高不可预测性PUF电路设计

Design methodology of Unpredictable Physical Unclonable Functions

报 告 人 唐文懿

导　　师 贾嵩

日　　期 2016-4-15

内容提要

背景介绍

- 技术背景
- 评价指标
- 相关工作

原理分析

- A-PUF建模
- BRPUF建模
- XOR-PUF建模

新结构介绍

- 电路结构
- 运作机制
- 测试结果

总结

- 工作总结
- 前景展望

技术背景

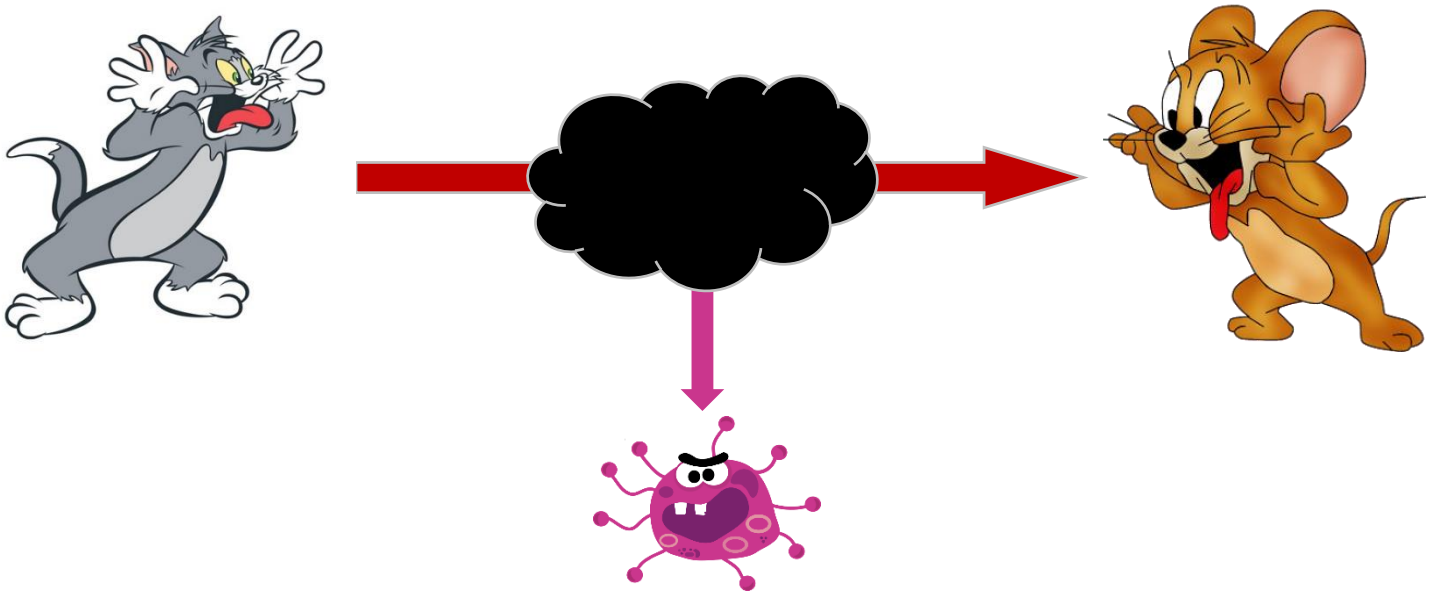
- 从信息安全说起.....

技术背景

- 从信息安全说起.....

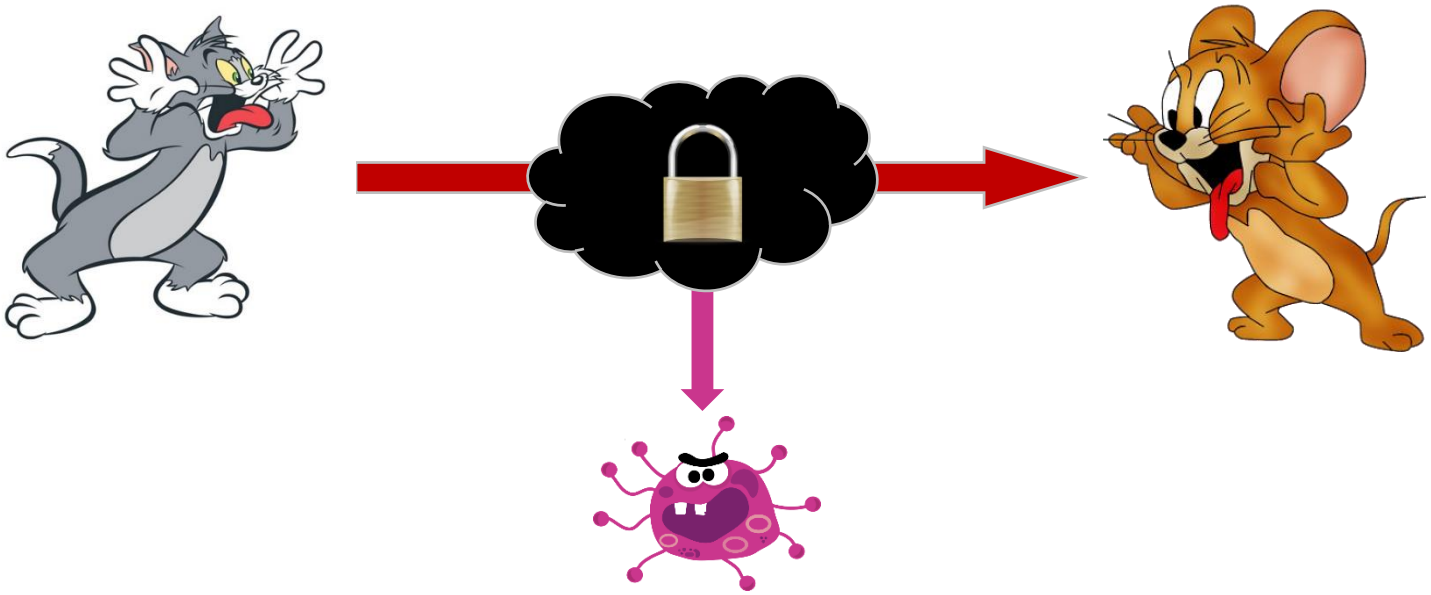
技术背景

- 从信息安全说起.....



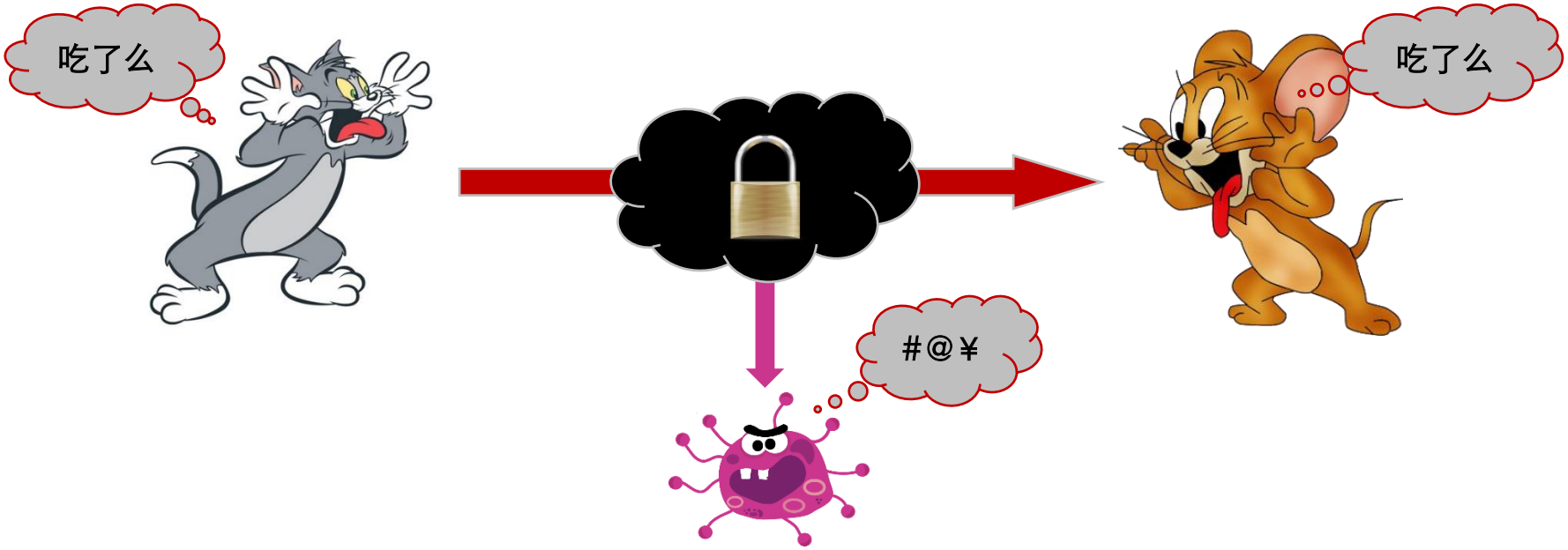
技术背景

- 从信息安全说起.....



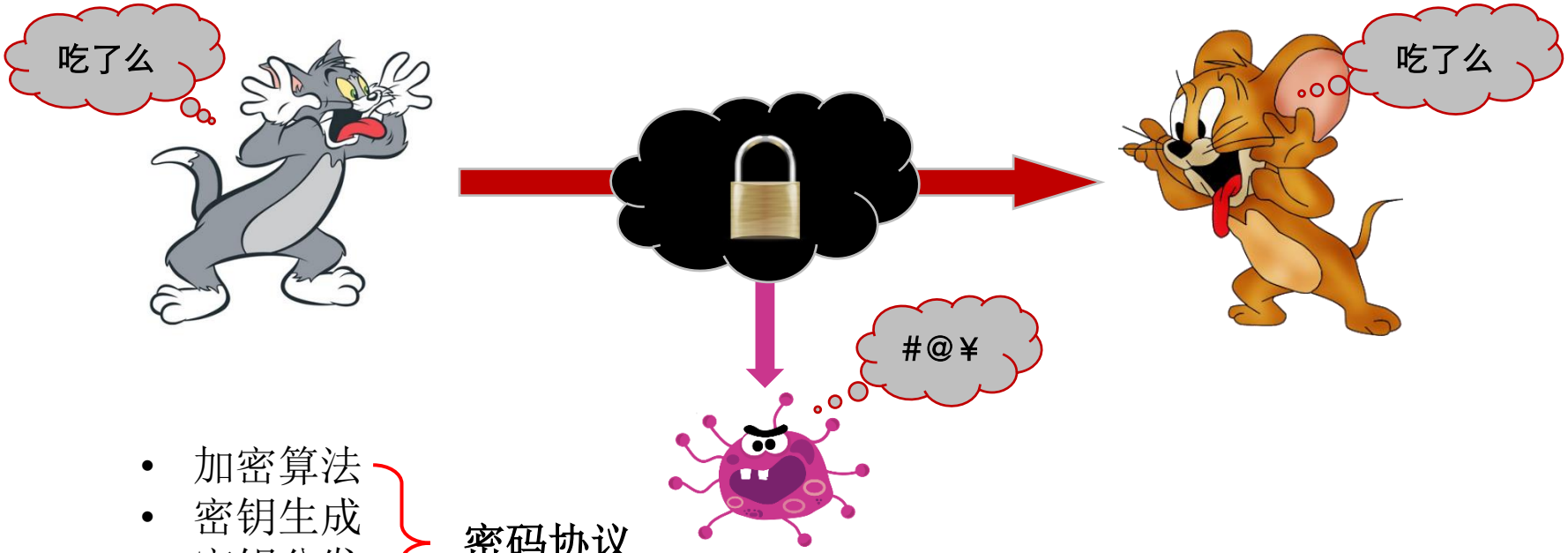
技术背景

- 从信息安全说起.....



技术背景

◆从信息安全说起.....



- 加密算法
- 密钥生成
- 密钥分发
- 密钥储存

密码协议

技术背景

◆密码协议的特点：

- 加密便捷
- 信任方解密便捷
- 拦截放解密困难

➢ *单向函数（HASH）*

- $y = f(x_0, x_1, \ldots, x_n)$
- $f^{-1}(y) = ?$
- $f^{-1}(y, x_{i \neq key}) = ?$
- $f^{-1}(y, x_{key}) = x_i$

技术背景

◆密码协议的特点：
- 加密便捷
- 信任方解密便捷
- 拦截放解密困难

➢ *单向函数（HASH）*
- $y = f(x_0, x_1, \ldots, x_n)$
- $f^{-1}(y) = ?$
- $f^{-1}(y, x_{i \neq key}) = ?$
- $f^{-1}(y, x_{key}) = x_i$

- MD5
- SHA
- PJW
- ELF
- EHC
- Trivium
- MicKey
- BKDR
- RSA
- AES
- ECC
- **PUF**

技术背景

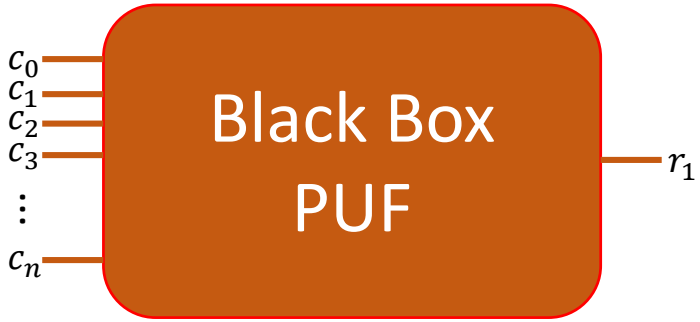
◆密码协议的特点：
- 加密便捷
- 信任方解密便捷
- 拦截放解密困难

➢ *单向函数（HASH）*
- $y = f(x_0, x_1, \ldots, x_n)$
- $f^{-1}(y) = ?$
- $f^{-1}(y, x_{i \neq key}) = ?$
- $f^{-1}(y, x_{key}) = x_i$

- MD5
- SHA
- PJW
- ELF
- EHC
- Trivium
- MicKey
- BKDR
- RSA
- AES
- ECC
- **PUF**
  - •结构简单
  - •成本低廉

技术背景

- **PUF——**Physical Unclonable Function（*物理不可克隆函数*）
  - 输入：**Challenge**
  - 输出：**Response**
  - **CRP: C-R Pairs**



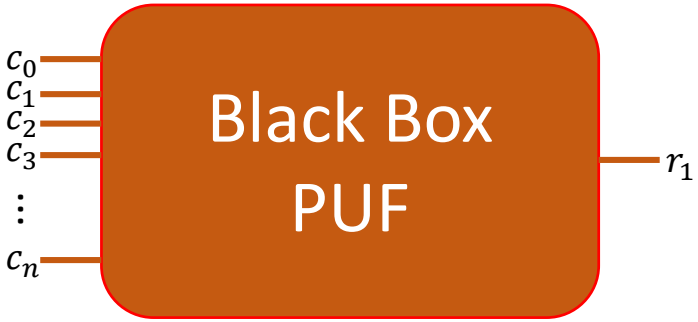
技术背景

◆**PUF——**Physical Unclonable Function（*物理不可克隆函数*）

- 输入：**Challenge**
- 输出：**Response**
- **CRP: C-R Pairs**

✓不可知物理系统

✓观测点



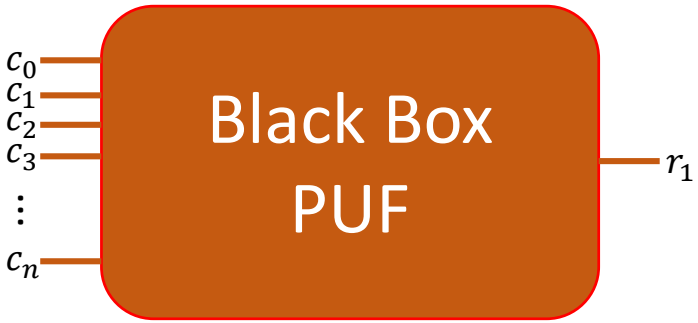
技术背景

◆**PUF——Physical Unclonable Function**（*物理不可克隆函数*）

- 输入：**Challenge**
- 输出：**Response**
- **CRP: C-R Pairs**

✓不可知物理系统

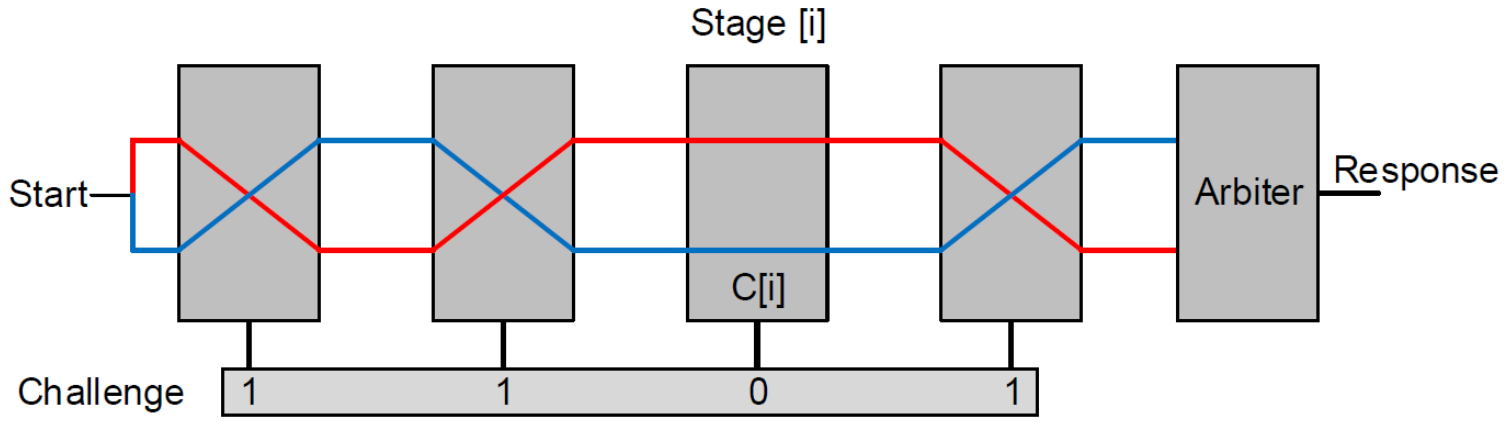
✓观测点



- **Weak PUF**
  - CRP空间小
  - 没有对外IO接口
- **Strong PUF**
  - CRP空间极大
  - 不可预测性
  - 不受保护的对外IO接口

技术背景

- PUF在电路中的实现
  - 未知物理系统：**制作工艺波动**
    - 不可控
    - 不可仿真
  - 观测点：**数字化输出**



Arbiter PUF： B. Gassend, “*Silicon Physical Random Functions*”, 2002

评价指标

- ◆唯一指标——**安全性**
  - *直观？量化？充要性？*
  - 量化指标——统计特性——安全性必要条件
    1. （片内）随机性：$Rand = \frac{1}{N} \cdot \sum^{N} f(c_i)$
    2. （片间）独特性：$Uniq = \frac{2}{M(M-1)} \sum_{i=1}^{M} \sum_{j=i+1}^{M} \frac{HD(P_i,P_j)}{N}$
    3. 可靠性（可重复性）：$Reliability = \frac{1}{MN} \sum_{j}^{M} \sum_{i}^{N} |f(c') - f(c_i)|$
    4. （*）NIST测试（随机数测试标准）

评价指标

- ◆唯一指标——**安全性**
  - *直观？量化？充要性？*
  - 量化指标——统计特性——安全性必要条件
    1. （片内）随机性：$Rand = \frac{1}{N} \cdot \sum^{N} f(c_i)$
    2. （片间）独特性：$Uniq = \frac{2}{M(M-1)} \sum_{i=1}^{M} \sum_{j=i+1}^{M} \frac{HD(P_i,P_j)}{N}$
    3. 可靠性（可重复性）：$Reliability = \frac{1}{MN} \sum_{j}^{M} \sum_{i}^{N} |f(c') - f(c_i)|$
    4. （*）NIST测试（随机数测试标准）
- ◆Strong PUF的**不可预测性**
  - 不能根据CRP某一子集推算出其他子集或全集

评价指标

- **唯一指标——安全性**
  - *直观？量化？充要性？*
  - 量化指标——统计特性——安全性必要条件
    1. （片内）随机性：$Rand = \frac{1}{N} \cdot \sum^{N} f(c_i)$
    2. （片间）独特性：$Uniq = \frac{2}{M(M-1)} \sum_{i=1}^{M} \sum_{j=i+1}^{M} \frac{HD(P_i,P_j)}{N}$
    3. 可靠性（可重复性）：$Reliability = \frac{1}{MN} \sum_{j}^{M} \sum_{i}^{N} |f(c') - f(c_i)|$
    4. （*）NIST测试（随机数测试标准）
- **Strong PUF的不可预测性**
  - 不能根据CRP某一子集推算出其他子集或全集
- **建模攻击**
  - 利用CRP子集，建立PUF**模型**，通过特定算法拟合模型**参数**。
  - **参数+模型=CRP全集**

相关工作

- 2002年——Arbiter PUF
- 2004年——Arbiter PUF建模攻击
- 2007年——XOR PUF、Lightweight PUF
- 2010年——XOR建模
- 2011年——Bistable Ring PUF

相关工作

- 2002年——Arbiter PUF
- 2004年——Arbiter PUF建模攻击
- 2007年——XOR PUF、Lightweight PUF
- 2010年——XOR建模
- 2011年——Bistable Ring PUF

本文主要贡献：

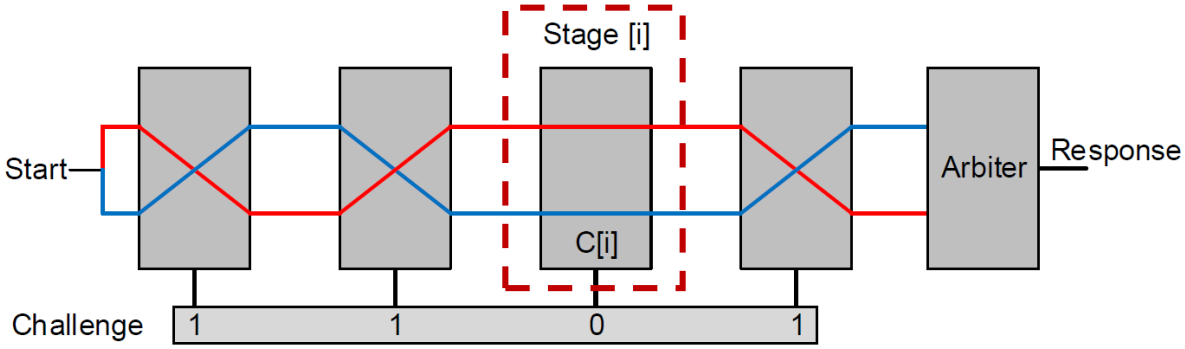
- 建立BRPUF模型，成功实行对其建模攻击；
- 设计新型Strong PUF方案，使其能够抵御建模攻击。

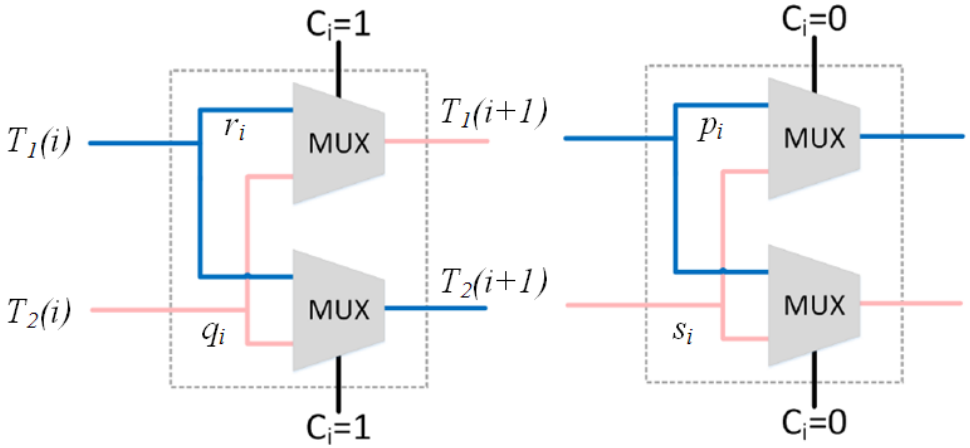
原理分析

背景介绍	原理分析	新结构介绍	总结
技术背景	A-PUF建模	电路结构	工作总结
评价指标	BRPUF建模	运作机制	前景展望
相关工作	XOR-PUF建模	测试结果	

Arbiter PUF建模

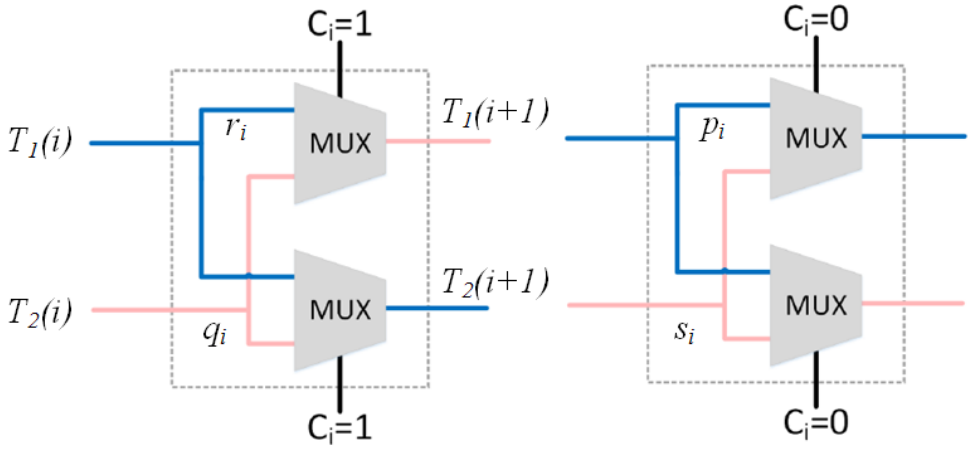
- 一个交换器4条路径延迟：p, q, r, s





Arbiter PUF建模

- 一个交换器4条路径延迟：p, q, r, s

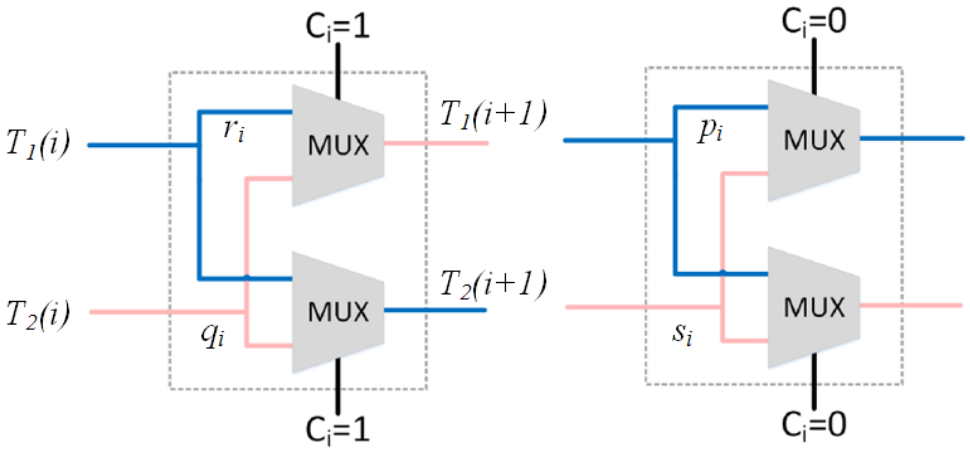


$$t_1(i+1) = \frac{1+c_i}{2}(t_2(i) + r_i) + \frac{1-c_i}{2}(t_1(i) + p_i)$$
$$t_2(i+1) = \frac{1+c_i}{2}(t_1(i) + q_i) + \frac{1-c_i}{2}(t_2(i) + s_i)$$

$$\Delta t(i+1) = \Delta t(i)c_i + \alpha_i c_i + \beta_i$$

Arbiter PUF建模

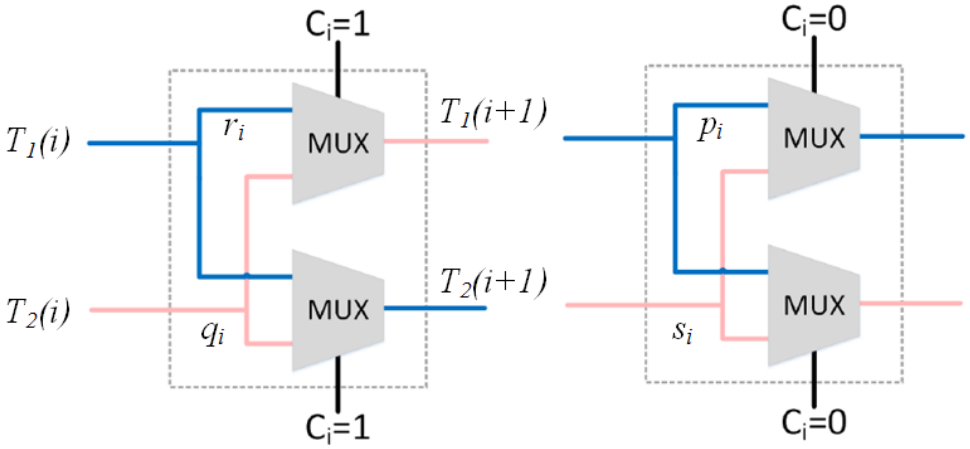
- 一个交换器4条路径延迟：p, q, r, s



$$\Delta t(n) = p'd$$

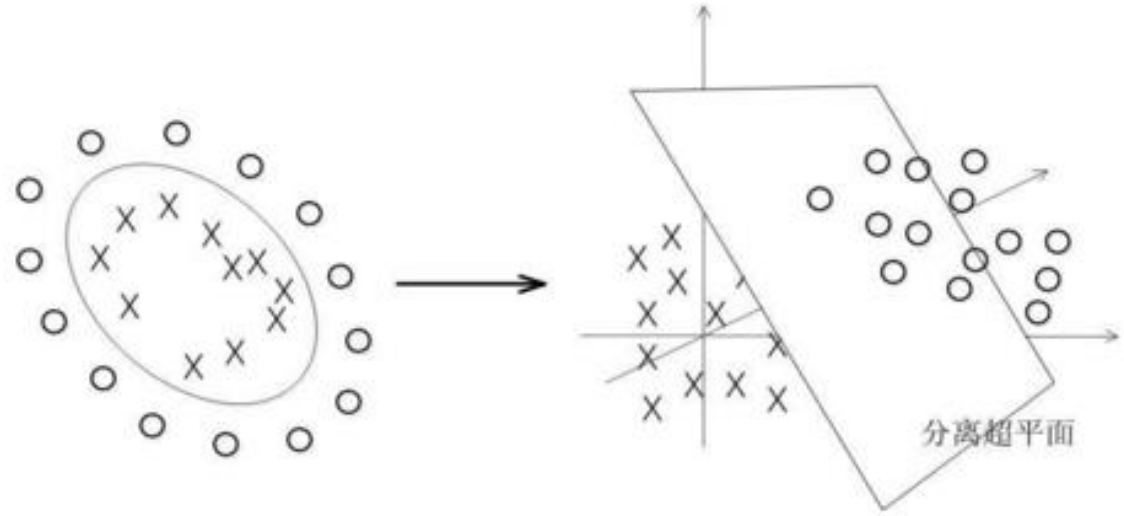
Arbiter PUF建模

- 一个交换器4条路径延迟：p, q, r, s



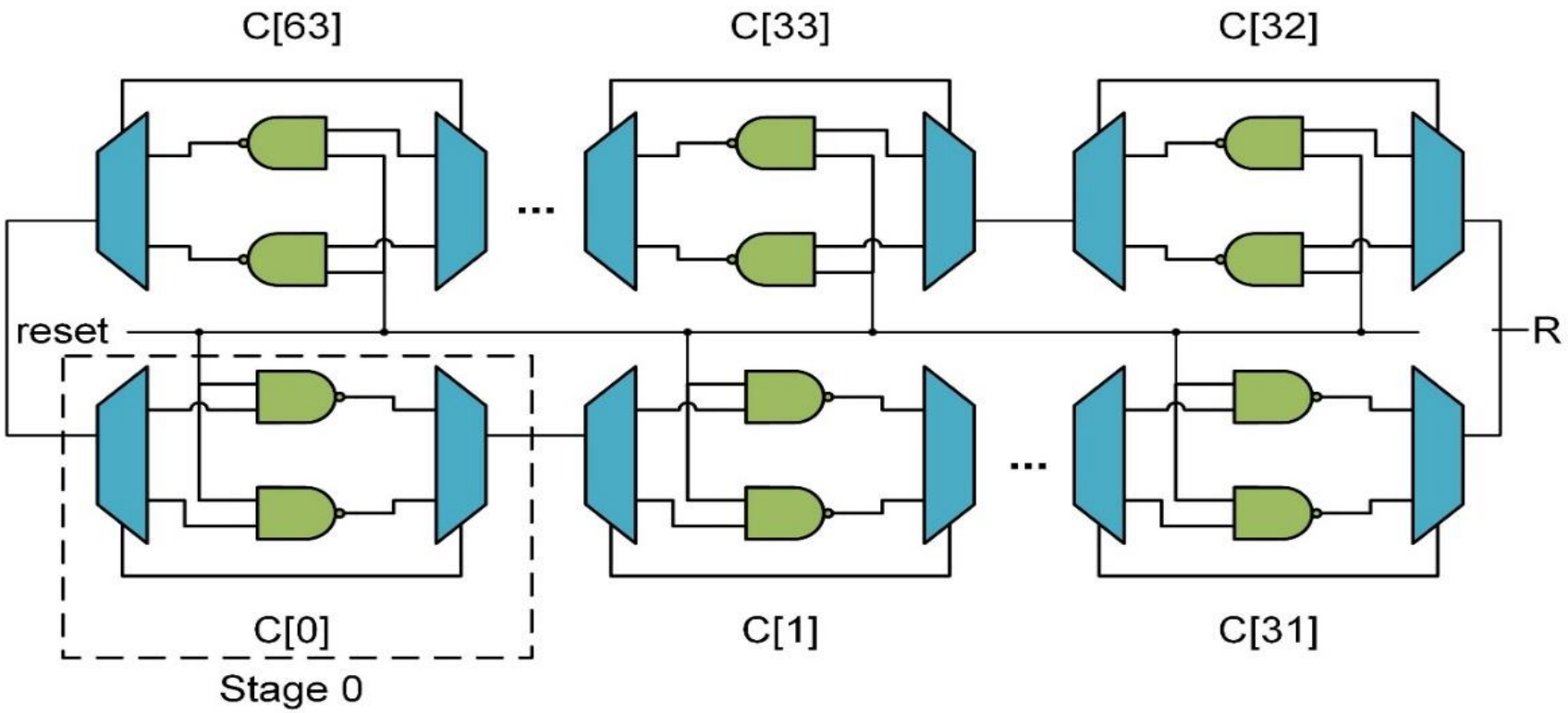
$$\Delta t(n) = p'd \quad \begin{cases} \Delta t(n) > 0 \rightarrow R = +1 \\ \Delta t(n) < 0 \rightarrow R = -1 \end{cases}$$

SVM线性分类器



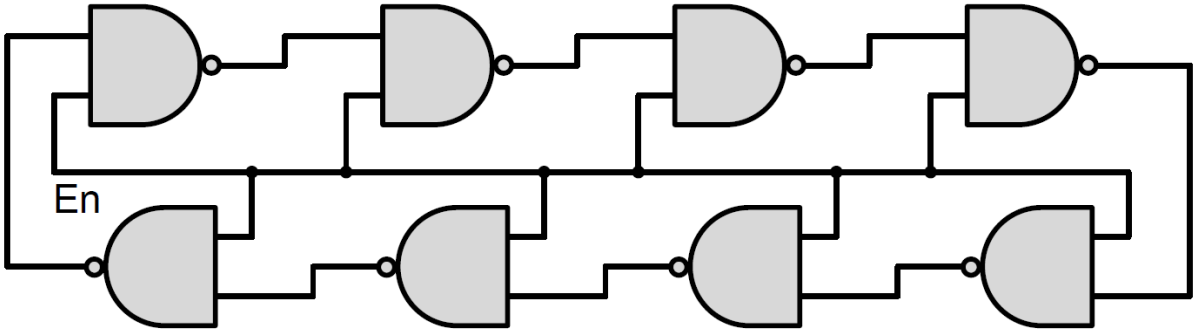
- $\Delta t(n) = p'd$
  - N维空间线性可分
  - 分界线——超平面
  - SVM——求解超平面解析式$p'd = 0$
  - $d \to p, q, r, s$

BR-PUF建模



Q. Chen, *HOST 2011*, pp 134-141

BR-PUF建模

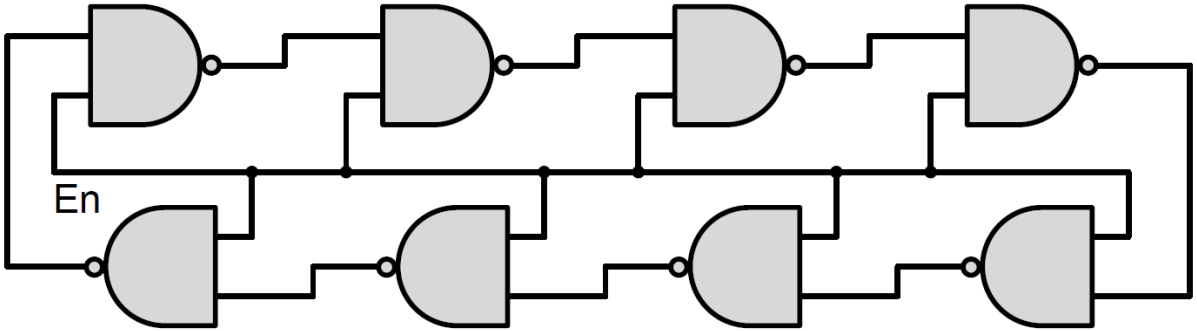


- NAND：上升沿--下降沿延迟tr，下降沿—上升沿延迟tf
- W：周期信号占空比

$$W_{i+1} = W_i + \frac{tf_i - tr_i}{T}(-1)^i$$

$$W \in [0,1]$$

BR-PUF建模



- NAND：上升沿--下降沿延迟tr，下降沿—上升沿延迟tf
- W：周期信号占空比

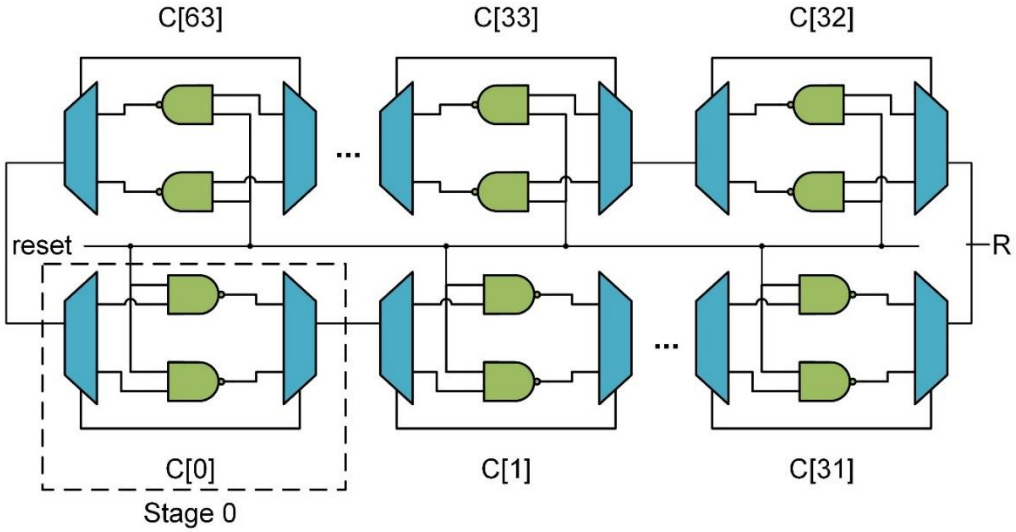
$$W_{i+1} = W_i + \frac{tf_i - tr_i}{T}(-1)^i$$

$$W \in [0,1]$$

$$W > 1 \rightarrow R = 1; W < 0 \rightarrow R = 0$$

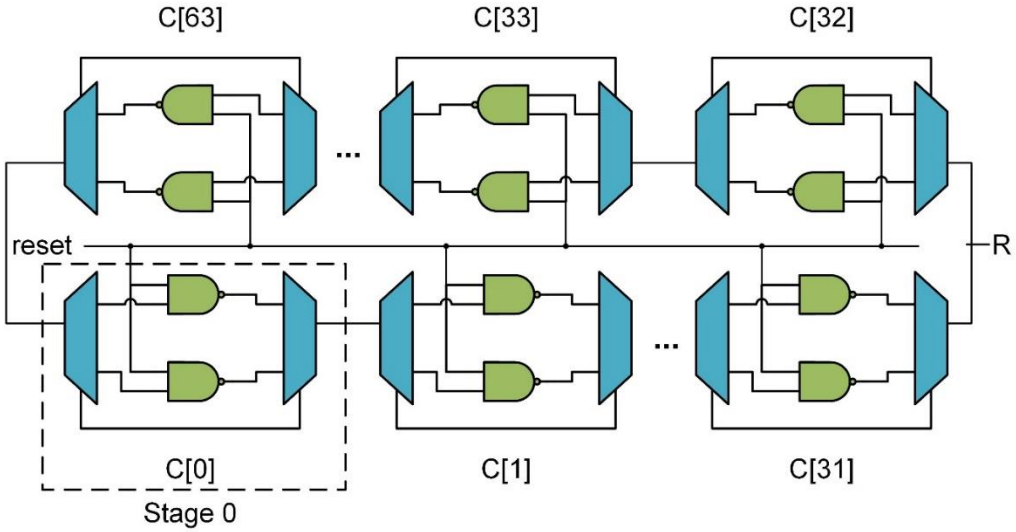
BR-PUF建模

◆每级两个与非门tr，tf设为p, q, r, s



BR-PUF建模

◆每级两个与非门tr，tf设为p, q, r, s



$$R = sgn\left(\sum_{i}^{N}(-1)^{i}\left(\frac{1+c_i}{2}(p_i - q_i) + \frac{1-c_i}{2}(r_i - s_i)\right)\right)$$

$$= sgn\left(\sum(\alpha_i c_i + \beta_i)\right) = sgn(p'd)$$

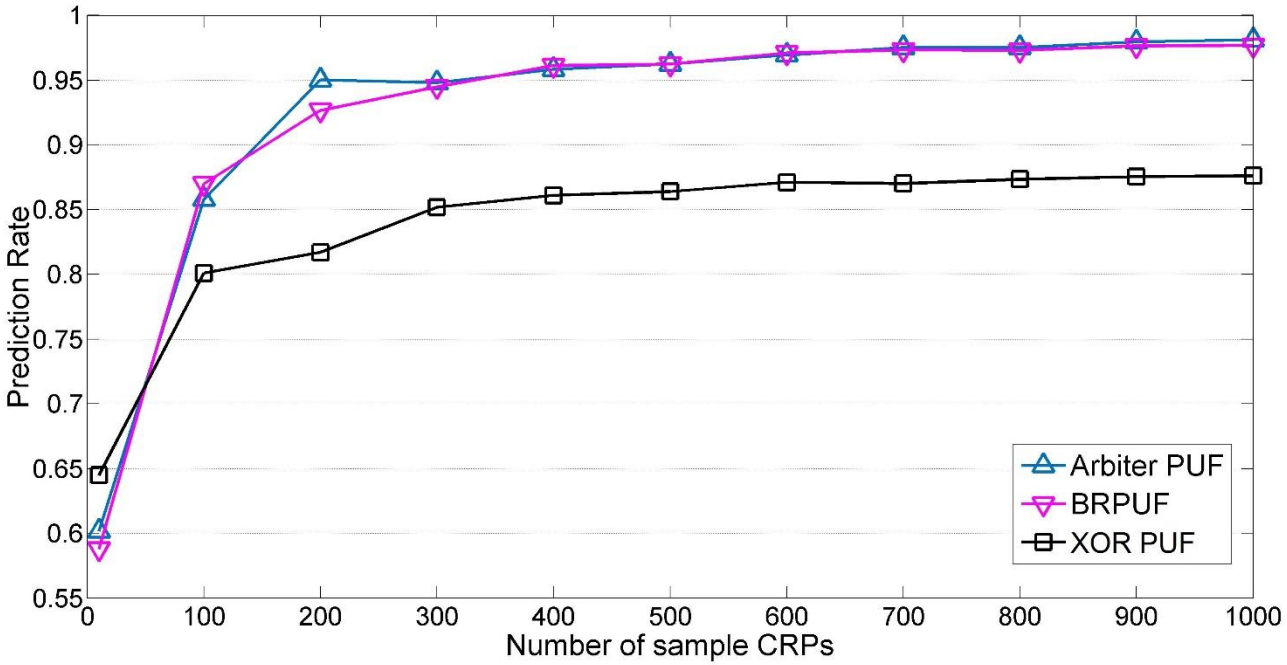
XOR-PUF建模

- $R = r_1 \oplus r_2 = p'd_1 \times p'd_2$

XOR-PUF建模

- $R = r_1 \oplus r_2 = p'd_1 \times p'd_2$

片内分布仿真曲线



新结构介绍

背景介绍	原理分析	新结构介绍	总结
技术背景	A-PUF建模	电路结构	工作总结
评价指标	BRPUF建模	运作机制	前景展望
相关工作	XOR-PUF建模	测试结果	

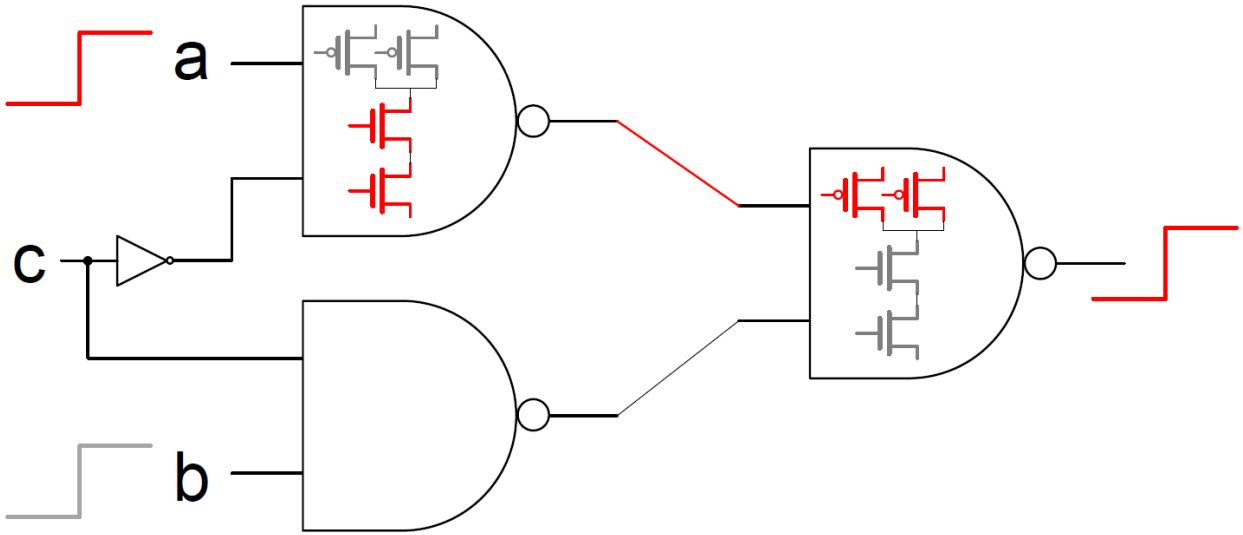
Strong PUF设计指标

高不可预测性PUF

- 主要指标：
  - 最小线性可分维度$n \to +\infty$
  - 片内分布$\mu \to 0.5, \sigma \to 0$
  - 片间分布$\mu \to 0.5, \sigma \to 0$（工艺相关）
- 次要指标：
  - 面积开销
  - 激励——响应速度

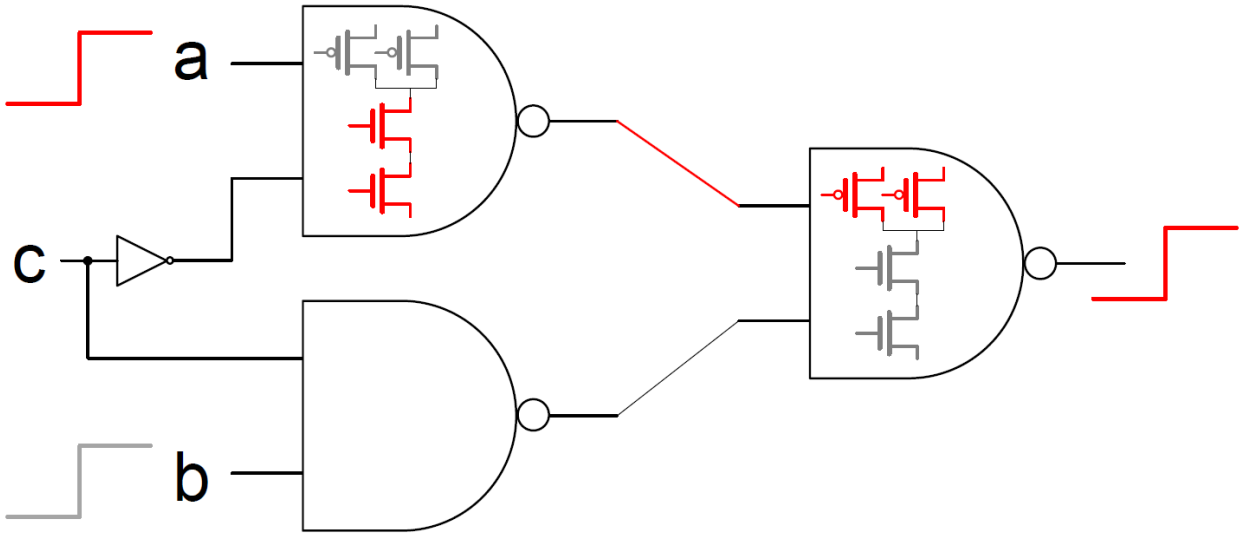
交换器逻辑结构

- 交换器实现细节



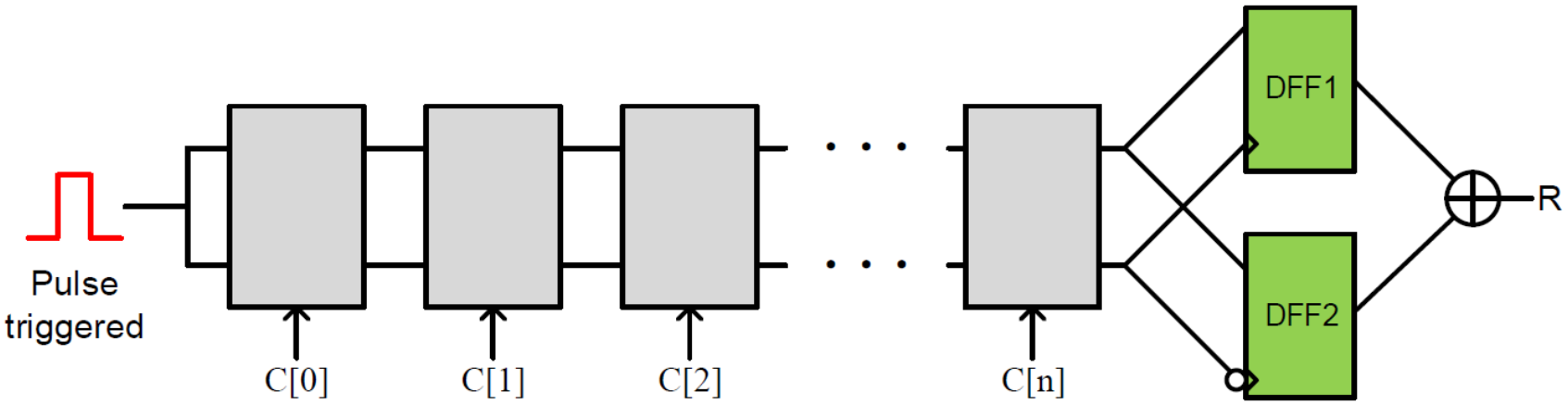
交换器逻辑结构

- 交换器实现细节
  - 驱动上升沿/下降沿是不同MOS管



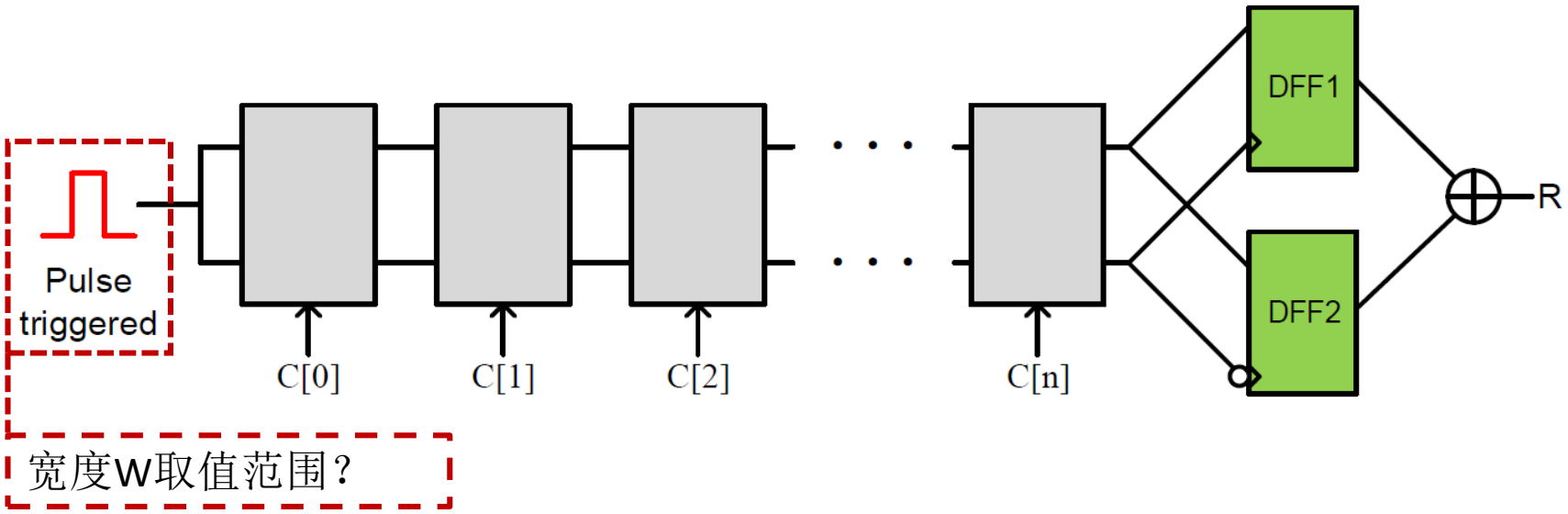
PA-PUF

- Pulse Arbiter PUF
  - DFF1—正边沿触发
  - DFF2—负边沿触发
  - $R = Q_1 \oplus Q_2$



PA-PUF

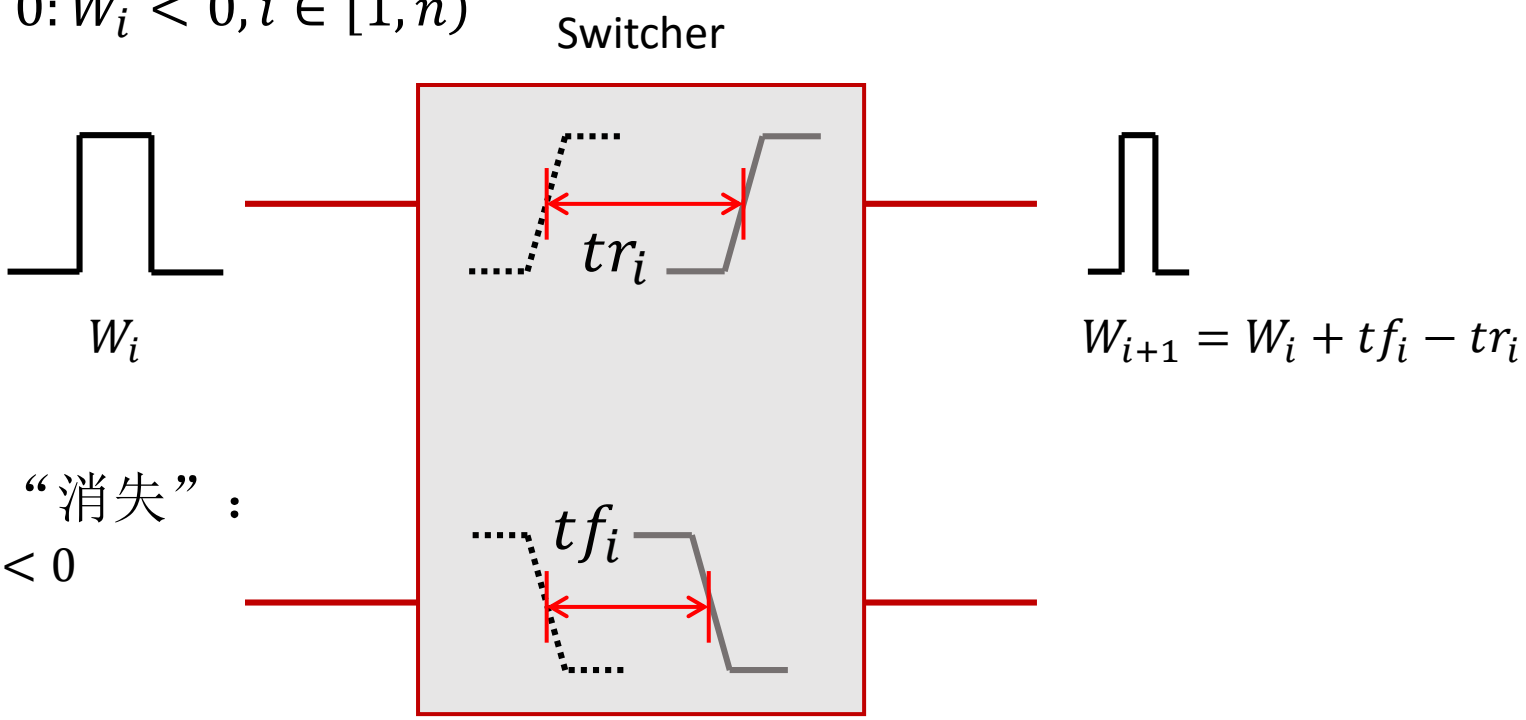
- Pulse Arbiter PUF
  - DFF1—正边沿触发
  - DFF2—负边沿触发
  - $R = Q_1 \oplus Q_2$



宽度W取值范围？

脉冲信号传递

- $W \to +\infty$: 一般情况
- $W \to 0$: 信号无法传递
- $W \sim 0: W_i < 0, i \in [1, n)$

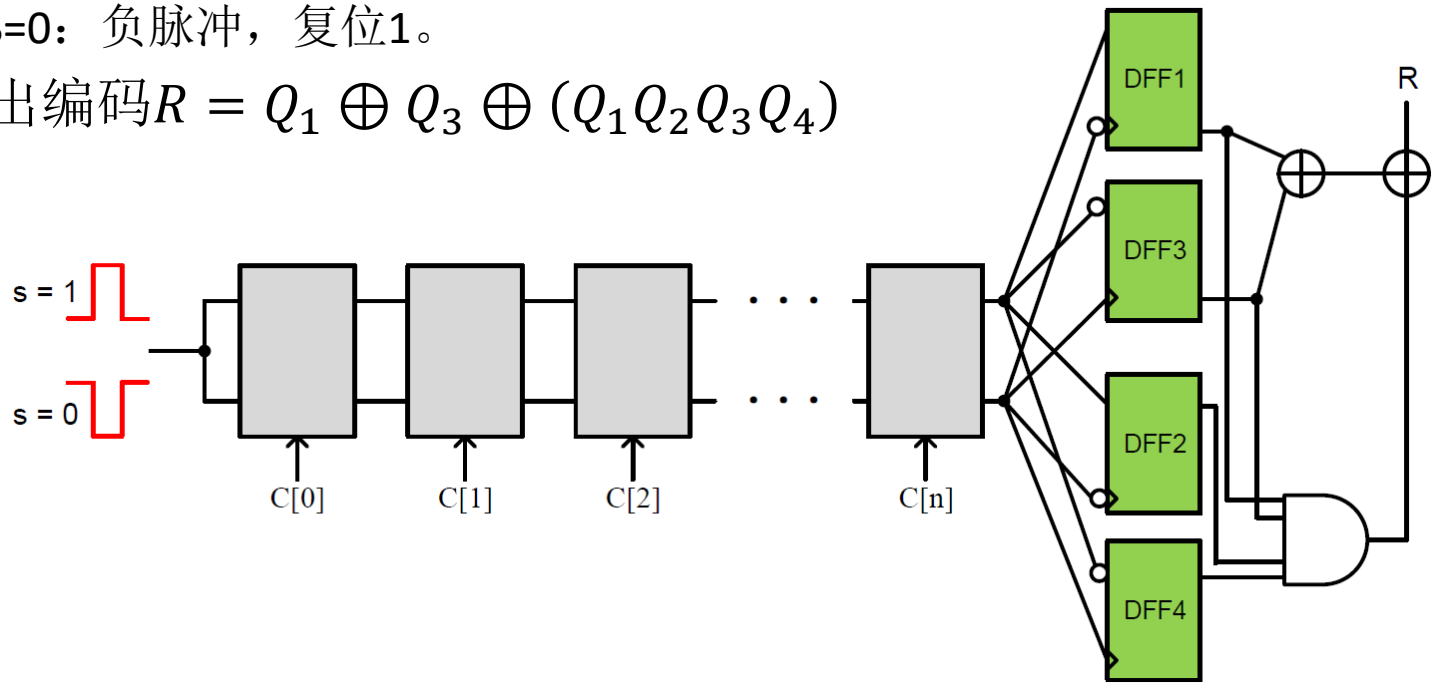


- 信号“消失”：
  - $W < 0$

RPA-PUF

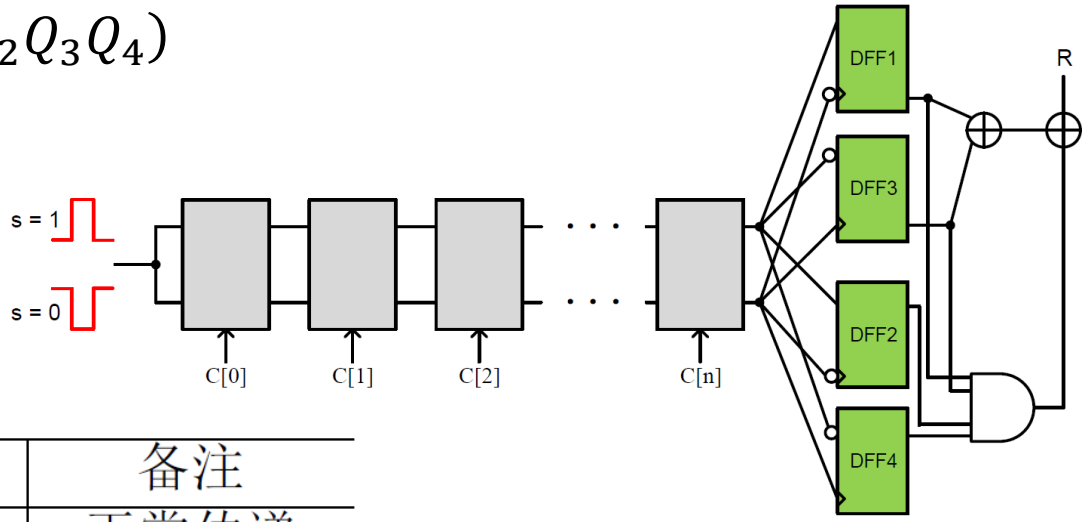
随机脉冲PUF

- 随机码s：
  - S=1：正脉冲，复位0；
  - S=0：负脉冲，复位1。
- 输出编码$R = Q_1 \oplus Q_3 \oplus (Q_1Q_2Q_3Q_4)$



RPA-PUF

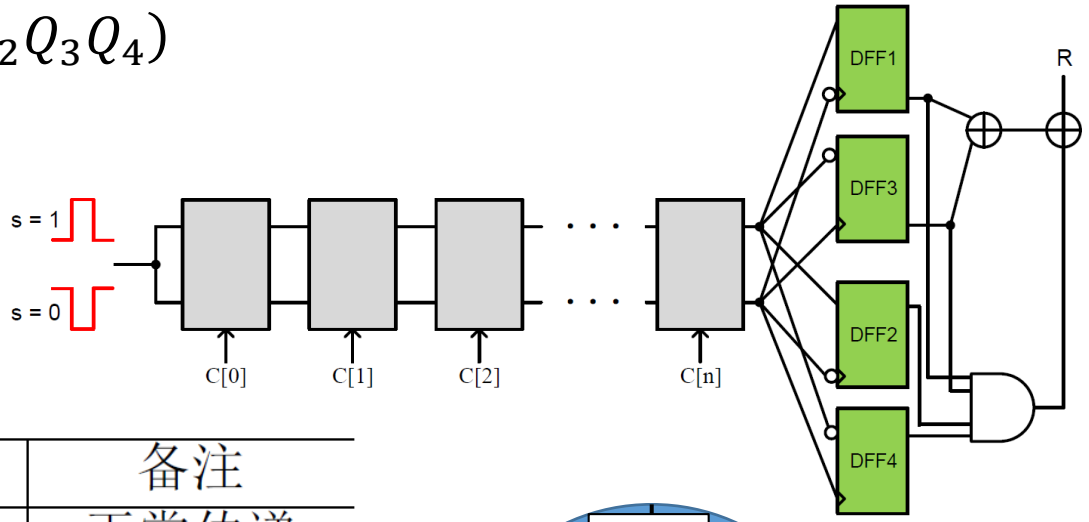
- $R = Q_1 \oplus Q_3 \oplus (Q_1 Q_2 Q_3 Q_4)$
  - 均不“消失”；
  - “消失”其一；
  - 均“消失”。



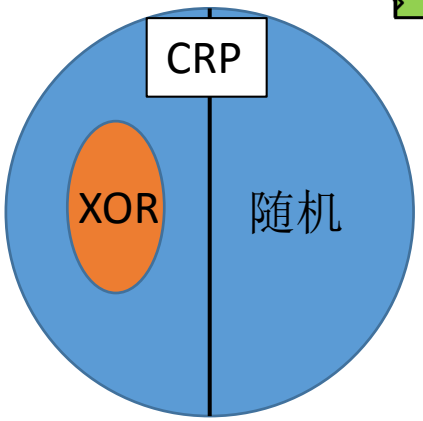
s	Q_1	Q_2	Q_3	Q_4	备注
x	0	1	0	1	正常传递
x	0	1	1	0	正常传递
x	1	0	0	1	正常传递
x	1	0	1	0	正常传递
1	1	1	1	1	负脉冲消失
0	0	0	0	0	正脉冲消失

RPA-PUF

- $R = Q_1 \oplus Q_3 \oplus (Q_1 Q_2 Q_3 Q_4)$
  - 均不“消失”；
  - “消失”其一；
  - 均“消失”。

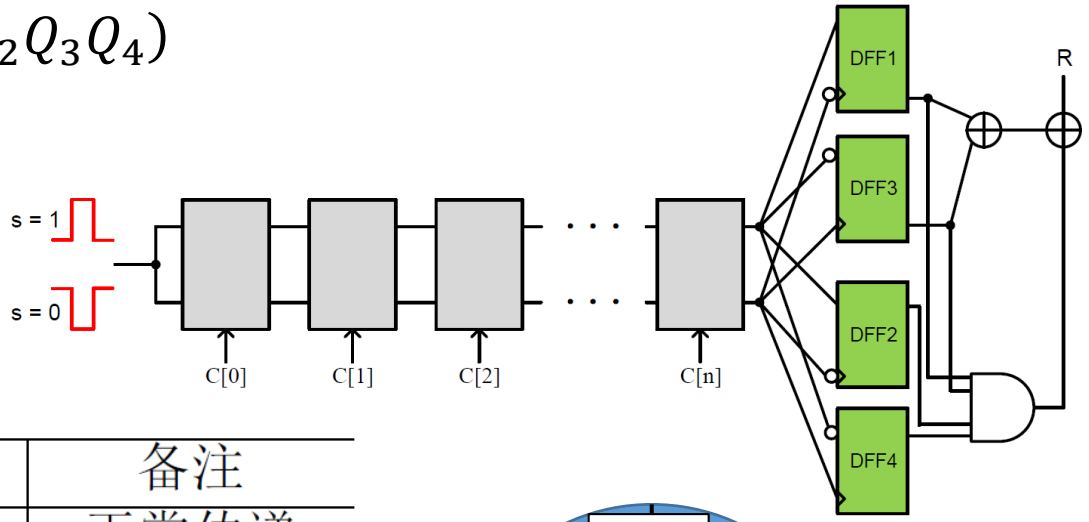


s	Q_1	Q_2	Q_3	Q_4	备注
x	0	1	0	1	正常传递
x	0	1	1	0	正常传递
x	1	0	0	1	正常传递
x	1	0	1	0	正常传递
1	1	1	1	1	负脉冲消失
0	0	0	0	0	正脉冲消失

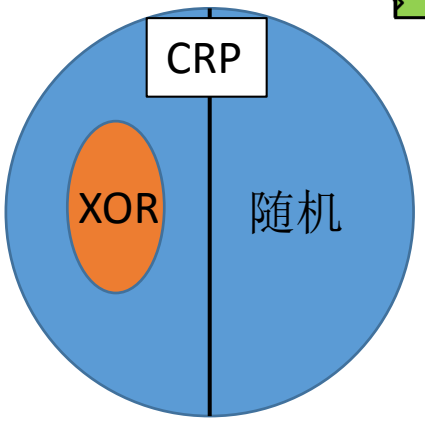


RPA-PUF

- $R = Q_1 \oplus Q_3 \oplus (Q_1 Q_2 Q_3 Q_4)$
  - 均不“消失”；
  - “消失”其一；
  - 均“消失”。



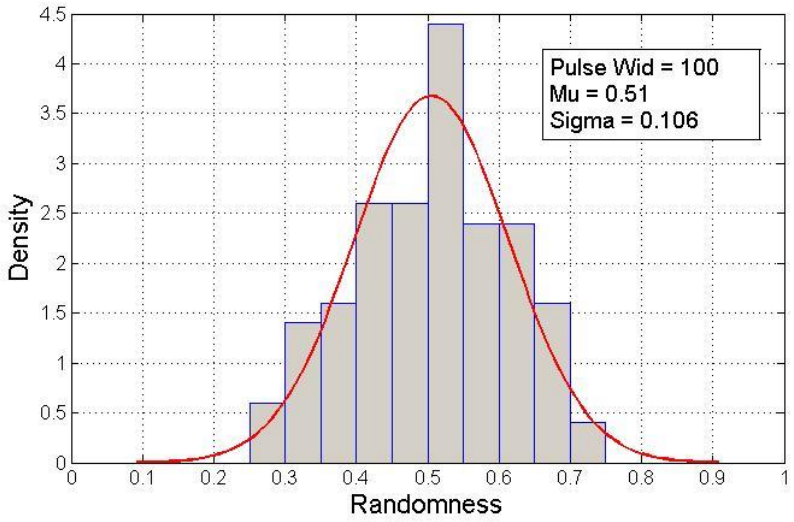
s	Q_1	Q_2	Q_3	Q_4	备注
x	0	1	0	1	正常传递
x	0	1	1	0	正常传递
x	1	0	0	1	正常传递
x	1	0	1	0	正常传递
1	1	1	1	1	负脉冲消失
0	0	0	0	0	正脉冲消失

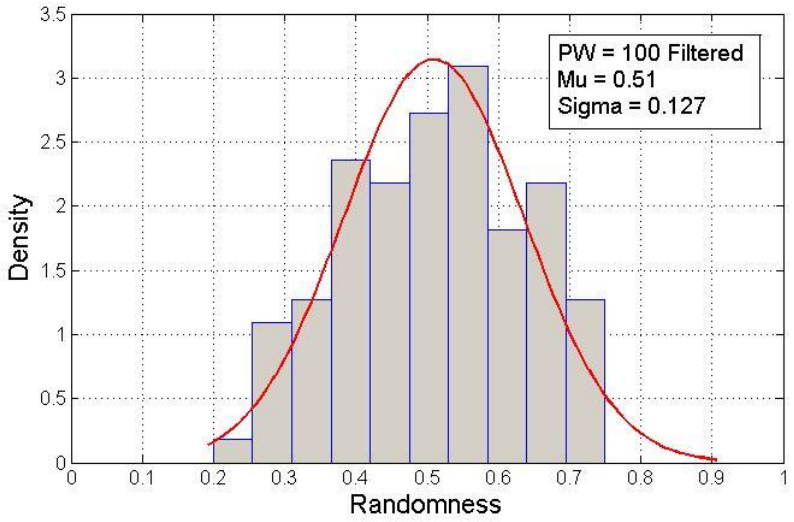


多次采样，舍弃随机响应

实验结果

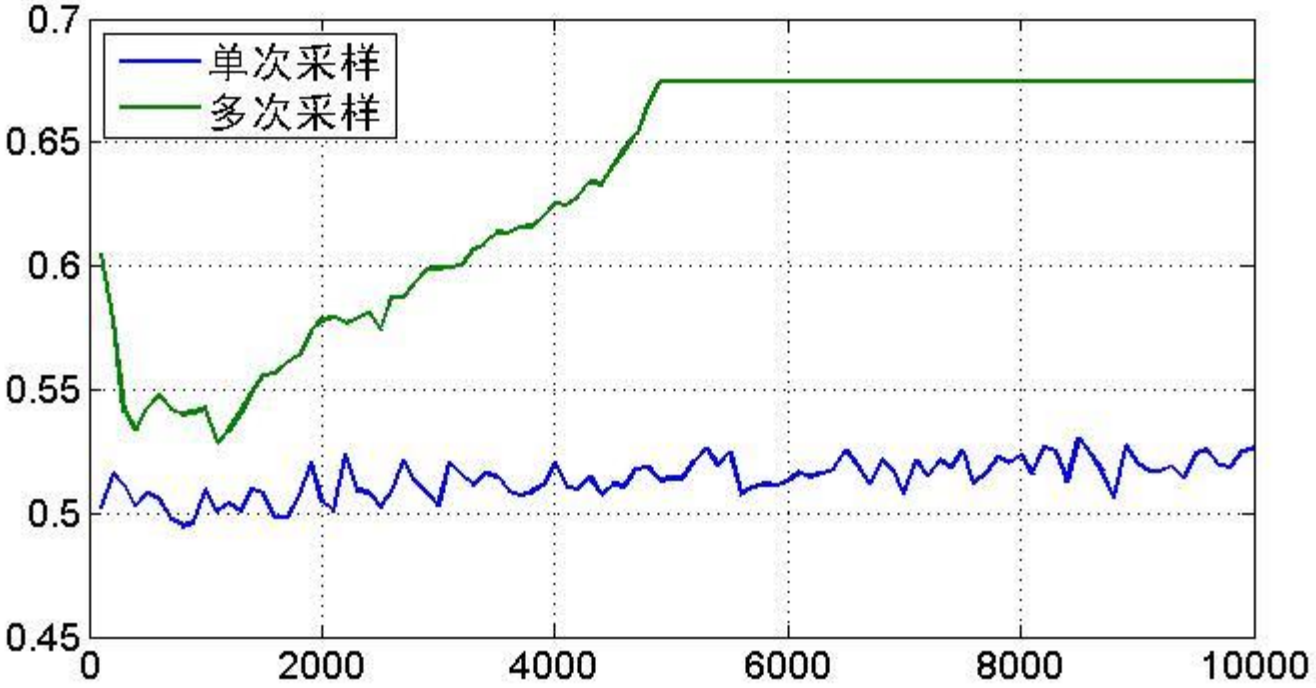
- 单次采样：=XOR+随机掩码
- 多次采样：近似XOR



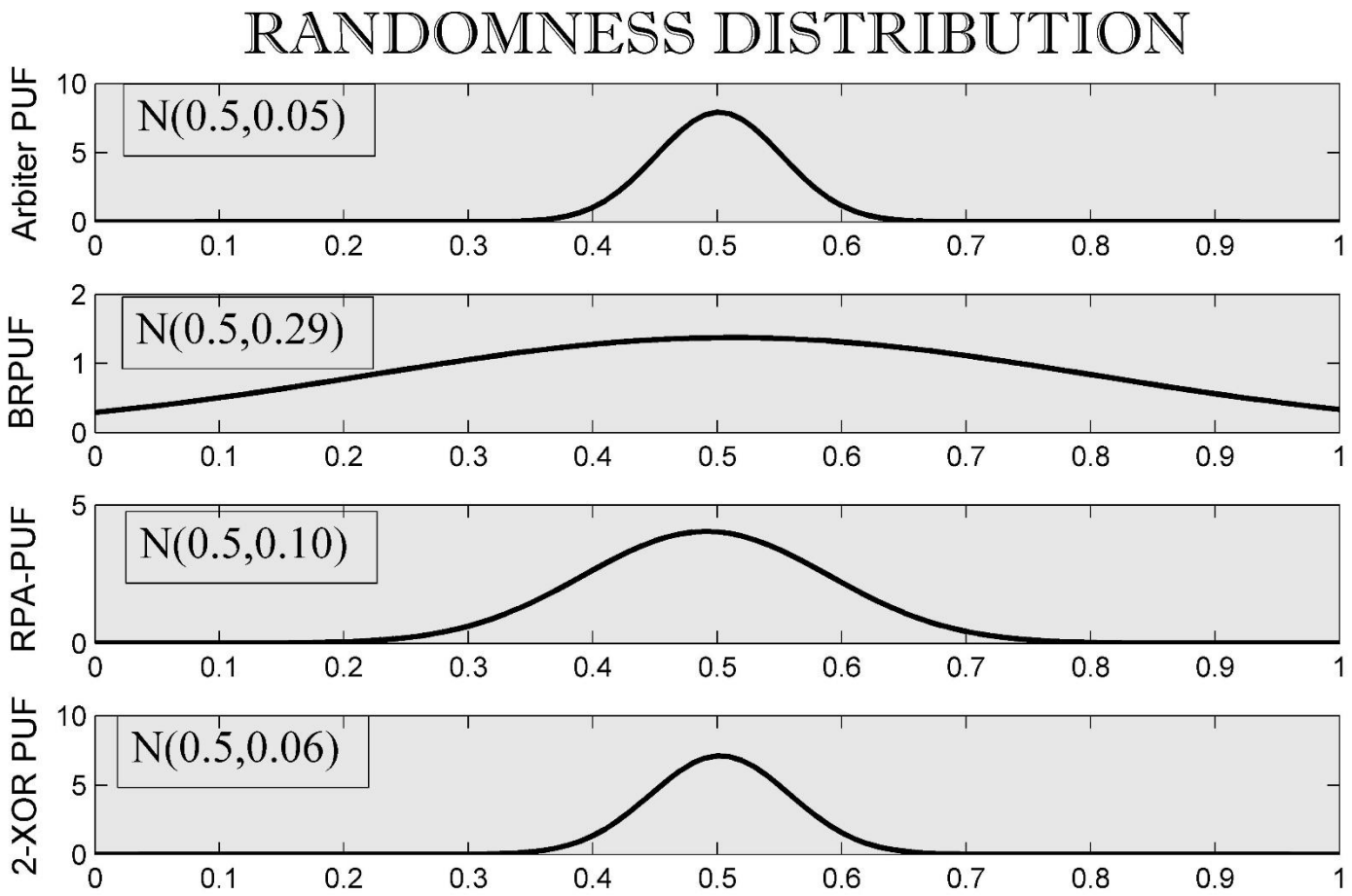


RPA-PUF建模攻击

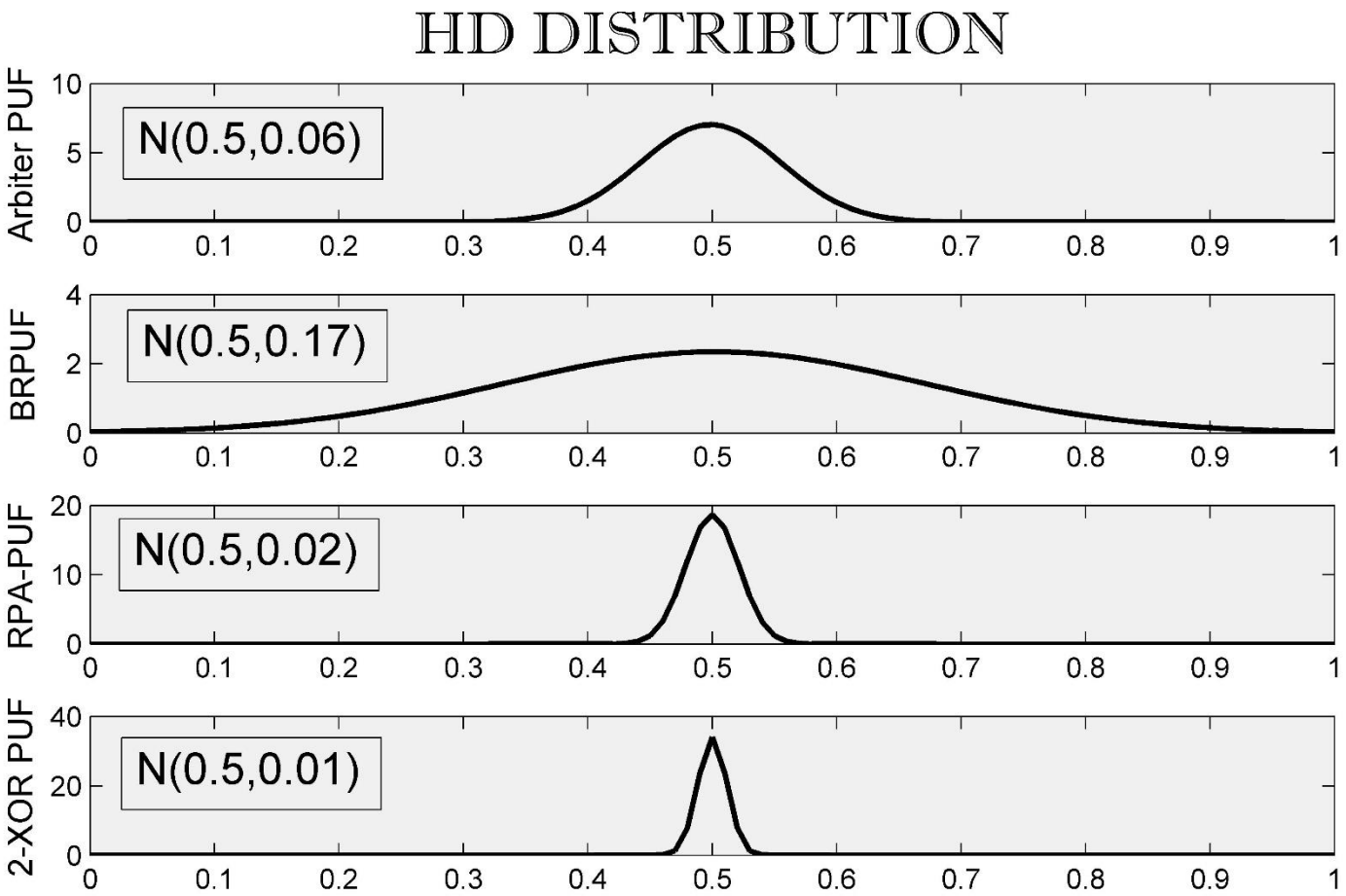
- SVM结果
  - RPAPUF使用XOR模型



随机性分布对比

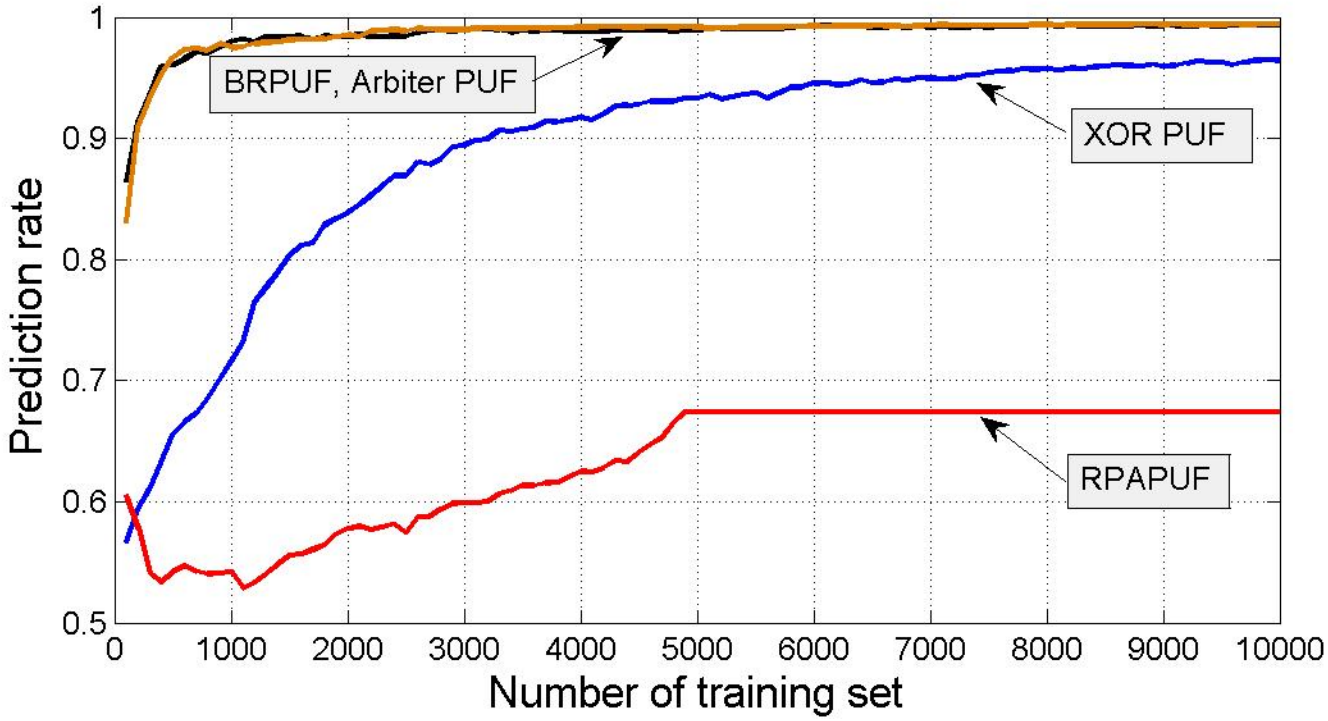

RANDOMNESS DISTRIBUTION
Arbiter PUF
N(0.5,0.05)
BRPUF
N(0.5,0.29)
RPA-PUF
N(0.5,0.10)
2-XOR PUF
N(0.5,0.06)
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

独特性分布对比


HD DISTRIBUTION
Arbiter PUF
N(0.5,0.06)
BRPUF
N(0.5,0.17)
RPA-PUF
N(0.5,0.02)
2-XOR PUF
N(0.5,0.01)
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

建模攻击结果对比

- SVM结果
  - RPAPUF使用XOR模型



结论

主要贡献：

- 对BRPUF结构建立模型，并成功实施建模攻击；
  - 预测率>99%
  - 训练集<5000 CRPs
- 提出新型PUF结构；
  - 具有良好的抗建模攻击性
  - 具有良好的统计分布特性

展望：

- PUF高层次应用：协议
- 流片实现以及PVT变化分析

主要参考文献

[1] Ravikanth Pappu, Ben Recht, Jason Taylor *et al. Physical one-way functions*. American Association for the Advancement of Science, **2002**: 2026–2030.

[2] Blaise Gassend, Dwaine Clarke, Marten Van Dijk *et al. Silicon physical random functions*, **2002**: 148–160.

[3] Daihyun Lim, Jae W Lee, Blaise Gassend *et al. Extracting secret keys from integrated circuits*. IEEE, **2005**: 1200–1205.

[4] Qingqing Chen, György Csaba, Paolo Lugli *et al.* "*The bistable ring puf: A new architecture for strong physical unclonable functions*". In: *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, **2011**: 134–141.

[5] Qingqing Chen, György Csaba, Paolo Lugli *et al.* "*Characterization of the bistable ring PUF*". In: *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012*, **2012**: 1459–1462.