UMassAmherst

Security Evaluation and Enhancement of Bistable Ring PUFs

RFIDSec, June 23, 2015

Xiaolin Xu(1), Ulrich Rührmair(2)
Daniel Holcomb(1) and Wayne Burleson(1)
(1) UMass Amherst (2) HGI, U Bochum

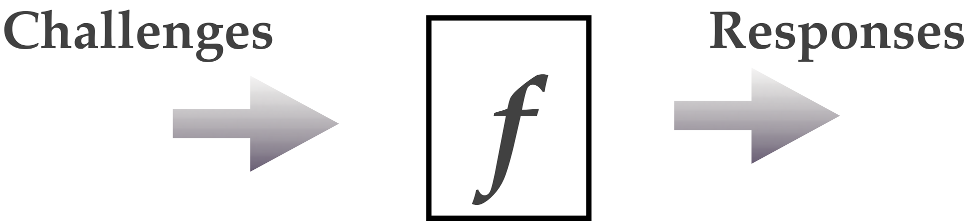
This material is based upon work supported by: NSF CNS-0964641 and SRC task 1836.074
Its contents are solely the responsibility of the authors and do not necessarily represent the official views of SRC or NSF.

Outline

- Background
  - PUFs
  - Modeling attacks on PUFs
  - Bistable Ring PUF
- Security Evaluation of BR PUFs
  - Modeling the BR PUF
  - Results against BR PUF and variants
- Security Enhancement of BR PUFs
  - XORing BR PUFs to enhance the security
  - Impact on other PUF parameters
- Conclusion and future work

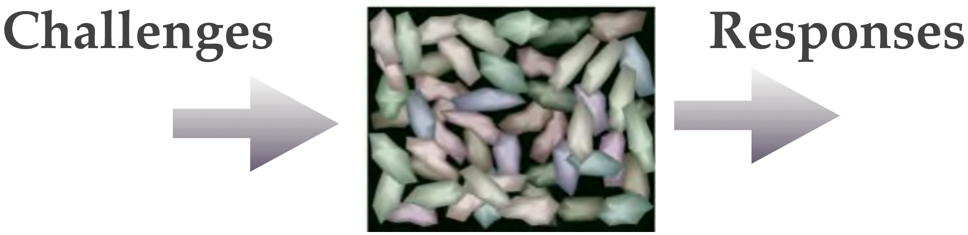
Physical Unclonable Functions

- Map challenges to responses according to physical variations
- Security applications include key storage and authentication



Physical Unclonable Functions

- Map challenges to responses according to physical variations
- Security applications include key storage and authentication



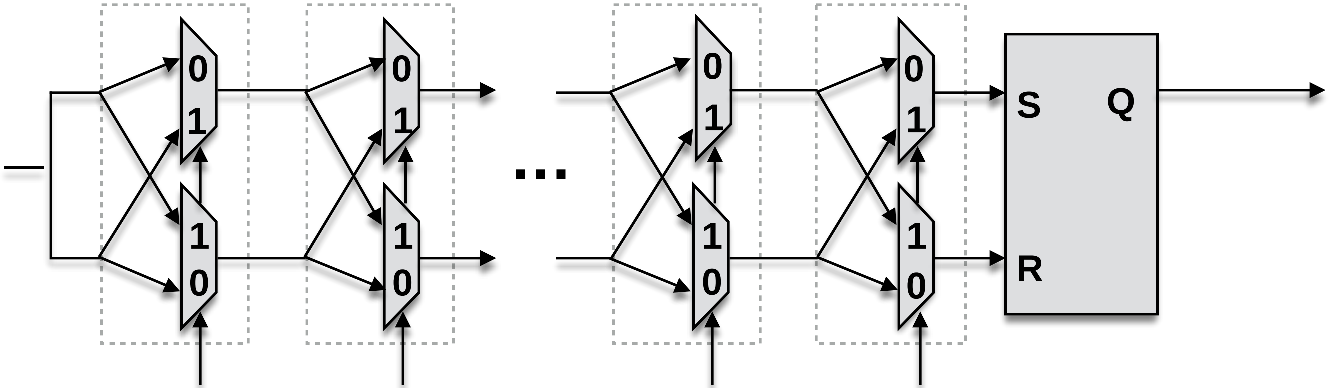
Challenges

Responses

PUF Characterized by Challenge-Response Pairs (CRPs)

- Exponential challenge space
- **Modeling attacks should not be possible**

PUFs and Modeling Attacks



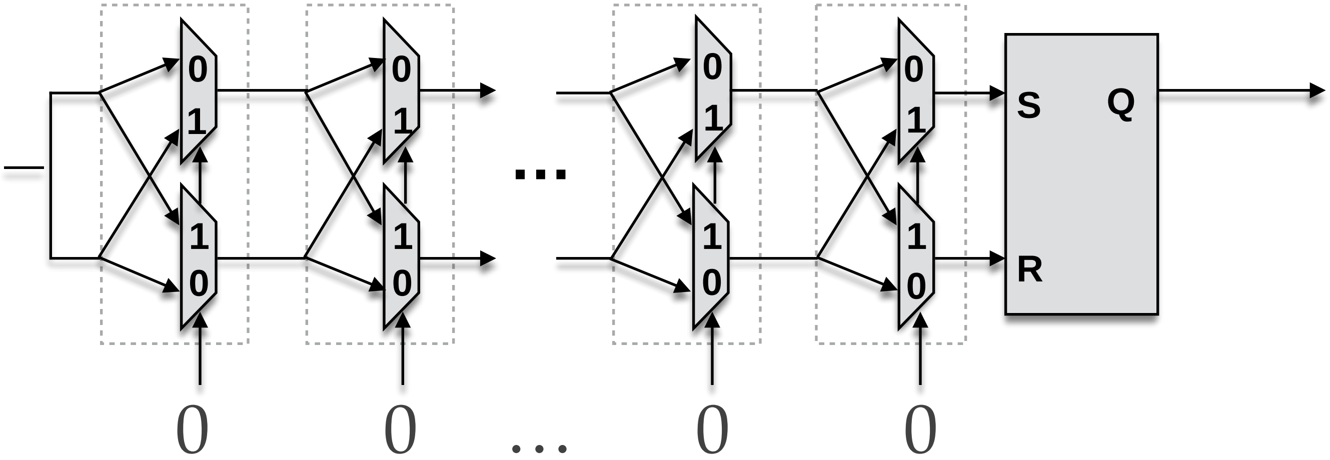
(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013

(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014

(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010

(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks



- Challenges: $C_i \in 2^n$ (n= num stages)

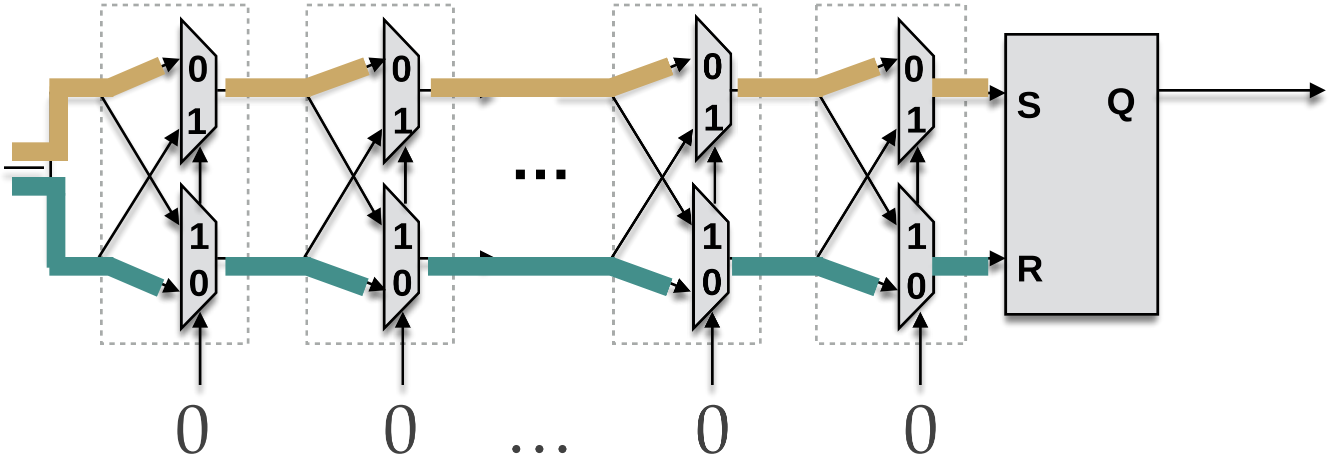
(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013

(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014

(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010

(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

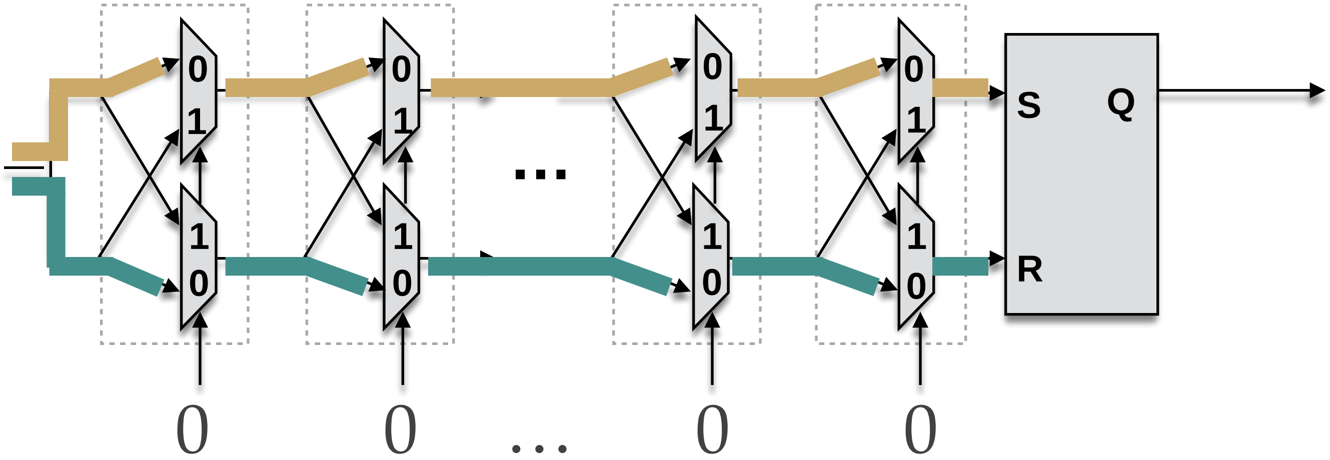
PUFs and Modeling Attacks

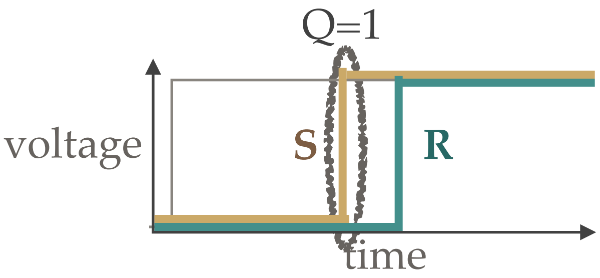


- Challenges: $C_i \in 2^n$ (n= num stages)

(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013
(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014
(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010
(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks

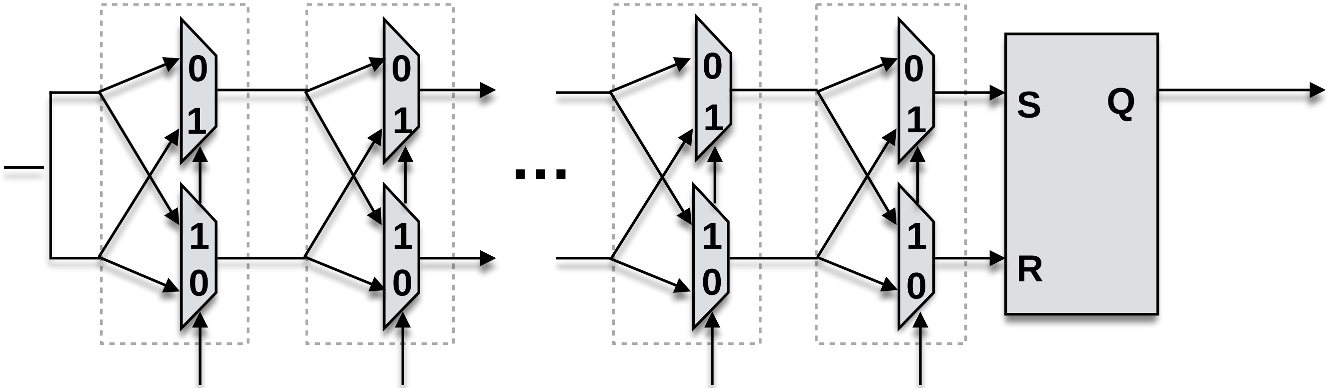


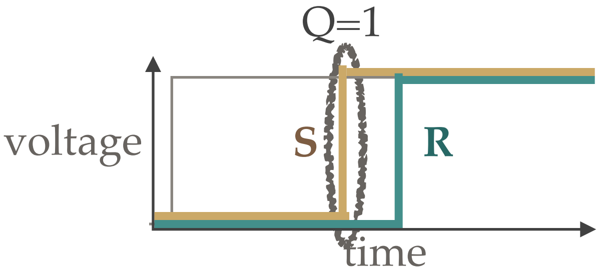


- Challenges: $C_i \in 2^n$ (n= num stages)
- Responses: $r_i \in \{0,1\}$ (n=1 shown)

(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013
(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014
(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010
(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks

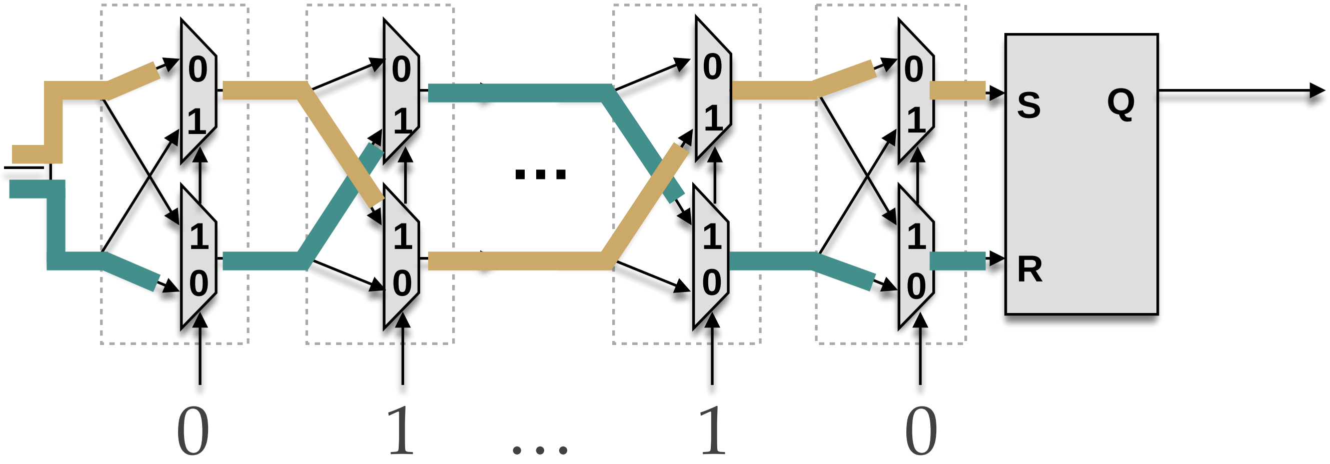


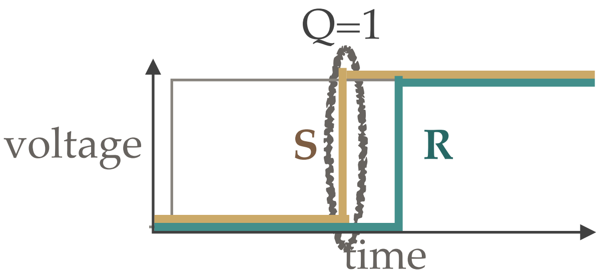


- Challenges: $C_i \in 2^n$ (n= num stages)
- Responses: $r_i \in \{0,1\}$ (n=1 shown)

(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013
(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014
(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010
(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks

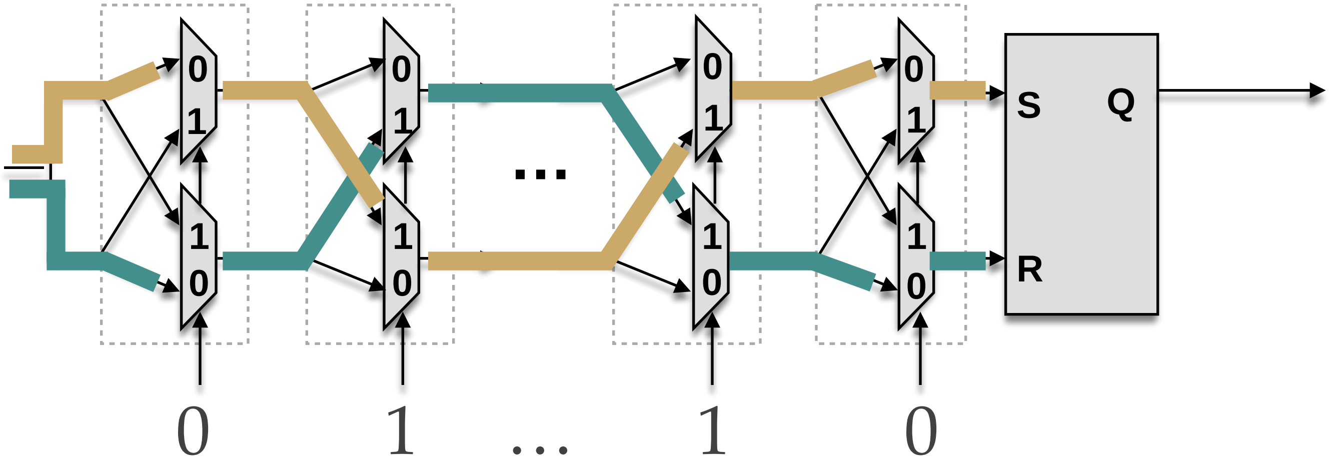




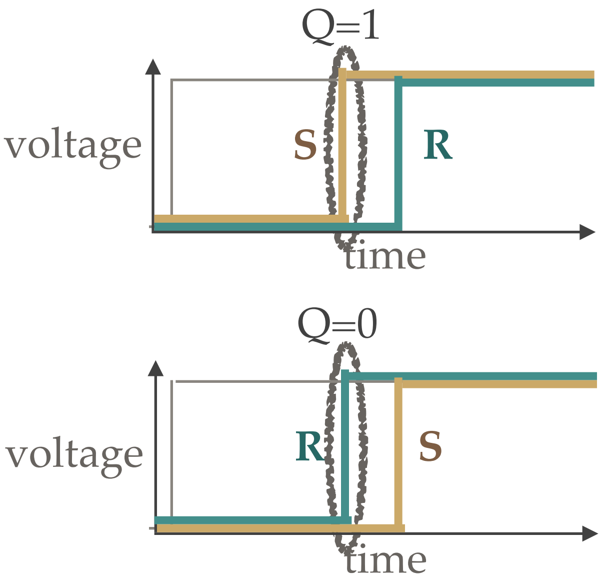
- Challenges: $C_i \in 2^n$ (n= num stages)
- Responses: $r_i \in \{0,1\}$ (n=1 shown)

(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013
(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014
(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010
(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks

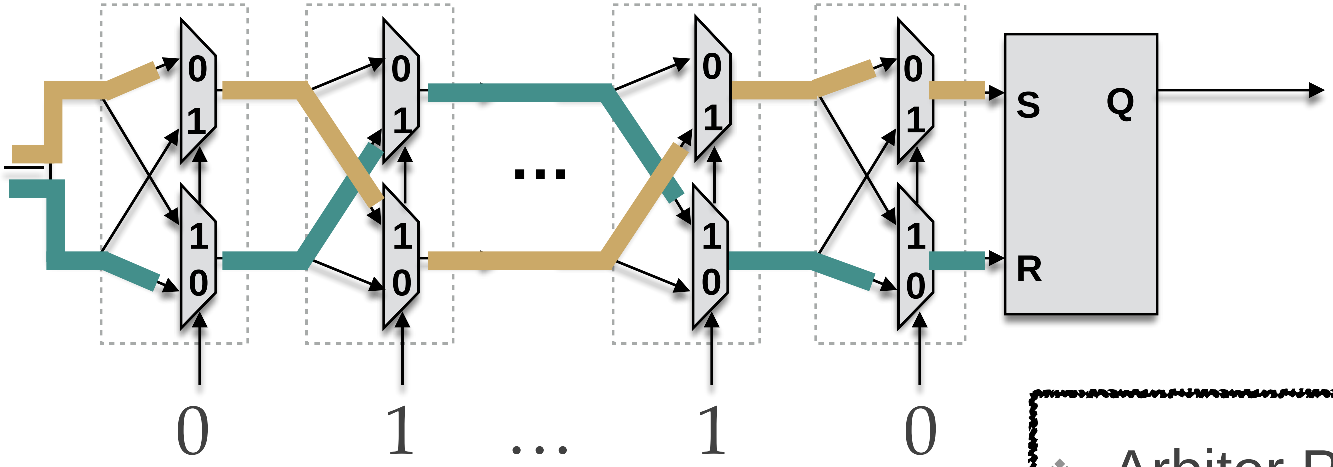


- Challenges: $C_i \in 2^n$ (n= num stages)
- Responses: $r_i \in \{0,1\}$ (n=1 shown)



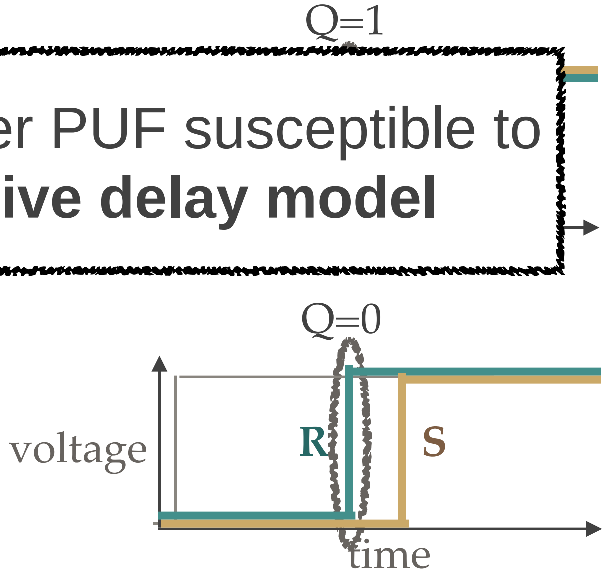
(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013
(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014
(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010
(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks



- Challenges: $C_i \in 2^n$ (n= num stages
- Responses: $r_i \in \{0,1\}$ (n=1 shown)

❖ Arbiter PUF susceptible to **additive delay model**



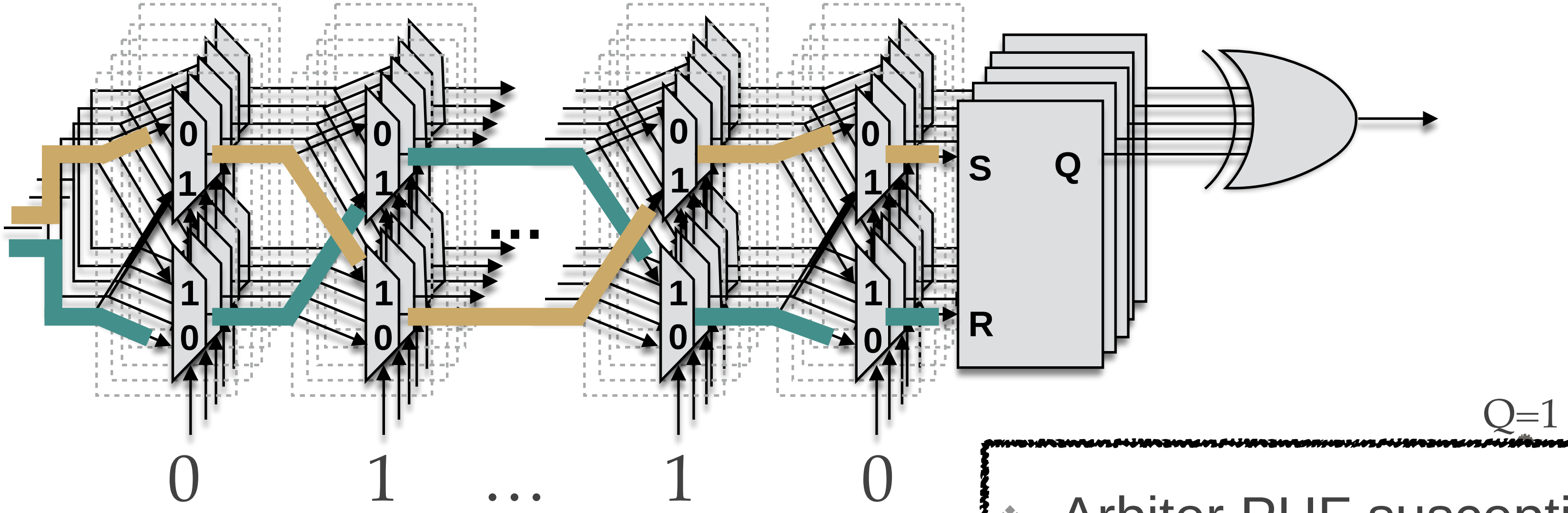
(1) D. Lim. MSc Thesis, MIT, 2004
(2) U. Rührmair, et al, T-IFS, 2013

(3) M. Majzoobi, et al. ICCAD 2008
(4) U. Rührmair, et al, CHES 2014

(5) G. Suh et al. DAC 2007
(6) U. Rührmair, et al, CCS 2010

(7) G. Becker, CHES 2015
(8) Schuster et al., TRUST 2015

PUFs and Modeling Attacks



- Challenges: $C_i \in 2^n$ (n= num stages
- Responses: $r_i \in \{0,1\}$ (n=1 shown)

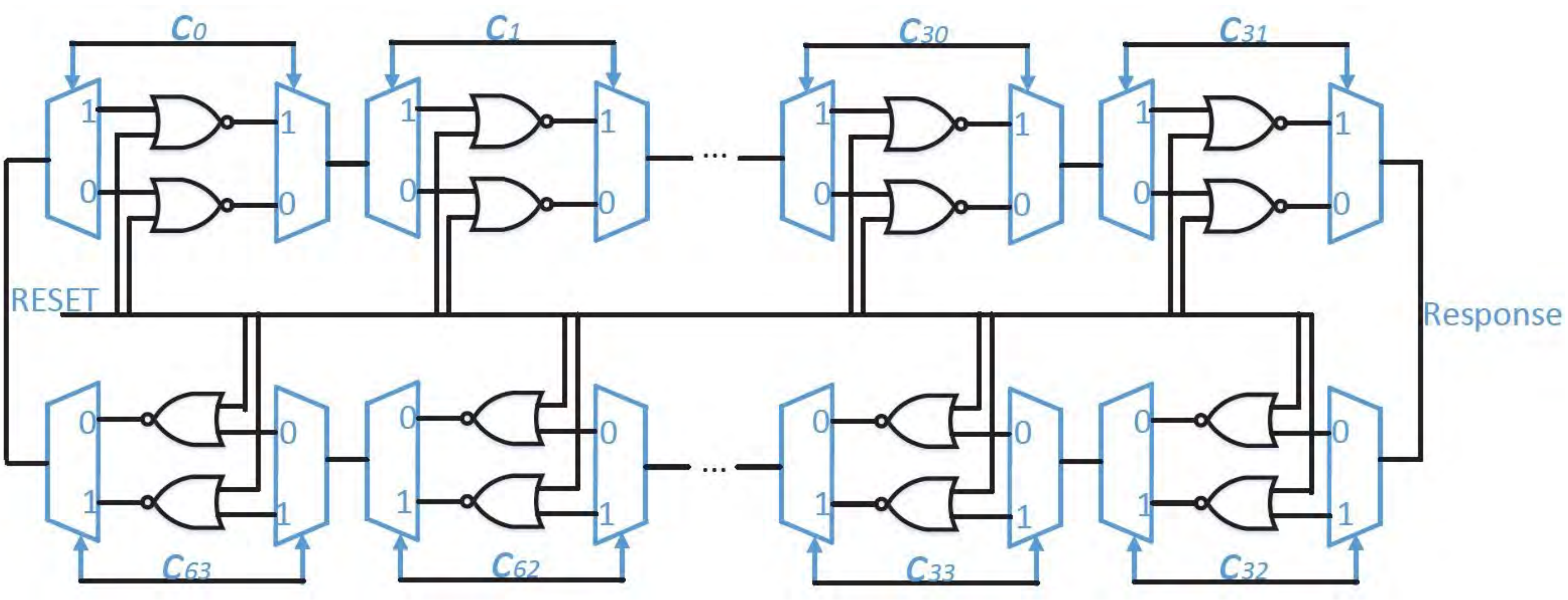
- Arbiter PUF susceptible to **additive delay model**

- Arms race of designs versus attacks ongoing….
- XOR PUF[5], Lightweight PUF[3]
- SVM[1], Evolutionary Strategies[6], Logistic Regression[6], ANN[8], Hybrid attacks[4]

[1] D. Lim. MSc Thesis, MIT, 2004
[2] U. Rührmair, et al, T-IFS, 2013
[3] M. Majzoobi, et al. ICCAD 2008
[4] U. Rührmair, et al, CHES 2014
[5] G. Suh et al. DAC 2007
[6] U. Rührmair, et al, CCS 2010
[7] G. Becker, CHES 2015
[8] Schuster et al., TRUST 2015

Bistable Ring PUFs

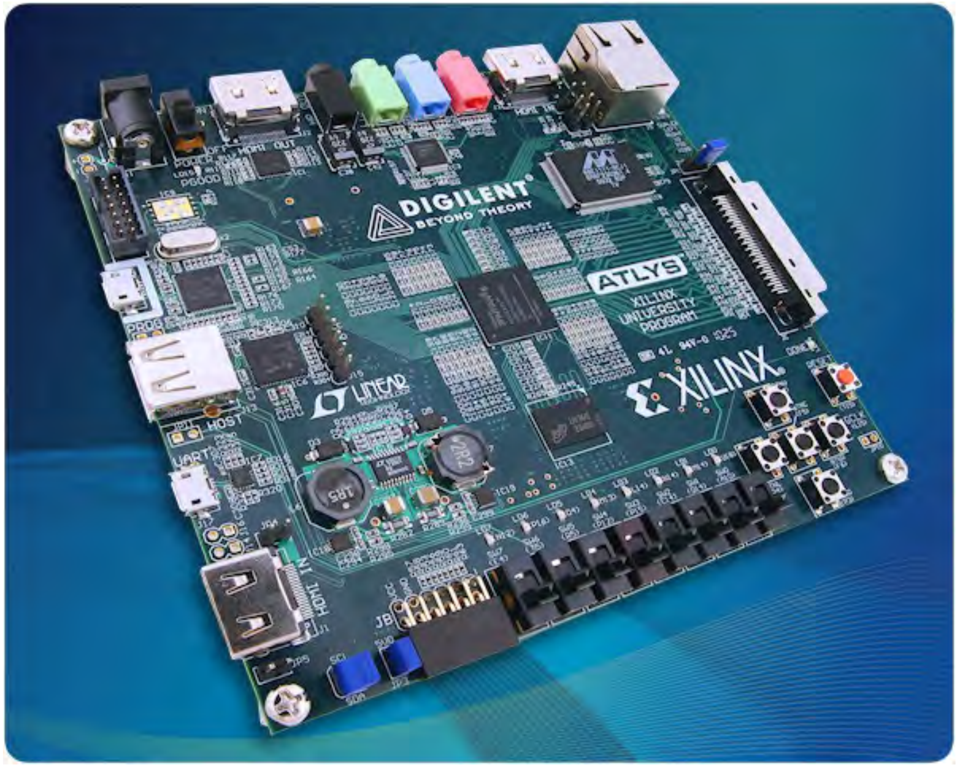
- BR PUF(5) is composed of n-stages, where each stage has two inverting delay elements (NOR gates as an example)
- Each challenge vector configures a unique ring $C_i \in 2^n$ (n= num stages)
- Ring has two stable states $r_i \in \{0,1\}$



(5) Q Chen, et al. *HOST,* 2011

FPGA implementation

BR PUF implemented on Spartan VI FPGA



64-bit BR PUF implementation including peripheral logic, I/O etc

# of slices	3556
# of slice flip flops	***3688***
# of LUTs	***6318***

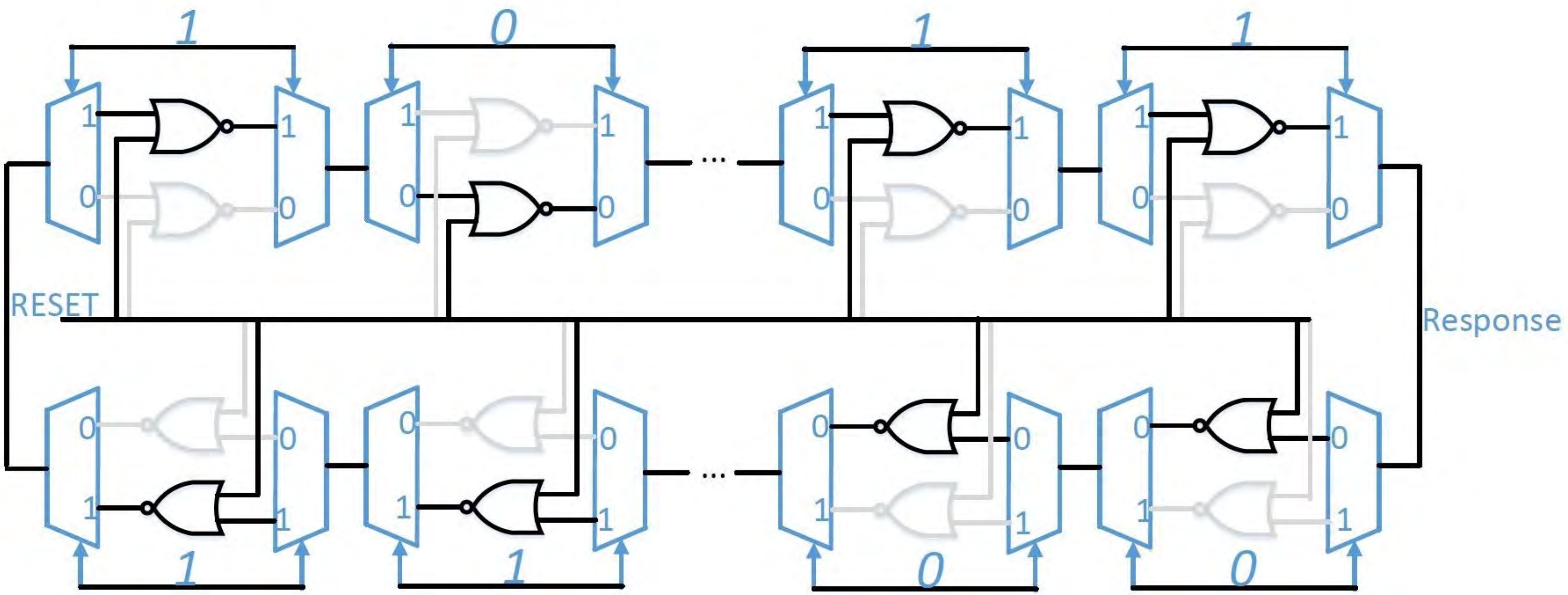
544 gates to implement only the basic BR PUF

Outline

- Background
  - PUFs
  - Modeling attacks on PUFs
  - Bistable Ring PUF
- Security Evaluation of BR PUFs
  - Modeling the BR PUF
  - Results against BR PUF and variants
- Security Enhancement of BR PUFs
  - XORing BR PUFs to enhance the security
  - Impact on other PUF parameters
- Conclusion and future work

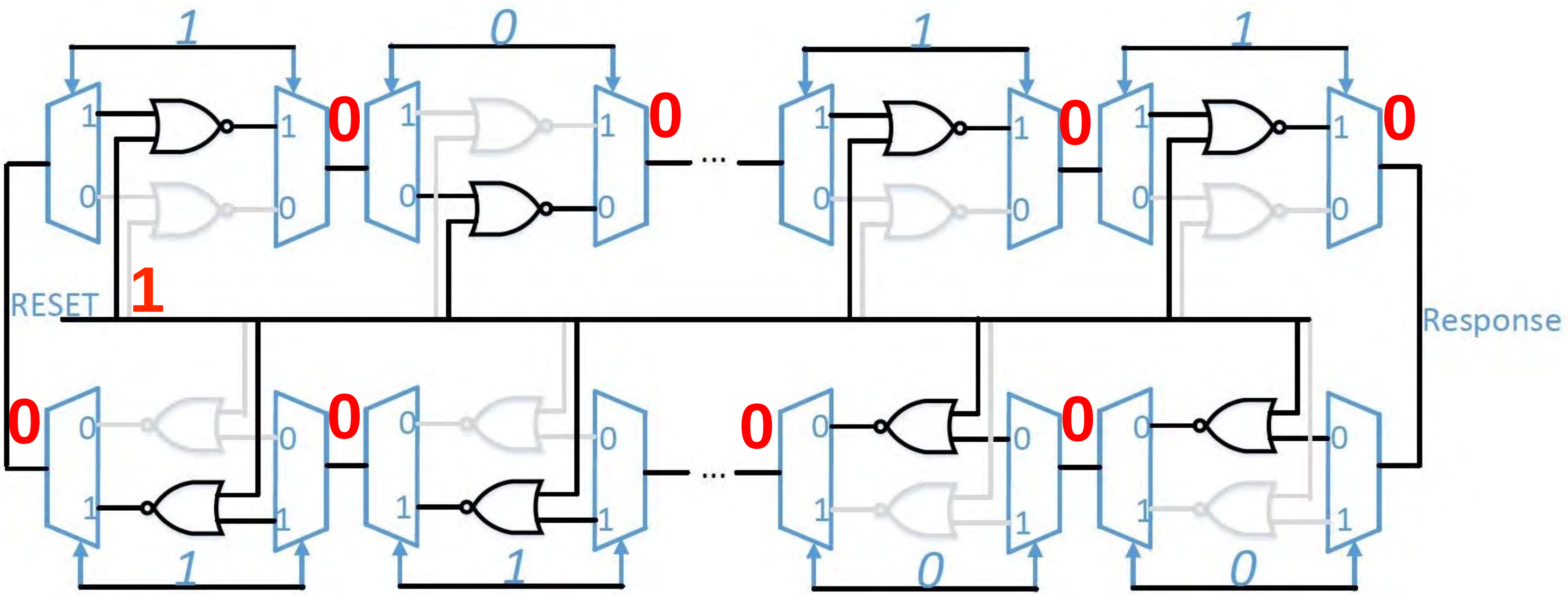
Evaluating Response of BR PUF

1. Apply reset and challenge to configure ring
2. Release reset
3. Read response after allow time for stabilization



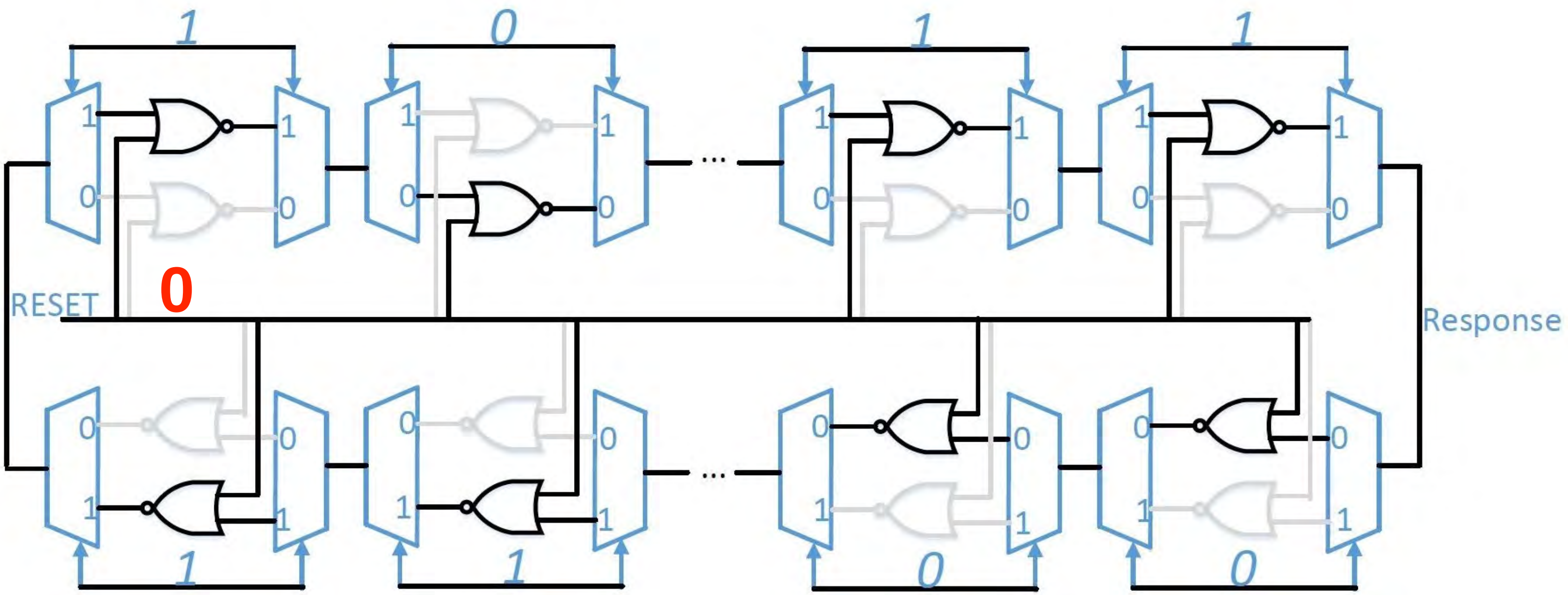
Evaluating Response of BR PUF

1. Apply reset and challenge to configure ring
2. Release reset
3. Read response after allow time for stabilization



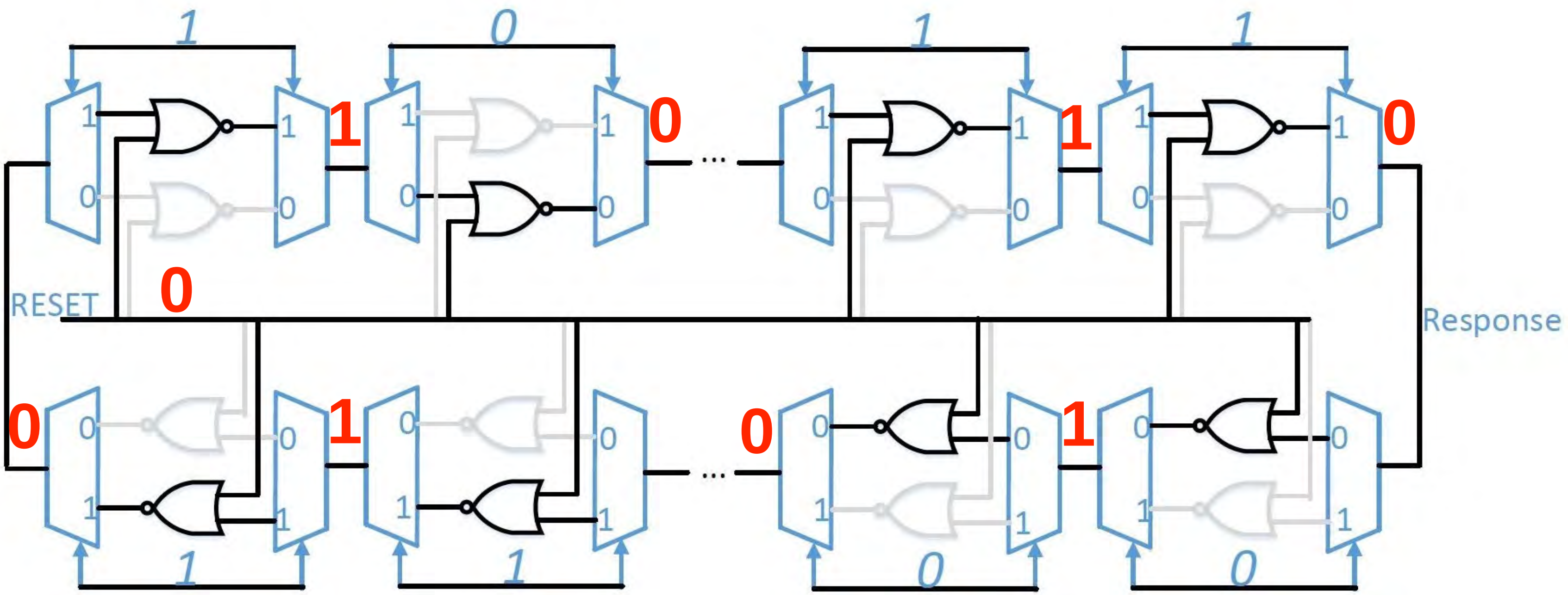
Evaluating Response of BR PUF

1. Apply reset and challenge to configure ring
2. Release reset
3. Read response after allow time for stabilization



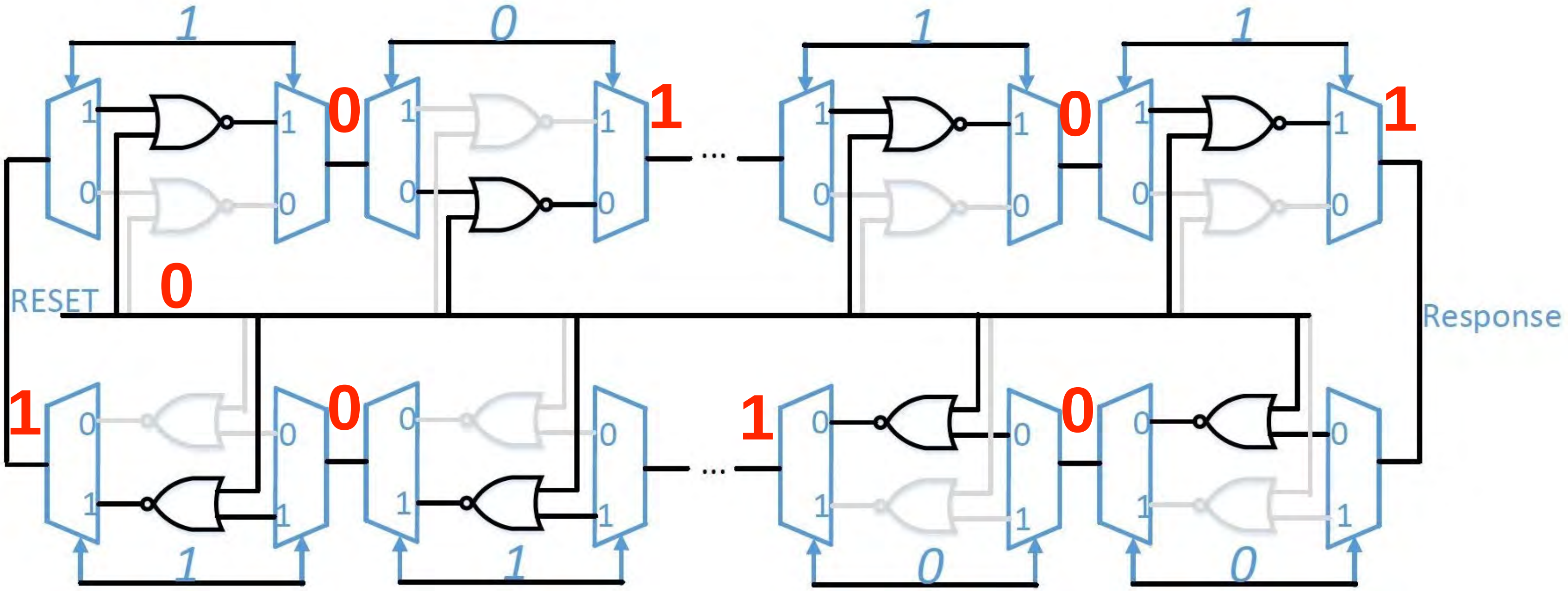
Evaluating Response of BR PUF

1. Apply reset and challenge to configure ring
2. Release reset
3. Read response after allow time for stabilization



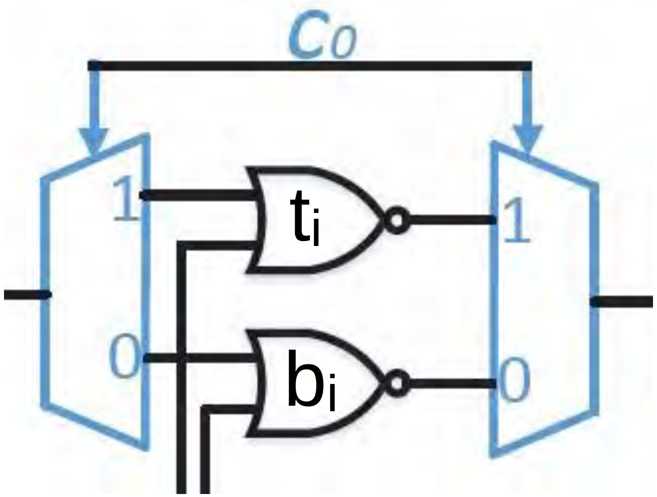
Evaluating Response of BR PUF

1. Apply reset and challenge to configure ring
2. Release reset
3. Read response after allow time for stabilization



Modeling the BR PUF

- Represent each stage by two weights
- Weights represent tendency to favor a stage output of 1 over stage output of 0
- t_i represents weight of top gate in i^{th} stage
- b_i represents weight of bottom gate in i^{th} stage

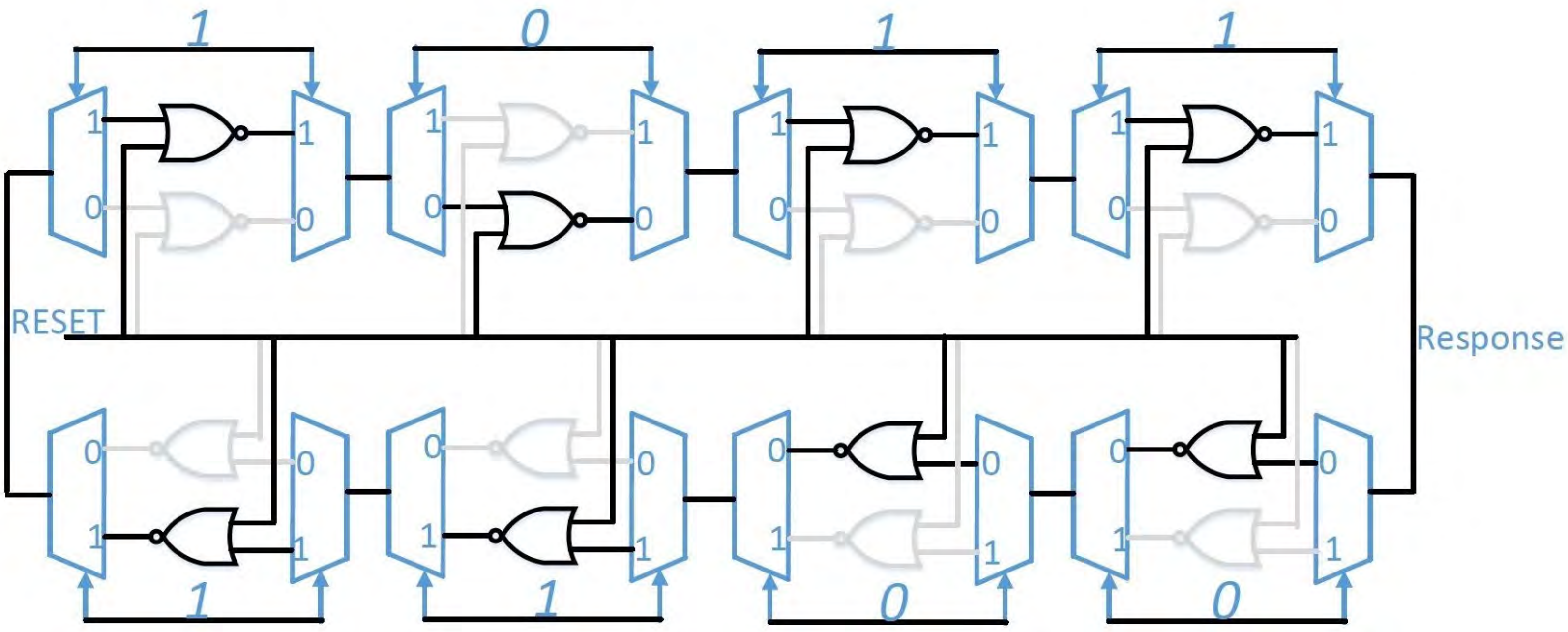


Assumption: there exist weights that explain the challenge response mapping of BR PUF

Example

- Challenge bits select weights, stage index determines signs
- Response tells whether sum is negative or positive
- Additive delay model (like Arbiter PUF)

$$t_0 - b_1 + t_2 - t_3 + b_4 - b_5 + t_6 - t_7$$


1
0
1
1
RESET
Response
1
1
0
0