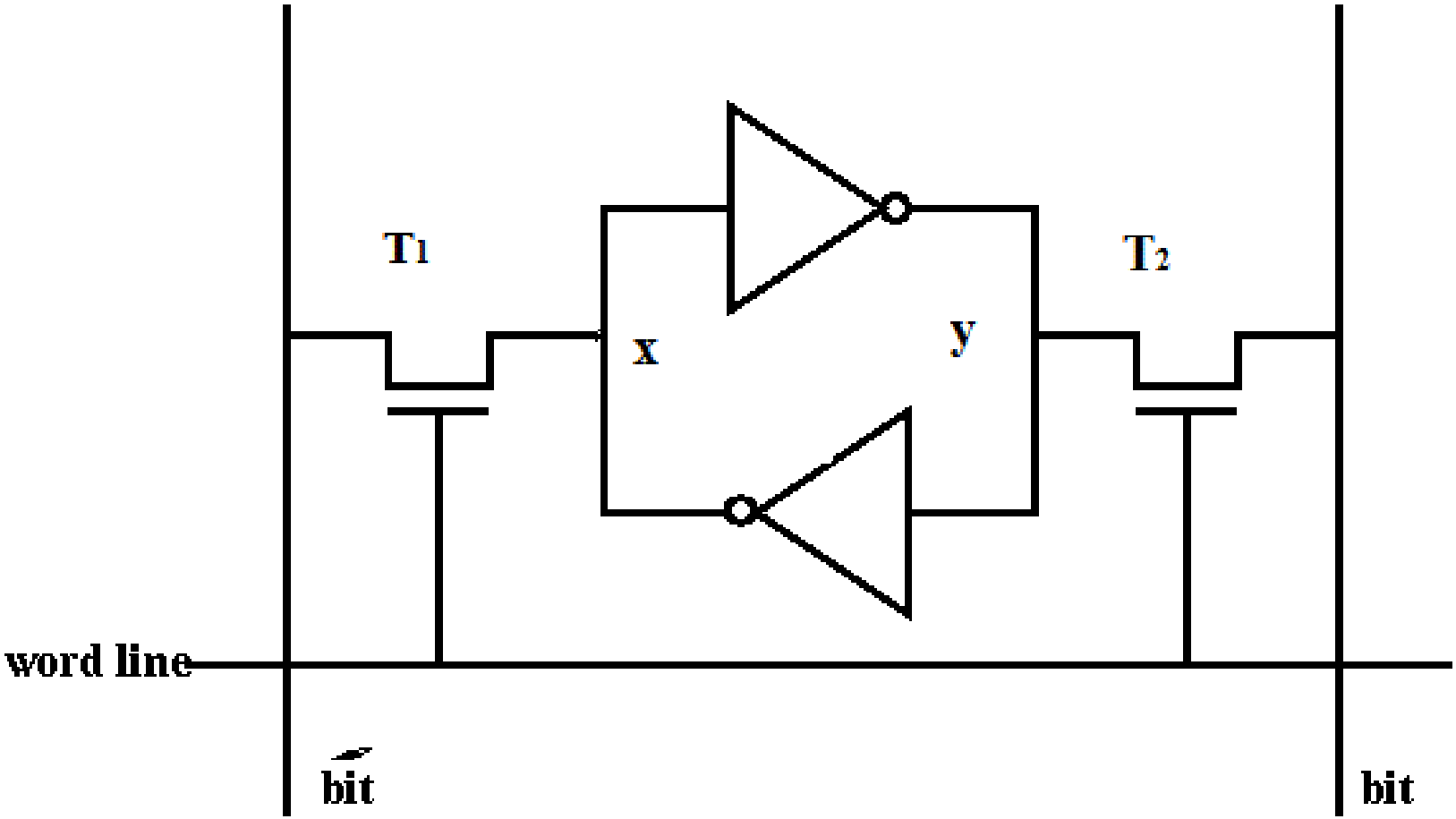
Systems Security: Hardware, embedded system and IoT security Lab

Stjepan Picek
s.picek@tudelft.nl

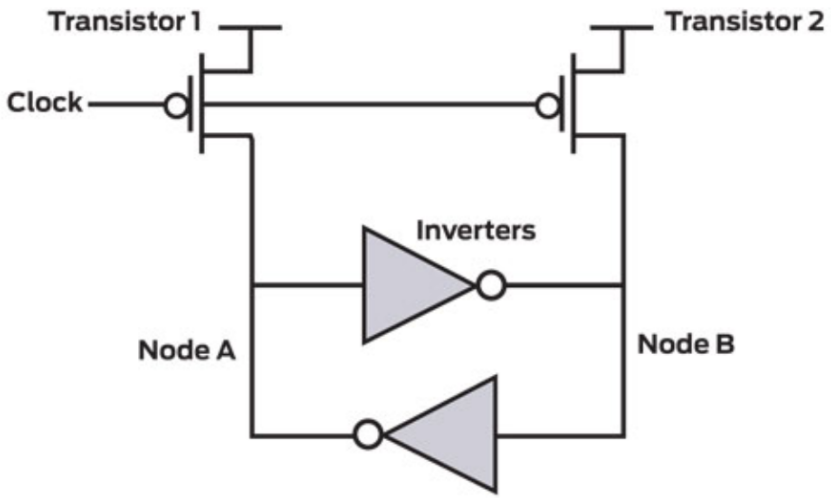
Delft University of Technology, The Netherlands

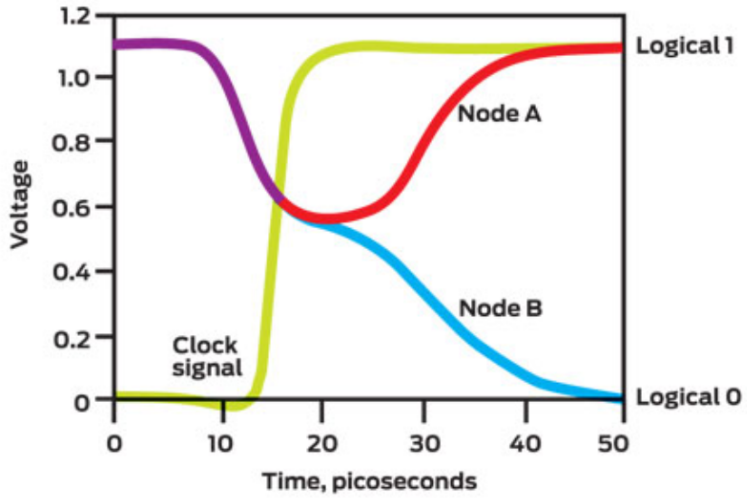
May 3, 2018

SRAM

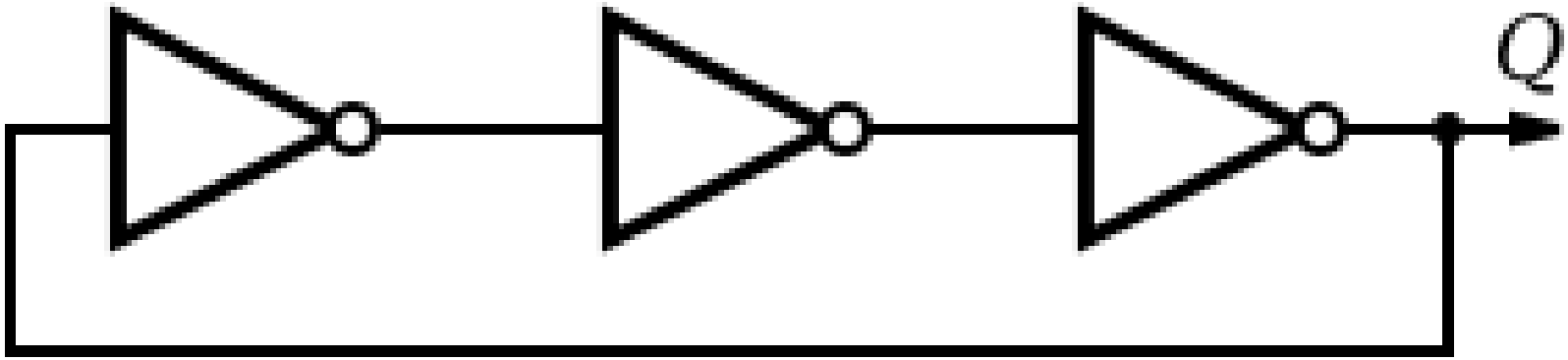


Intels Hardware RNG





Ring Oscillator



- Arbiter PUF consists of one or more chains of two 2-bit multiplexers that have identical layouts.
- Each multiplexer pair is denoted a *stage*, with n stages in a single chain.
- There is a single input signal that is introduced to the first stage to both bottom and top multiplexer in the pair.
- The chain is fed a control signal of n bits called a challenge, where each bit determines whether the two input signals in that stage would be switched (crossed over) or not.
- In ideal conditions, the input signal would propagate at the same speed through each stage and both the lower and upper signal would arrive at the arbiter at the same time.

- Due to the manufacturing inconsistencies, the delay of each multiplexer is slightly different, and the top and bottom input signals are not synchronized.
- The arbiter at the end of the chain determines which signal arrived earlier and thus forms the response (0 or 1).
- The response of a PUF is determined by the delay difference between the top and bottom input signal, which is in turn the sum of delay differences of the individual stages.
- To efficiently model a PUF, one usually tries to determine the delay vector $w = (w_1, \ldots, w_{n+1})$ which models the delay differences in each stage.

Arbiter PUF

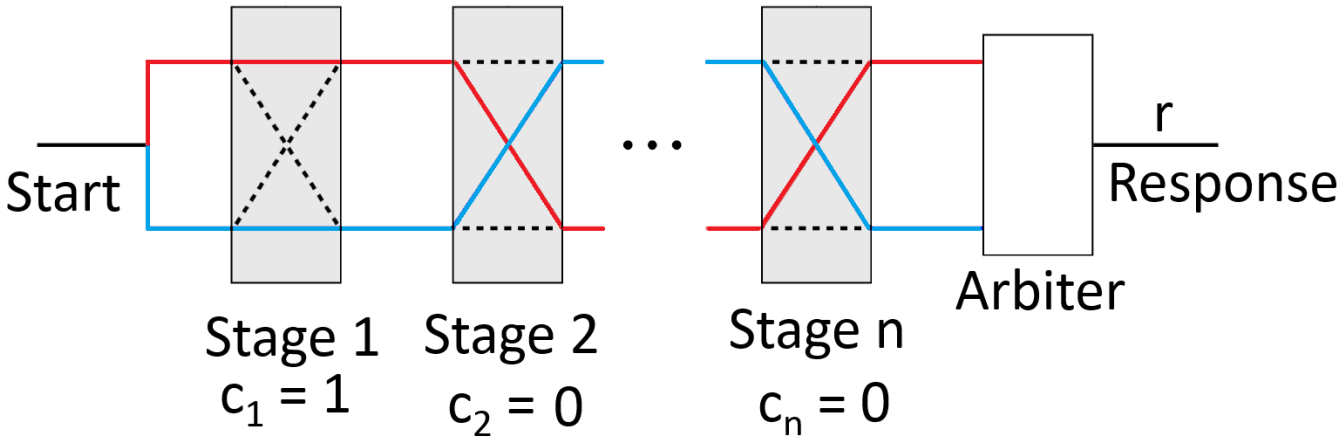


Figure: *n*-bit Arbiter PUF.

Modeling Arbiter PUF

- The idea behind the attack is to model the delay vector $\vec{w}$.

$$\phi_i = \prod_{l=1}^{k} (-1)^{c_l}, \text{for } 1 \leq i \leq k. \tag{1}$$

$$\Delta D = \vec{w}^T \vec{\phi}^T.$$

$$r = \begin{cases} 1 & \text{if } \Delta D < 0 \\ 0 & \text{if } \Delta D > 0 \end{cases}$$

Modeling Arbiter PUF

- The number of stages.
- The number of responses.
- The number of PUFs.
- The level of noise.

Bonus Assignment

- https://security1.win.tue.nl
- Submit the results for phase 1 by June 1st.
- Submit the results for stage 2 by June 25th.
- If you have really good results, win the competition!