CS771 : Assignment 1

Team Members

Anaavi Alok
Anurag Bohra
Dhwanit Balwani
Kartikeya Raghuvanshi
Prakhar Pratap Mall
Ujwal Kumar

1 Simple XORRO PUF

A simple XORRO PUF contains two XORROs each with R configuration bits for each of their R XORs in the ring oscillator.

Consider the first XORRO, and let the time taken by the i^{th} XOR gate in it, before giving its output, when the input to that gate is 00, 01, 10 and 11 be $\alpha_{00}^{i-1}, \alpha_{01}^{i-1}, \alpha_{10}^{i-1}, \alpha_{11}^{i-1}$ respectively.

Similarly for the second XORRO, the corresponding times are $\beta_{00}^{i-1}, \beta_{00}^{i-1}, \beta_{00}^{i-1}, \beta_{00}^{i-1}$ respectively.

Now let us try to find to find the time period of the oscillation for both the XORROs, given a particular R configuration bits, namely, $a_0, a_1, ...a_R$.

Time period for first XORRO(given as sum of time it takes for oscillator to switch from to 0 to 1 and time it takes for oscillator to switch from 1 to 0) is given as,

$$T_1 = t_{0\to1} + t_{1\to0}$$

where,

$$t_{0\to1} = \alpha_{00}^0(1-a_0) + \alpha_{01}^0(a_0) + \alpha_{00}^1(1-a_1) + \alpha_{01}^1(a_1) + ... + \alpha_{00}^{R-1}(1-a_{R-1}) + \alpha_{01}^{R-1}(a_{R-1})$$
$$t_{1\to0} = \alpha_{10}^0(1-a_0) + \alpha_{11}^0(a_0) + \alpha_{10}^1(1-a_1) + \alpha_{11}^1(a_1) + ... + \alpha_{10}^{R-1}(1-a_{R-1}) + \alpha_{11}^{R-1}(a_{R-1})$$

So that T_1 becomes,

$$\begin{gathered} T_1 = (\alpha_{00}^0 + \alpha_{10}^0)(1-a_0) + (\alpha_{01}^0 + \alpha_{11}^0)(a_0) \\ +(\alpha_{00}^1 + \alpha_{10}^1)(1-a_1) + (\alpha_{01}^1 + \alpha_{11}^1)(a_1) + ... \\ .... + (\alpha_{00}^{R-1} + \alpha_{10}^{R-1})(1-a_{R-1}) + (\alpha_{01}^{R-1} + \alpha_{11}^{R-1})(a_{R-1}) \end{gathered}$$

Similarly, the time period for the second XORRO is given as,

$$\begin{gathered} T_2 = (\beta_{00}^0 + \beta_{10}^0)(1-a_0) + (\beta_{01}^0 + \beta_{11}^0)(a_0) \\ +(\beta_{00}^1 + \beta_{10}^1)(1-a_1) + (\beta_{01}^1 + \beta_{11}^1)(a_1) + ... \\ .... + (\beta_{00}^{R-1} + \beta_{10}^{R-1})(1-a_{R-1}) + (\beta_{01}^{R-1} + \beta_{11}^{R-1})(a_{R-1}) \end{gathered}$$

Now the time difference between the two gives us the delay at the COUNTER in the XORRO PUF arrangement,

$$\Delta T = \sum_{i=0}^{R-1}(1-a_i)(\beta_{00}^i + \beta_{10}^i - \alpha_{00}^i - \alpha_{10}^i) + \sum_{i=0}^{R-1}(a_i)(\beta_{01}^i + \beta_{11}^i - \alpha_{01}^i - \alpha_{11}^i)$$

$$\Delta T = \sum_{i=0}^{R-1}(\beta_{00}^i + \beta_{10}^i - \alpha_{00}^i - \alpha_{10}^i) + \sum_{i=0}^{R-1}(a_i)(-\beta_{00}^i + \beta_{01}^i - \beta_{10}^i + \beta_{11}^i + \alpha_{00}^i - \alpha_{01}^i + \alpha_{10}^i - \alpha_{11}^i)$$

Above equation can be written in vector notation as,

$$\Delta T = \left[\boldsymbol{w}^T\right]_{1\times R}\left[\boldsymbol{a}\right]_{R\times 1} + b$$

where $b = \sum_{i=0}^{R-1}(\beta_{00}^i + \beta_{10}^i - \alpha_{00}^i - \alpha_{10}^i)$ and the **w** and **a** vectors are defined as,

a = $\begin{bmatrix} a_0 \\ a_1 \\ . \\ . \\ a_{R-1} \end{bmatrix}$ and **w** = $\begin{bmatrix} -\beta_{00}^0 + \beta_{01}^0 - \beta_{10}^0 + \beta_{11}^0 + \alpha_{00}^0 - \alpha_{01}^0 + \alpha_{10}^0 - \alpha_{11}^0 \\ -\beta_{00}^1 + \beta_{01}^1 - \beta_{10}^1 + \beta_{11}^1 + \alpha_{00}^1 - \alpha_{01}^1 + \alpha_{10}^1 - \alpha_{11}^1 \\ . \\ . \\ -\beta_{00}^{R-1} + \beta_{01}^{R-1} - \beta_{10}^{R-1} + \beta_{11}^{R-1} + \alpha_{00}^{R-1} - \alpha_{01}^{R-1} + \alpha_{10}^{R-1} - \alpha_{11}^{R-1} \end{bmatrix}$

The R configuration bits represented here as **a** are the challenge bits $\phi(\boldsymbol{c})$ given to us. Also the sign of ΔT determines the final response. Hence the final response can be given as,

$$\frac{1 + sign(\Delta T)}{2}$$

$$\frac{1 + sign(\boldsymbol{w}^T\phi(\boldsymbol{c}) + b)}{2}$$

Hence PROVED that there exists a linear model for simple XORRO PUF.

2 Advanced XORRO PUF

Now an advanced XORRO PUF will have 2^S XORROs. So we need to write the expression for time period of each of these XORROs. Using the results from previous question and generalising for i^{th} XORRO, we get,

$$\begin{aligned} T_i = ((\alpha_i)_{00}^0 + (\alpha_i)_{10}^0)(1-a_0) + ((\alpha_i)_{01}^0 + (\alpha_i)_{11}^0)(a_0) \\ +((\alpha_i)_{00}^1 + (\alpha_i)_{10}^1)(1-a_1) + ((\alpha_i)_{01}^1 + (\alpha_i)_{11}^1)(a_1) + ... \\ .... + ((\alpha_i)_{00}^{R-1} + (\alpha_i)_{10}^{R-1})(1-a_{R-1}) + ((\alpha_i)_{01}^{R-1} + (\alpha_i)_{11}^{R-1})(a_{R-1}) \end{aligned}$$

Now let the XORRO being selected for MUX1 will have a time period of T_1 and XORRO selected for MUX2 will have a time period of T_2,

$$T_1 = \sum_{i=0}^{2^S-1} T_i \times (C_1)_i$$

$$T_2 = \sum_{i=0}^{2^S-1} T_i \times (C_2)_i$$

where, $(C_1)_i$ and $(C_2)_i$ are selection bit calculated from S_1 and S_2 bits given to us as input in the following way:

Considering S_1 and S_2 as binary numbers, we first convert it into decimal number, say p and q. Now we create two matrices $[\boldsymbol{C_1}]$ and $[\boldsymbol{C_2}]$ which has value 1 at indices p and q respectively, while rest values are set to zero.

The time delay therefore is calulated as,

$$\Delta T = T_2 - T_1$$

$$\Delta T = \sum_{i=0}^{2^S-1} T_i((C_1)_i - (C_2)_i)$$

Let $(C_1)_i - (C_2)_i$ be denoted as ψ_i. Expanding the summation we get,

$$\Delta T = \sum_{i=0}^{2^S-1} \sum_{j=0}^{R-1} \psi_i(((\alpha_i)_{00}^j + (\alpha_i)_{10}^j)(1-a_j) + ((\alpha_i)_{01}^j + (\alpha_i)_{11}^j)(a_j))$$

$$\Delta T = \sum_{i=0}^{2^S-1} \sum_{j=0}^{R-1} \psi_i((\alpha_i)_{00}^j + (\alpha_i)_{10}^j) + \sum_{i=0}^{2^S-1} \sum_{j=0}^{R-1} ((\alpha_i)_{01}^j + (\alpha_i)_{11}^j - (\alpha_i)_{00}^j - (\alpha_i)_{10}^j)a_j\psi_i$$

$$\Delta T = b + \sum_{i=0}^{2^S-1} \sum_{j=0}^{R-1} ((\alpha_i)_{01}^j + (\alpha_i)_{11}^j - (\alpha_i)_{00}^j - (\alpha_i)_{10}^j)a_j\psi_i$$

writing this in matrix notation,

$$\Delta T = b + \sum_{i=0}^{2^S-1} ([\boldsymbol{w_i^T}])[\boldsymbol{a}]\psi_i$$

$$\Delta T = b + \sum_{i=0}^{2^S-1} ([\boldsymbol{w_i^T}])[\boldsymbol{\tilde{a}_i}]$$

$$\Delta T = \left[\boldsymbol{w}^T\right][\boldsymbol{A}] + b$$

Hence just as in the previous question, there exsists a linear model for advanced XORRO PUF.

3 Python Code

Code Link: https://home.iitk.ac.in/ ppmall20/protected.zip

4 Experimental Outcomes

LinearSVC	Hinge Loss	Sq Hinge Loss
accuracy	0.91785	0.917373
model size	8781	8787
train time(sec)	33.178	28.562
test time(sec)	0.596	0.507

Table 1: Hinge Loss vs Squared Hinge Loss Comparison

LinearSVC.	High Tolerance	Medium Tolerance	Low Tolerance
accuracy	0.917965	0.917955	0.91808
model size	8781	8779	8779
train time(sec)	36.248	14.74	4.95
test time(sec)	0.621	0.507	0.62915

Table 2: Variations because of changing tolerance values in LinearSVC

Logistic Reg.	High Tolerance	Medium Tolerance	Low Tolerance
accuracy	0.91709	0.91709	0.91709
model size	8897	8897	8897
train time(sec)	5.22	5.27	5.47
test time(sec)	0.588	0.624	0.604

Table 3: Variations because of changing tolerance values in Logistic Reg.