物理不可克隆函数的建模与设计研究

Modeling and Design of Physical Unclonable Functions

报 告 人 唐文懿

导　　师 贾嵩

日　　期 2016-5-30

内容提要

背景介绍

- 技术背景
- 评价指标

建模推导

- BRPUF简介
- BRPUF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

背景介绍

- **密码：**
  - 保护隐私数据
  - 确保数据可靠
  - 身份认证
- **现代密码学：**
  - 加密算法
  - 通信协议
- **单向函数：**
  - 密码学的原型（基础）

技术背景

- 单向函数（One-Way Function）的存在性尚未被证明*
- 有许多应用于实际的“单向函数”：
  - RSA：整数分解问题
  - ECC：离散对数问题
- 物理单向函数：
  - 用物理原理实现单向函数
    - 实现简单
    - 成本低廉
  - 不可复制性

*https://en.wikipedia.org/wiki/Cryptography

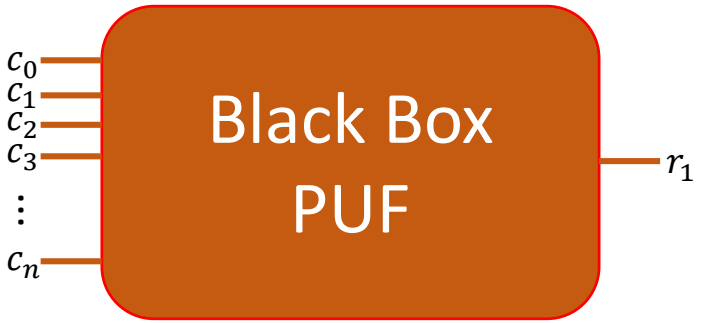
技术背景

◆**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

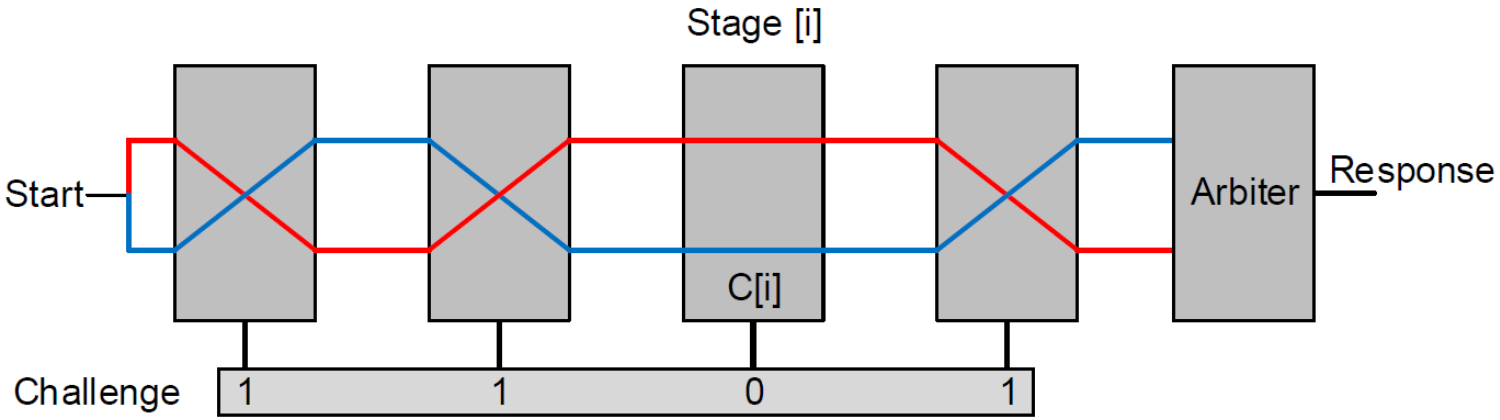
✓观测点



- **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[1]： B. Gassend, “*Silicon Physical Random Functions*”, 2002

评价指标

- 量化指标
  - 输出统计特性：
    1. （片内分布）随机性：$Rand = \frac{1}{N} \cdot \sum^{N} f(c_i)$
    2. （片间分布）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：$Reliability = \frac{1}{MN} \sum_{j}^{M} \sum_{i}^{N} |f(c') - f(c_i)|$
  - 逆向计算复杂度O(·)
- 理想指标：
  - 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

逆向算法——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

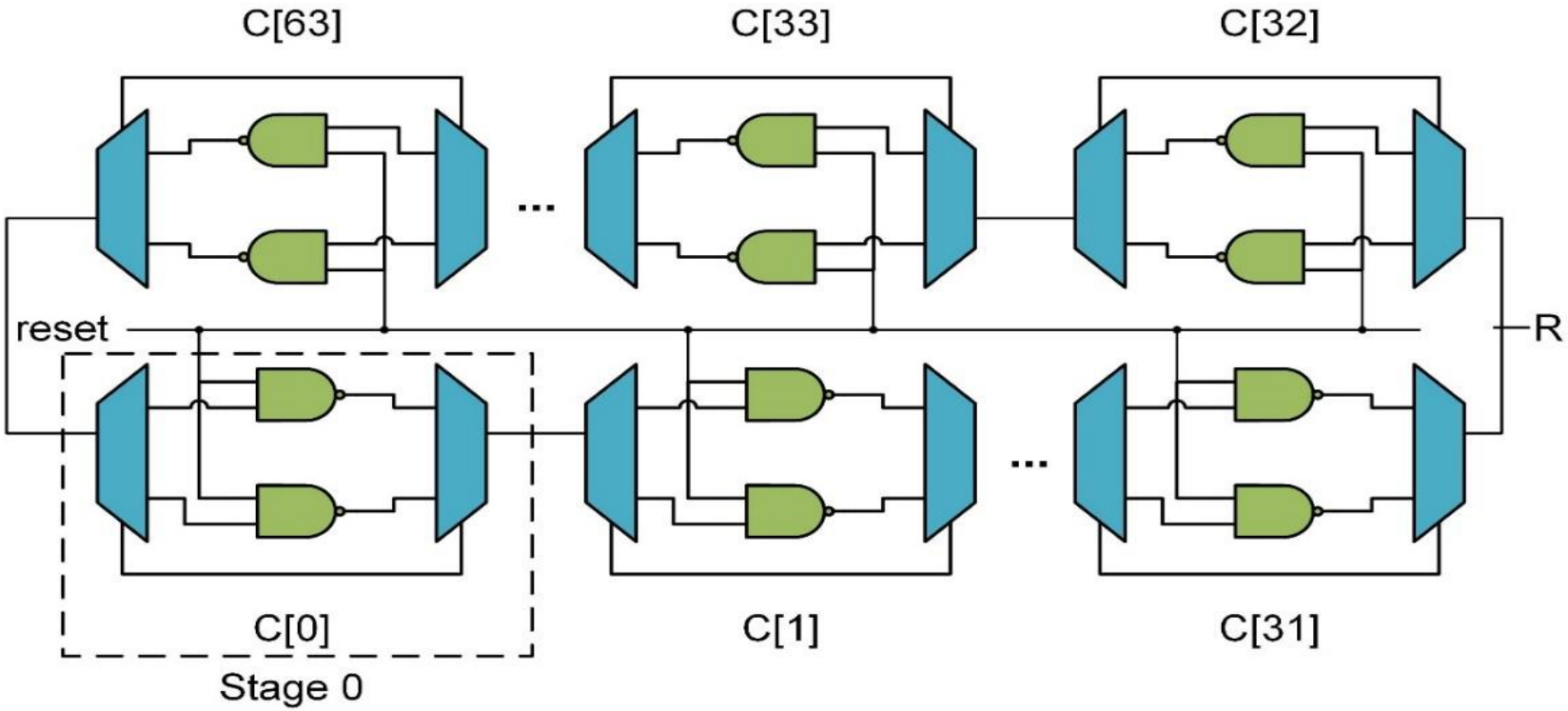
- 建模攻击评价指标：
  - 算法复杂度
  - 预测率，所需训练集大小

原理分析

背景介绍	建模推导	新结构介绍	总结
技术背景	BRPUF简介	电路结构	工作总结
评价指标	BRPUF建模	运作机制	前景展望
		测试结果	

BR-PUF

参考文献[2]：Q. Chen, *HOST 2011*, pp 134-141的设计：

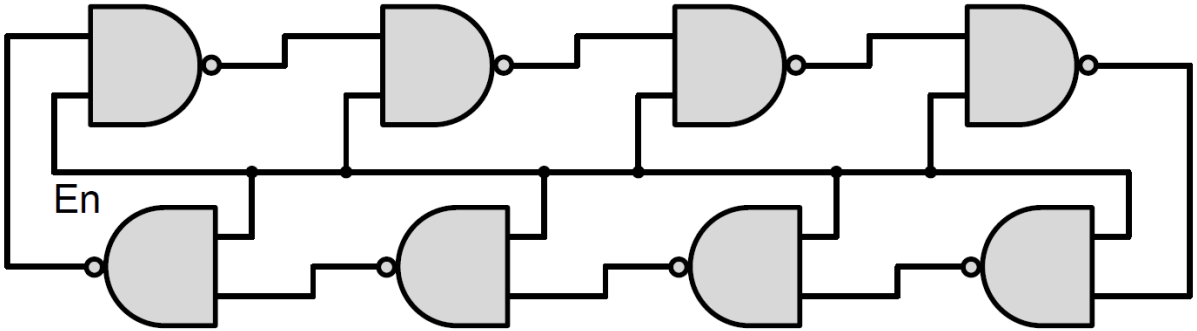


现有建模工作

- Q. Chen, *DATE 2012*, pp. 1459—1462:
  - BRPUF的统计分析
- D. Schuster et., al., *TRUST 2014*, pp. 101—109:
  - 单层神经网络模型

- 已有结论：
  - BRPUF存在统计偏差
  - SNN预测率90%
- 不足：
  - 偏差根源尚未明确
  - 单层网络模型粗糙

BR-PUF建模推导过程



分析占空比变化

- 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

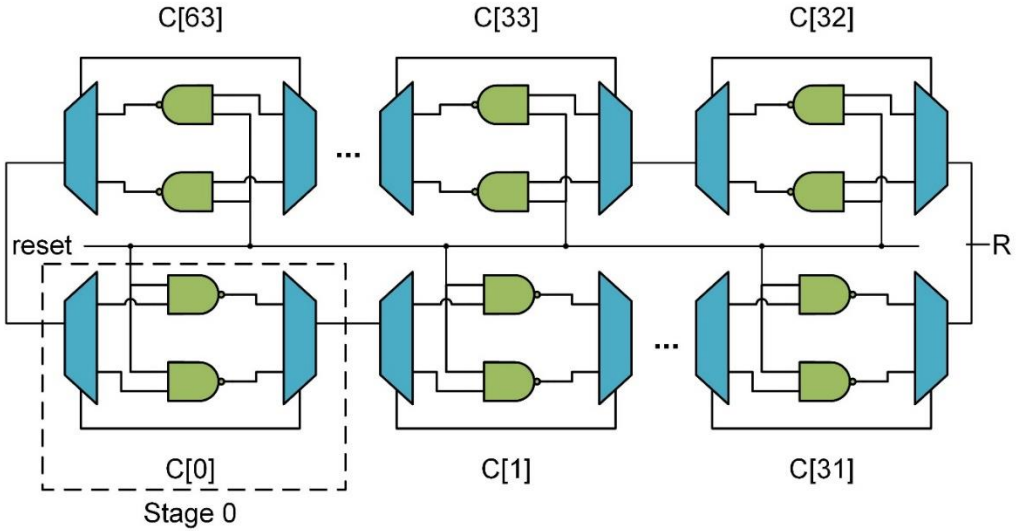
$$W_{i+1} = W_i + \frac{tf_i - tr_i}{T}(-1)^i$$

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

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

BR-PUF建模推导过程

◆每级两个与非门tr，tf设为p, q, r, s



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

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

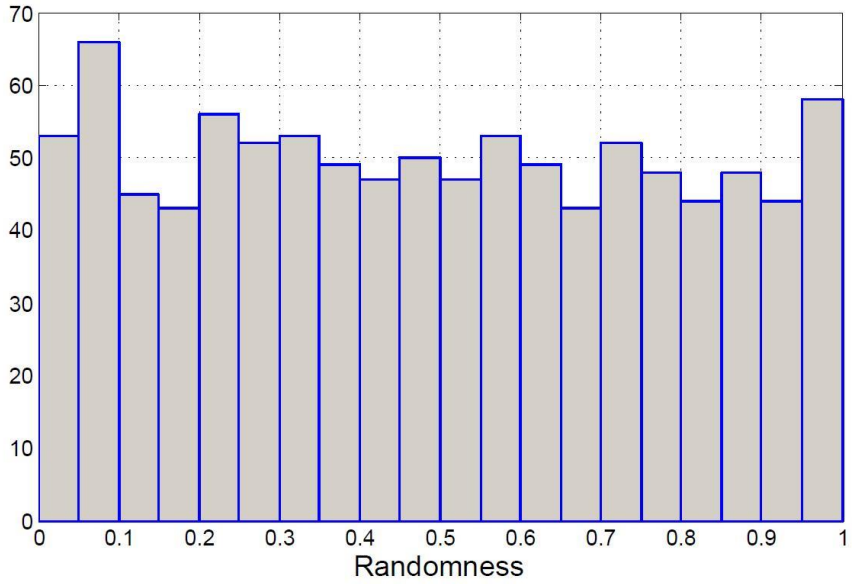
复杂度：$O(m \cdot \mathrm{Dim}(d)) = O(mn)$

对已有结论的延伸

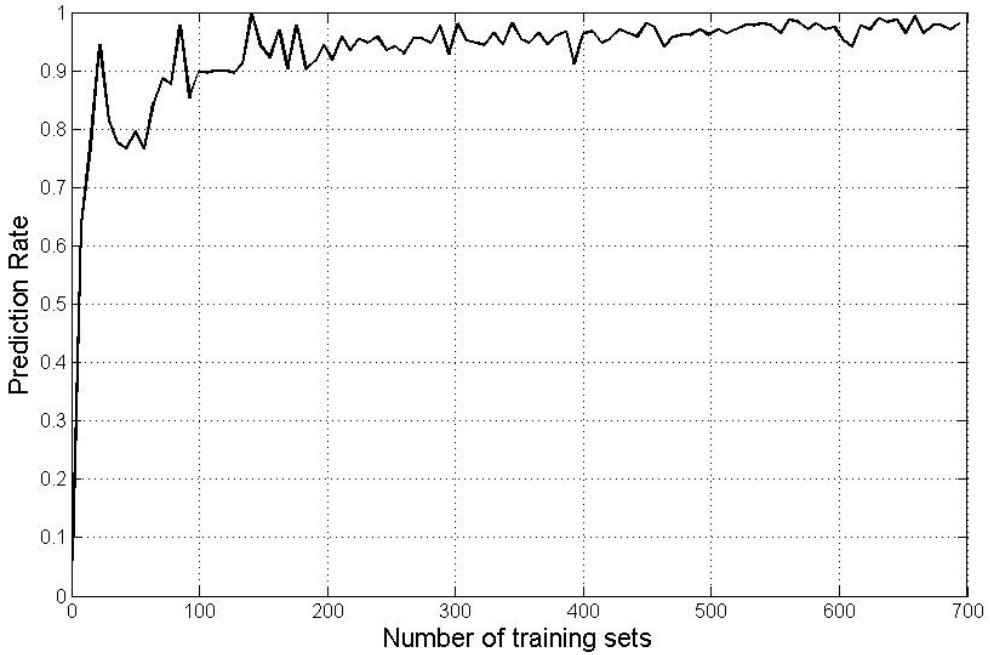
- 收敛状态只与δ有关 $R = sgn(\delta) = A'C + B$
- δ的分布如下：
  - $\mu(\delta) = B + \frac{\sum A'C}{2^N} = B, \sigma(\delta) = \frac{1}{2^{N/2}}\sqrt{\sum (A'C)^2} = \sqrt{\sum \alpha_i^2}$
- 则考察B的分布：
  - $\sigma(B) = \sqrt{\sum(\sigma^2(\beta_i))}$
- 推论：片内分布与δ均值的方差和δ方差的方差之比相关
  - $|Rand - 0.5| \propto \frac{\sigma(\sigma(\delta))}{\sigma(\mu(delta))}$
  - BRPUF比值大，片内分布偏差大

建模攻击模拟

BRPUF片内分布仿真
N=32bit

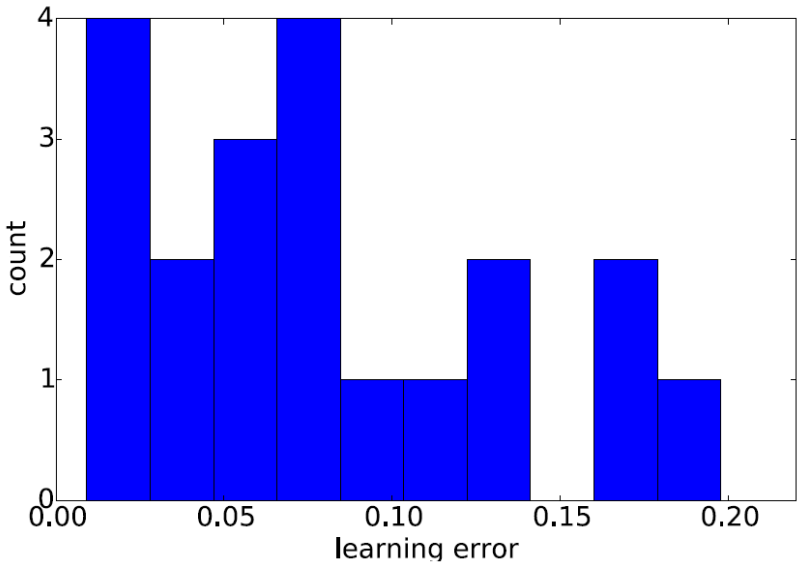


建模攻击预测率仿真曲线
N=32bit, m=x-axis

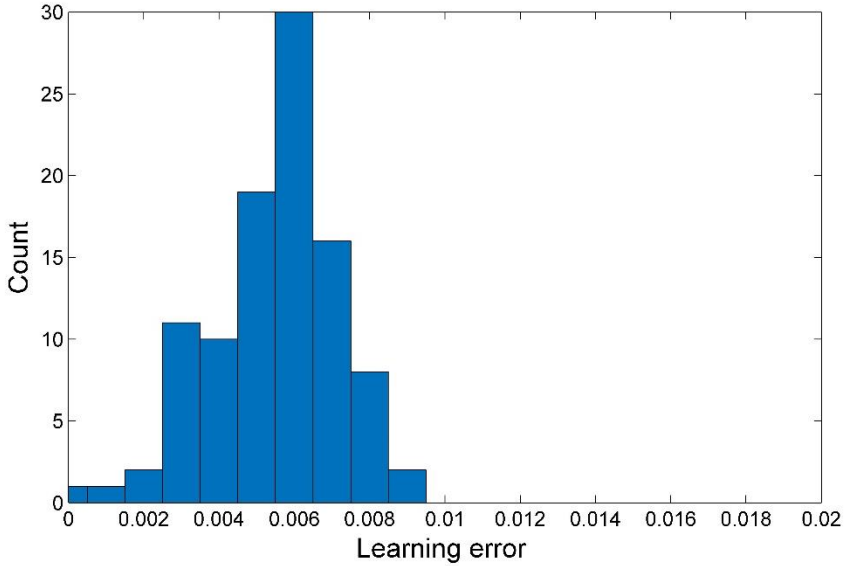


与SNN模型对比

单层神经网络拟合22个BRPUF的预测率分布图[3]



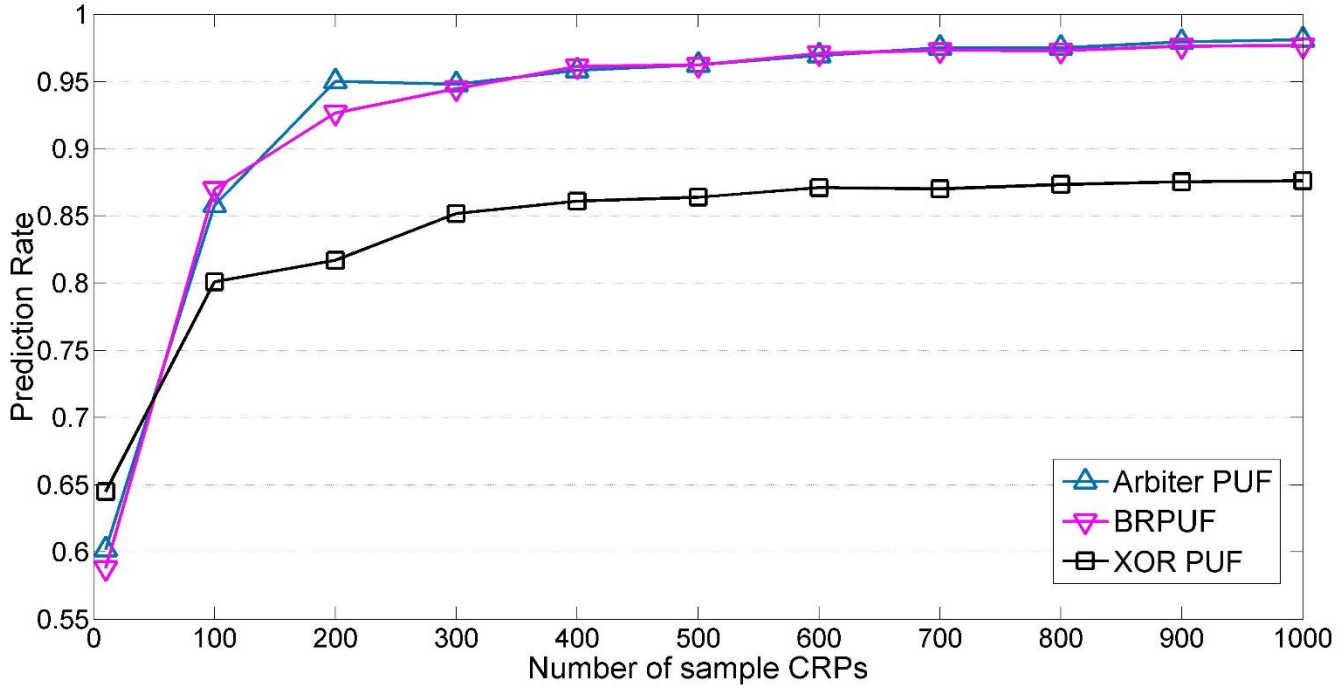
本模型对100个BRPUF的预测率分布图



[3] Dieter Schuster and Robert Hesselbarth, *TRUST 2014*, pp. 101—109

与其他模型间对比

- 不同PUF适用不同模型，本模型同经典仲裁PUF模型和XOR模型进行横向对比，比较本模型针对BRPUF的预测率和训练集



新结构介绍

背景介绍
- 技术背景
- 评价指标

建模推导
- BRPUF简介
- BRPUF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

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

Strong PUF研究现状

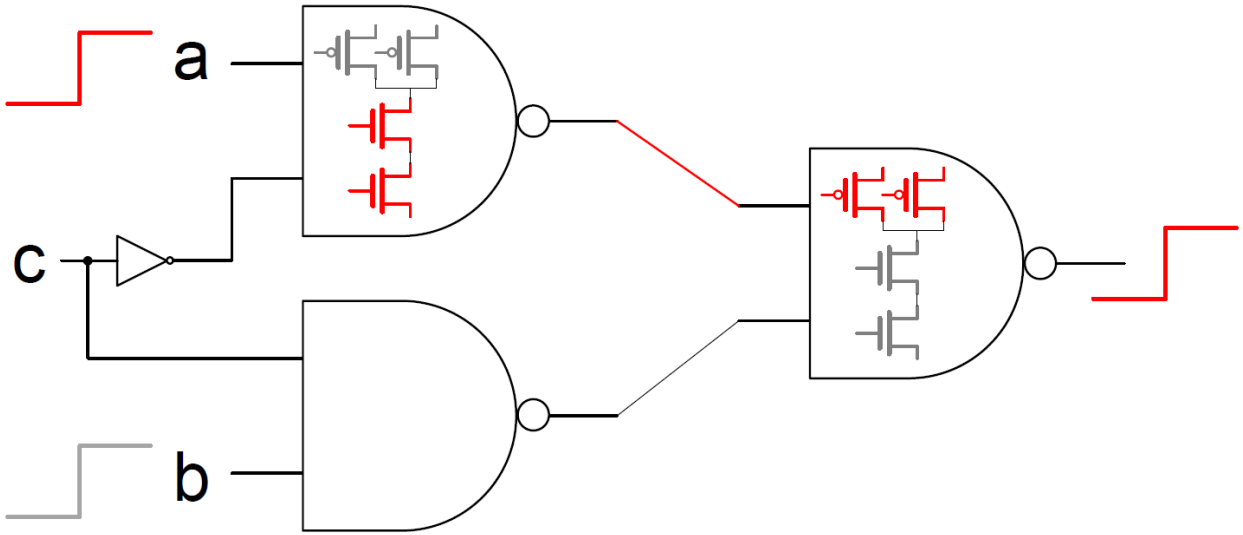
- 通过增加位宽和XOR算法提高建模算法复杂度[4]

PUF Type	激励位宽	预测率	输出异或个数	训练集CRP	学习时间
仲裁型PUF	128	99%	-	5.5k	0.51s
XOR PUF	64	99%	4	12k	3min42s
		99%	5	80k	2h8min
		99%	6	200k	31h1min
	128	99%	4	24k	2h52min
		99%	5	500k	16h36min
		-	6	-	-
Lightweight PUF	64	99%	4	12k	1h28min
		99%	5	300k	13h6min
		-	6	-	-
	128	99%	4	500k	59min42s
		99%	5	1000k	267days
		-	6	-	-

[4] A. Mahmoud, U. Ruhrmair & M. Majzoobi, *IACR* 2013: 632

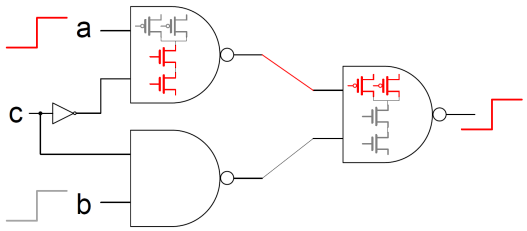
交换器逻辑结构

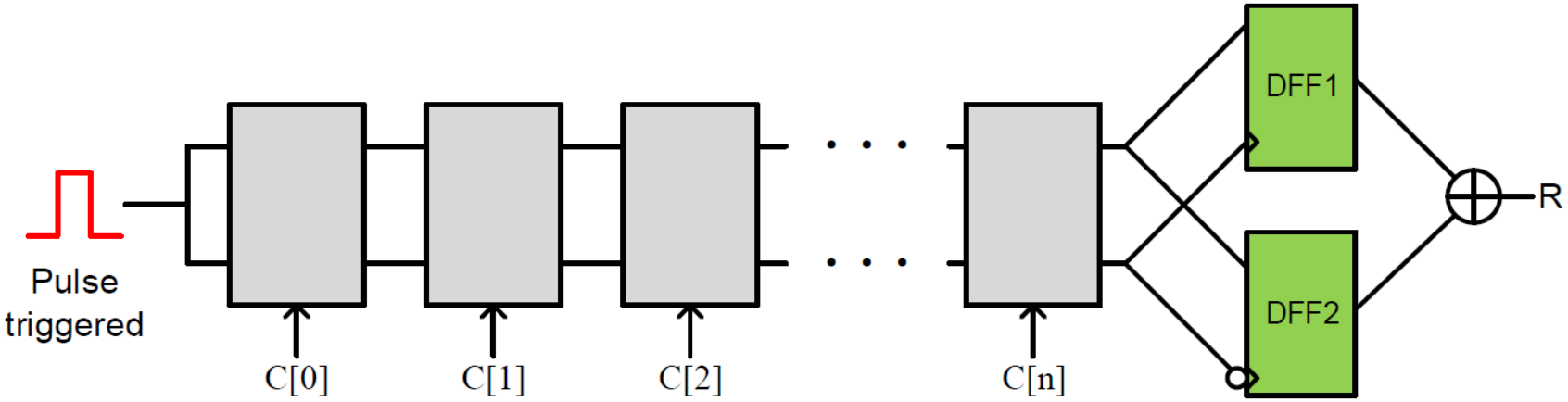
- 交换器实现细节
  - 驱动上升沿/下降沿是不同MOS管



PA-PUF

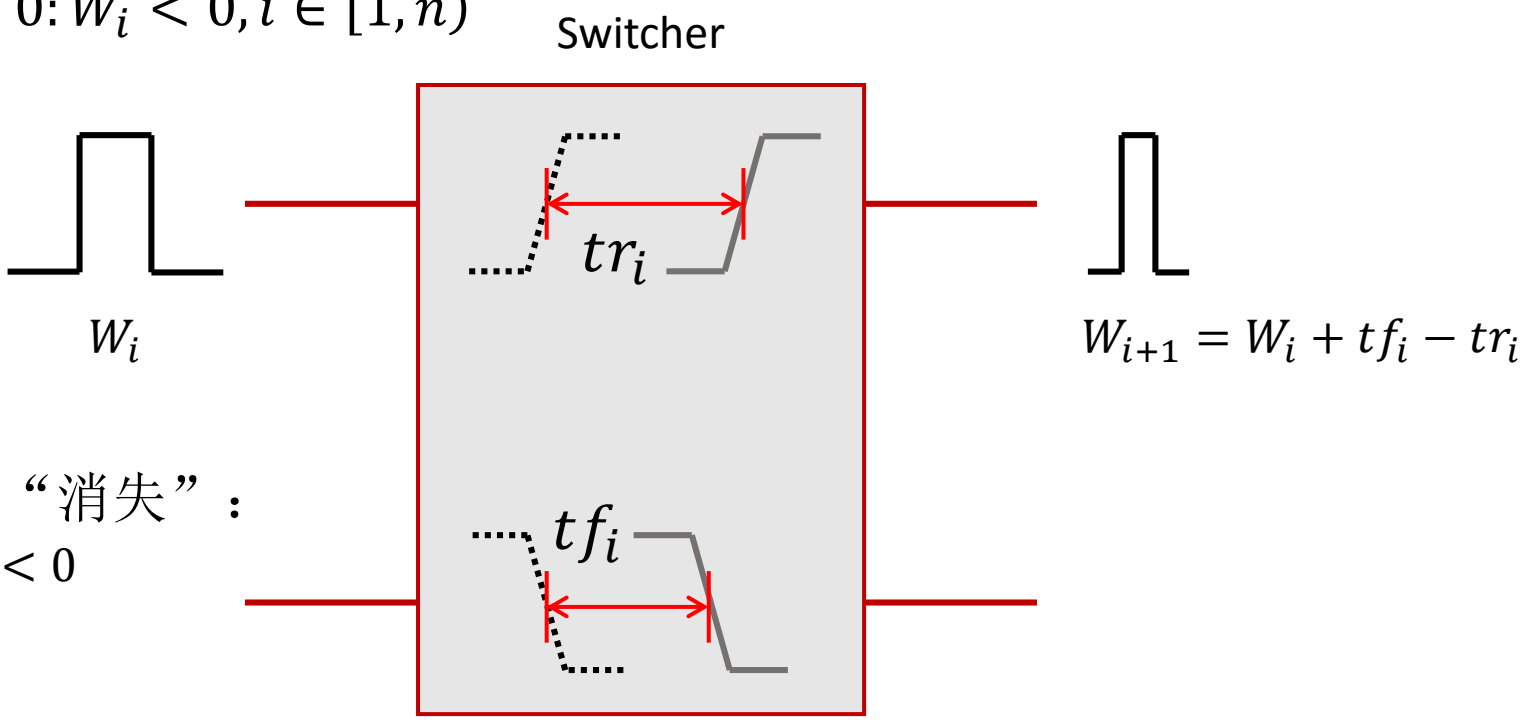
- 结构复用，减少面积
- Pulse Arbiter PUF
  - DFF1—正边沿触发
  - DFF2—负边沿触发





脉冲信号传递

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

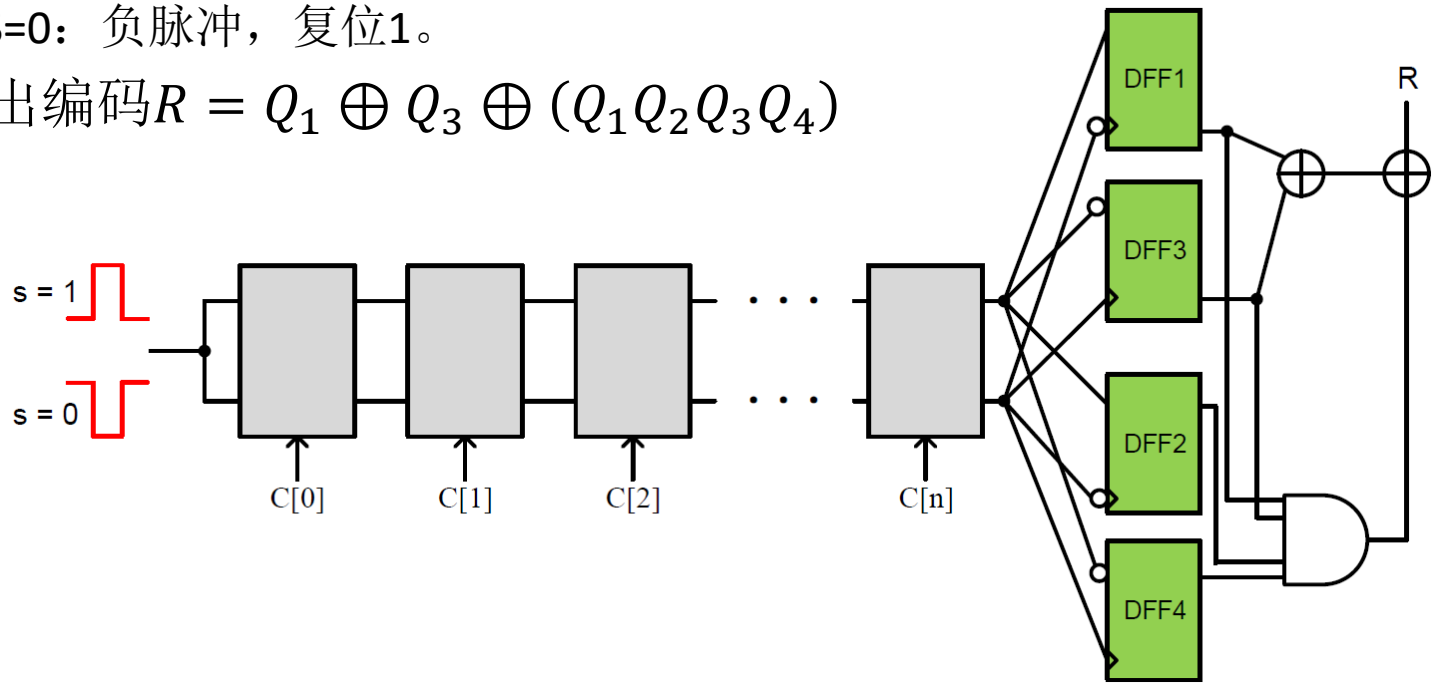


- 信号“消失”：
  - $W < 0$

RPA-PUF

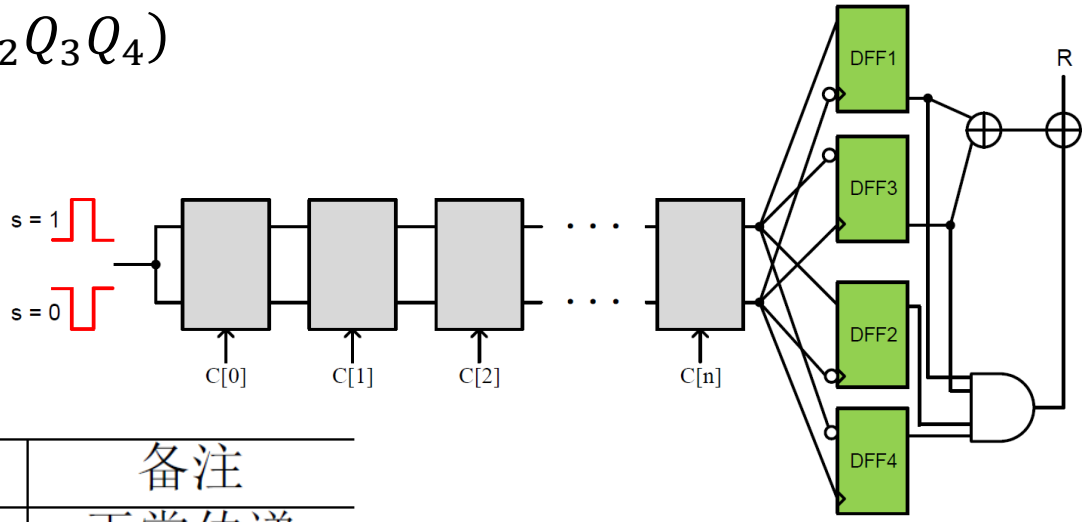
随机脉冲PUF，随机掩码，提高复杂度

- 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

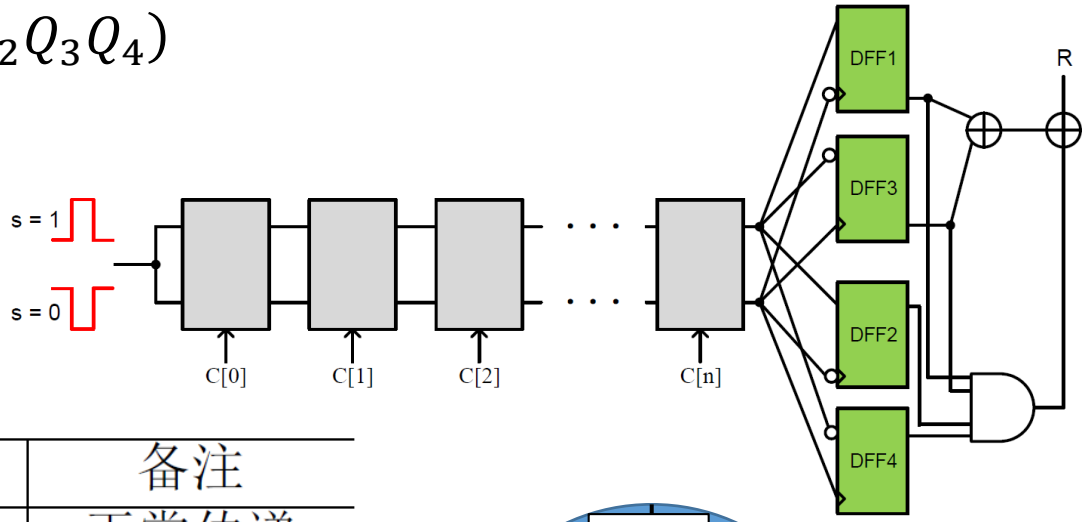
- $R = Q_1 \oplus Q_3 \oplus (Q_1 Q_2 Q_3 Q_4)$
  - 均不“消失”；
  - “消失”其一；
  - 均“消失”。



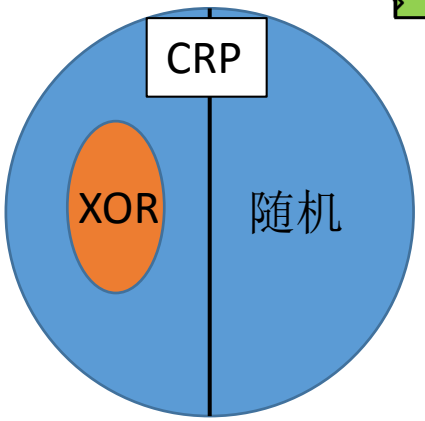
s	Q_1	Q_2	Q_3	Q_4	备注
x	0	1	0	1	正常传递
x	0	1	1	0	正常传递
x	1	0	0	1	正常传递
x	1	0	1	0	正常传递
1	1	1	1	1	负脉冲消失
0	0	0	0	0	正脉冲消失

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”。



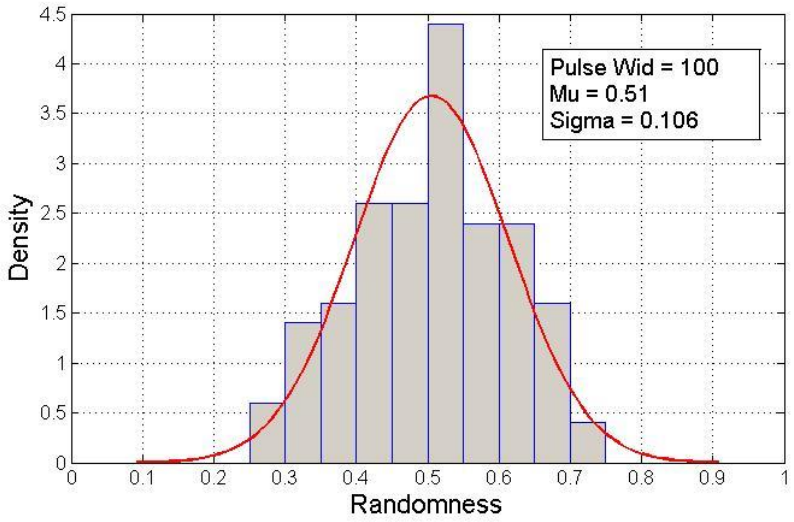
s	Q_1	Q_2	Q_3	Q_4	备注
x	0	1	0	1	正常传递
x	0	1	1	0	正常传递
x	1	0	0	1	正常传递
x	1	0	1	0	正常传递
1	1	1	1	1	负脉冲消失
0	0	0	0	0	正脉冲消失

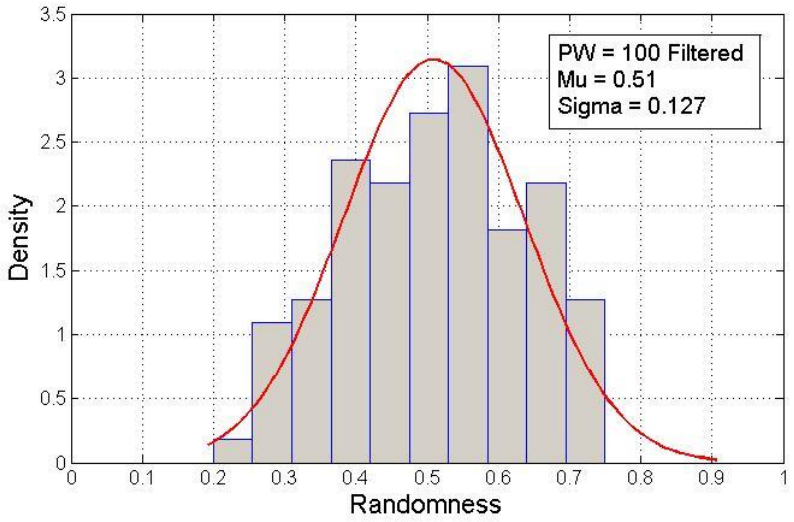


多次采样，舍弃随机响应

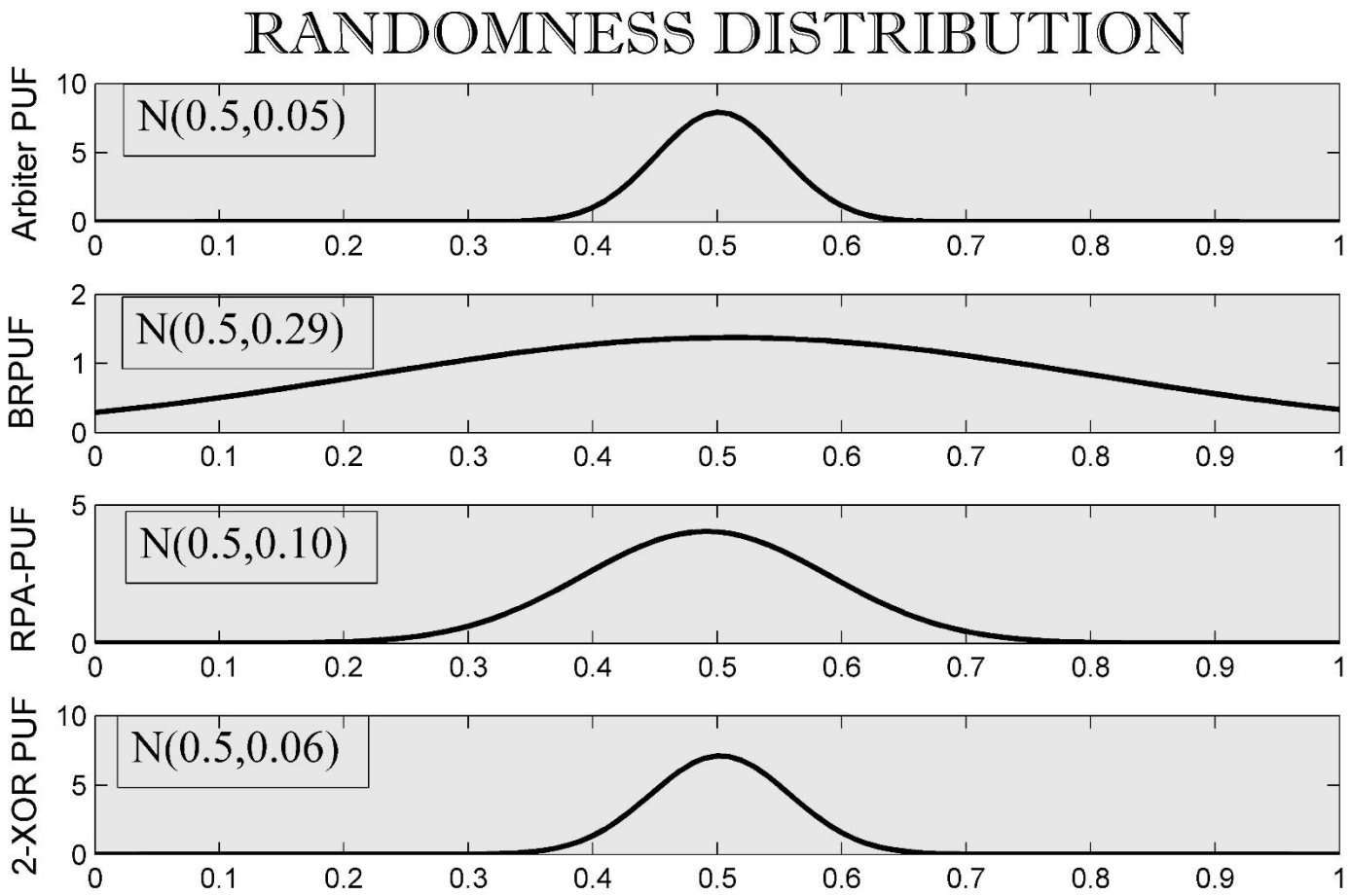
实验结果

- 单次采样：=XOR+随机掩码
- 多次采样：近似XOR

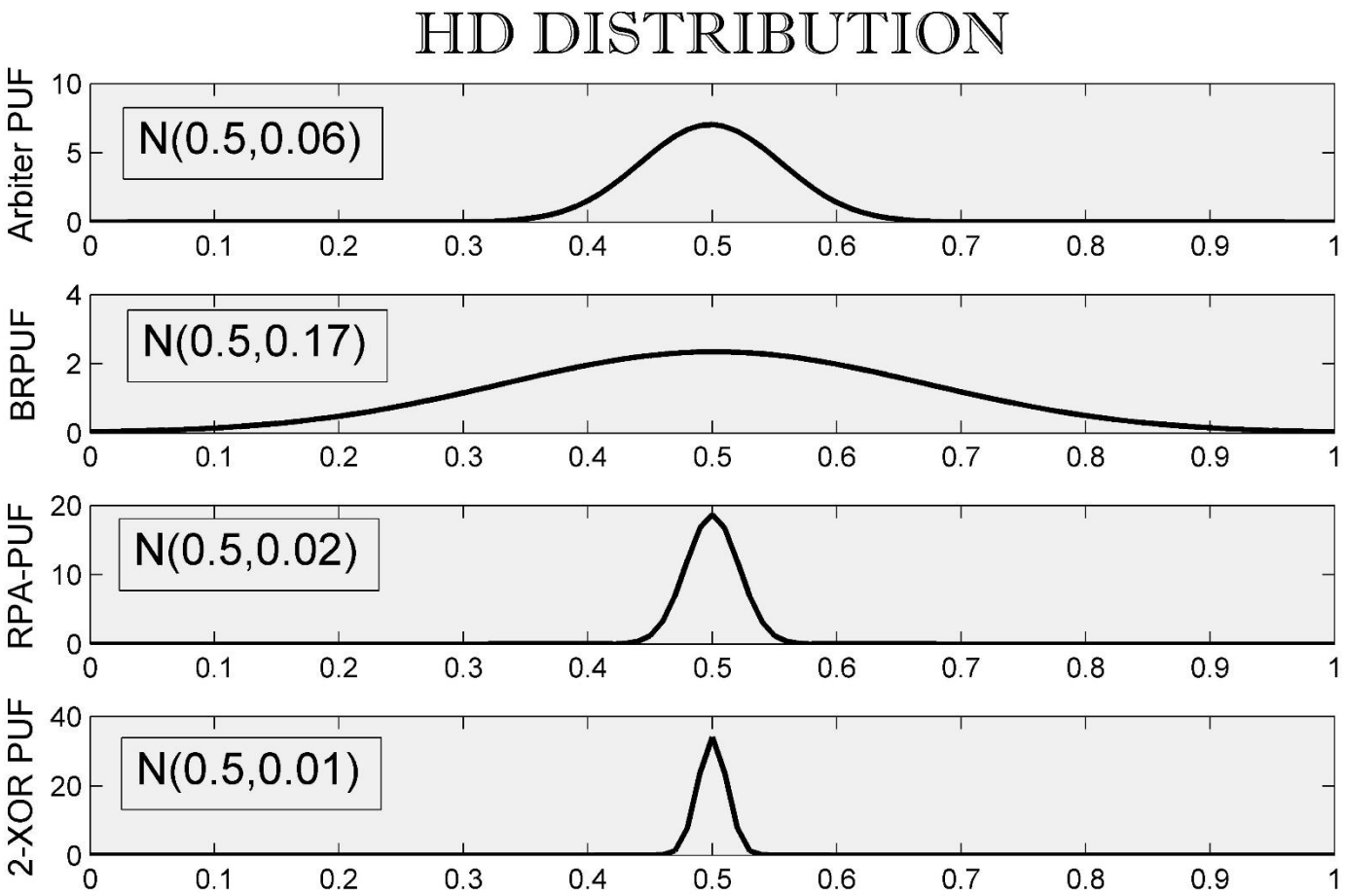




随机性分布对比

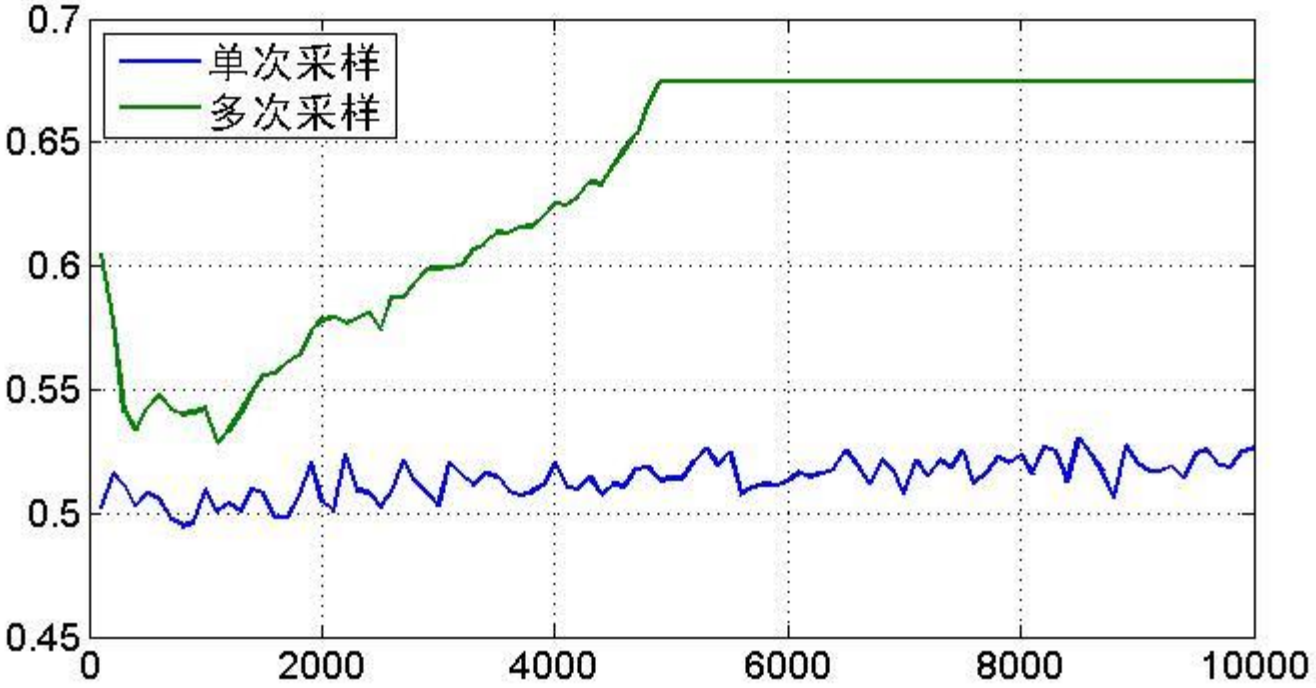

RANDOMNESS DISTRIBUTION
Arbiter PUF
N(0.5,0.05)
BRPUF
N(0.5,0.29)
RPA-PUF
N(0.5,0.10)
2-XOR PUF
N(0.5,0.06)
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

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

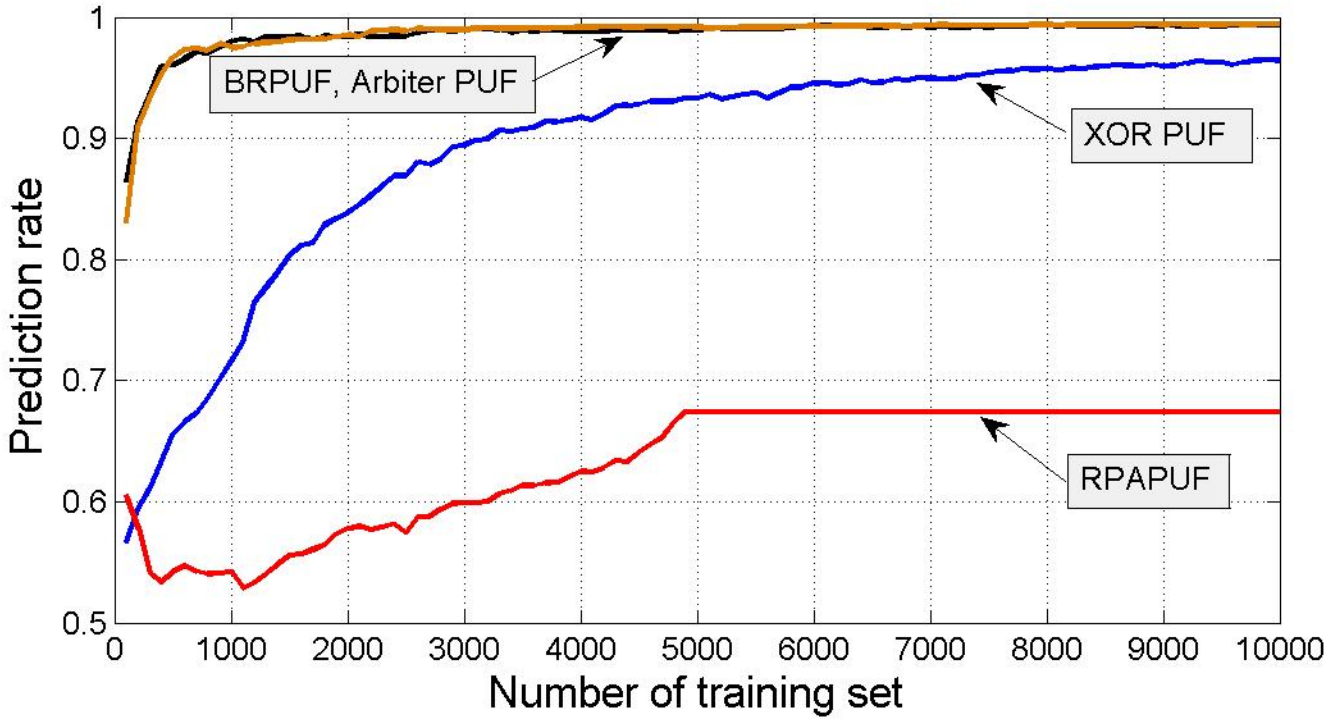
RPA-PUF建模攻击

- SVM结果
  - RPAPUF使用XOR模型



建模攻击结果对比

- SVM结果
  - RPAPUF使用XOR模型



高预测率

低预测率

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；
  - 新型掩码方式
  - 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

攻读硕士学位期间发表的论文

[1] **Wenyi Tang**, Song Jia, and Yuan Wang, *"A Dual-voltage Single-rail Dynamic DPA-resistant Logic Based on Charge Sharing Mechanism"*, Electron Devices and Solid-State Circuits (EDSSC), 2015 IEEE International Conference on, **2013**: 483-486

[2] **Wenyi Tang**, Song Jia, and Yuan Wang, *"A Short-time Three-phase Single-rail Precharge Logic Against Differential Power Analysis"*, IEICE Transactions on Electronics (Accepted)

谢谢！