6156 Hardware-Oriented Security and Trust

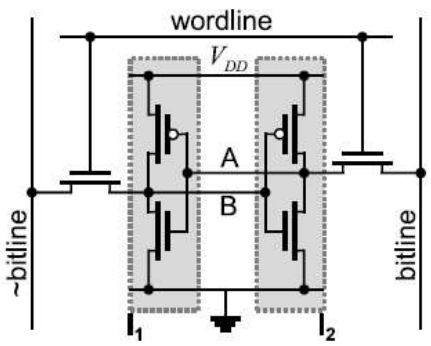
Spring 2024

Assoc. Prof. Vincent John Mooney III

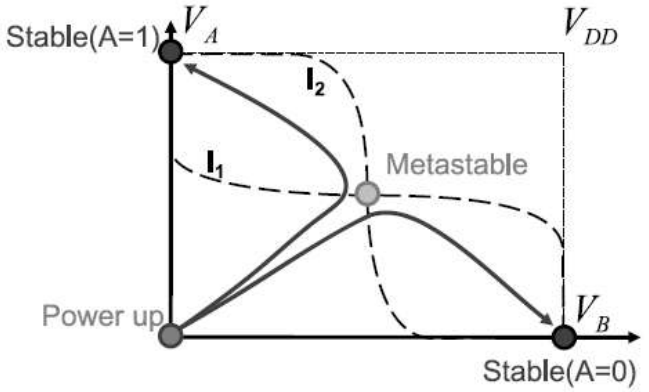
Georgia Institute of Technology

Reading

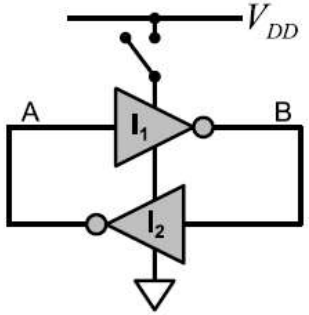
- J. Guajardo, S. Kumar, G. Schrijen and P. Tuyls, “FPGA Intrinsic PUFs and Their Use for IP Protection,” Cryptographic Hardware for Embedded Systems 2007 (CHES 2007), LNCS 4727, 2007, pp. 63-80



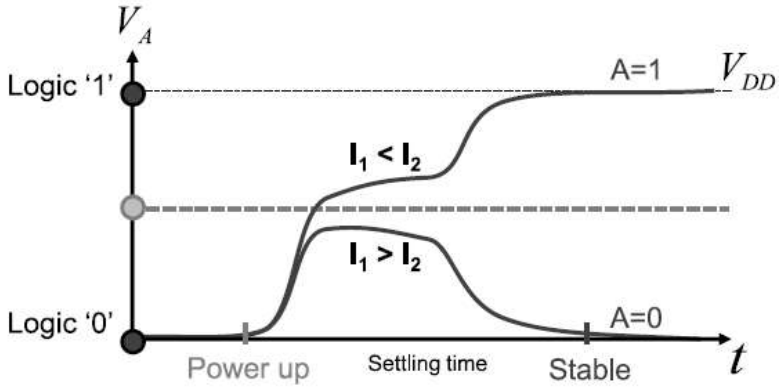
(a) SRAM cell CMOS circuit



(b) SRAM cell voltage transfer curves



(c) SRAM cell logic circuit



(d) SRAM cell power-up transient analysis

Maes **Fig. 2.5** Construction and power-up behavior of an SRAM cell

Key SRAM PUF Idea

- Upon power up, each SRAM bit settles to a one or a zero
- Some SRAM bits will randomly power up to one or zero
  - The main reason is the variation due to temperature and voltage
- Most SRAM bits will nearly deterministically power up to a one or a zero post-manufacture
  - Dopant and other physical variations, e.g., transistor length
- Chip testing can be done to statistically differentiate random versus deterministic SRAM bits

Standard SRAM

- Prior to the concept of an SRAM PUF
  - Power-on-reset
  - Traditionally all bits are set to zero
    - Flip-flops (registers)
    - Memory structures
- Chip initialization sequence may be altered for test

SRAM PUF Enrollment

- Apply statistical tests and error correction
  - Discard (mask out) bits which appear to be nondeterministic upon power up
  - Error correction can result in 128 bits with arbitrarily high reliability
  - Use the obscurity of the above to avoid brute-force attacks with other than a negligible probability of success
    - Analogy: use of a small password but lock up after 10 (or less, e.g., seven or three) guesses

Known Problems

- Aging effects
  - SRAM bit values upon power up may vary slightly (or a lot!) over time
    - Movement of atoms
    - Damage due to heat
- Bit correlations
  - Dopant and other manufacturing variations may be spatially correlated

Statistics

- To be covered later