CS771 Introduction to Machine Learning

Assignment 1

Naveen Kumar	Tejaswa	Gargi Jain
210654	211110	210379
knaveen21@iitk.ac.in	tejaswa21@iitk.ac.in	gargijain21@iitk.ac.in

Priyanshu Biswas
210779
priyanshu21@iitk.ac.in

Question 1

Introduction to Arbiter PUFs

Arbiter Physically Unclonable Functions (PUFs) are hardware systems that leverage inherent variations in data transmission speeds to enhance security. These systems consist of multiple multiplexers (MUXes) controlled by a series of selection bits. Each unique configuration of these bits, known as a "challenge," results in a distinct output or "response," determined by the particular hardware characteristics of the PUF.

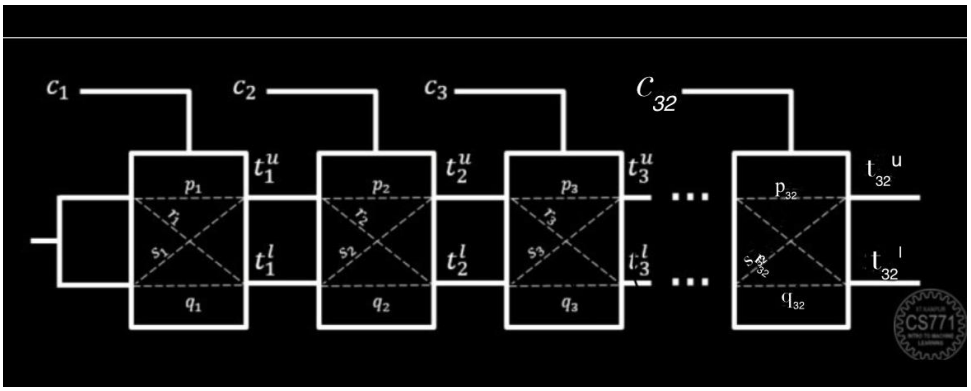

Figure 1: 32 switch PU

Using the class lectures we have following formulaes:

$$t_i^u = (1 - c_i) \cdot (t_{i-1}^u + p_i) + c_i \cdot (t_{i-1}^l + s_i) \quad \text{(i)}$$

$$t_i^l = (1 - c_i) \cdot (t_{i-1}^l + q_i) + c_i \cdot (t_{i-1}^u + r_i) \quad \text{(ii)}$$

Where:

- t_i^u is the time at which upper signal exits the i-th switch
- t_i^l is the time at which lower signal exits the i-th switch
- c_i dictates which previous exit time gets carried forward. It is 1 if the upper signal reaches first to the $i-1$-th switch and 0 if the lower signal reaches first.

adding equation (i) and (ii) we get:

$$t_i^u + t_i^l = t_{i-1}^u + t_{i-1}^l + (1 - c_i) \cdot (p_i + q_i) + c_i \cdot (r_i + s_i)$$

For n = 32:

$$t_{32}^u + t_{32}^l = t_{31}^u + t_{31}^l + (1 - c_{32}) \cdot (p_{32} + q_{32}) + c_{32} \cdot (r_{32} + s_{32})$$

Using Induction we can write it as :

$$t_{32}^u + t_{32}^l = \sum_{i=1}^{32}((1 - c_i) \cdot (p_i + q_i) + c_i \cdot (r_i + s_i)) \tag{iii}$$

Using the formulae from class lectures:
The equation is given by:

$$\Delta_i = d_i \cdot \Delta_{i-1} + \alpha_i \cdot d_i + \beta_i$$

Where:

- Δ_i is the time delay between the upper signal and the lower signal at i-th switch *i.e* $t_i^u - t_i^l$
- $d_i = (1 - 2c_i)$
- $\alpha_i = (p_i - q_i + r_i - s_i)/2$
- $\beta_i = (p_i - q_i - r_i + s_i)/2$
- $\Delta_0 = 0$

$$\Delta_2 = d_2 \cdot \Delta_1 + \alpha_2 \cdot d_2 + \beta_2$$
$$\Delta_2 = d_2 \cdot \Delta_1 + \alpha_2 \cdot d_2 + \beta_2$$
$$\Delta_3 = d_3 \cdot \Delta_2 + \alpha_3 \cdot d_3 + \beta_3$$
$$\Delta_1 = \alpha_1 \cdot d_1 + \beta_1$$

$$\Delta_2 = d_2 \cdot \Delta_1 + \alpha_2 \cdot d_2 + \beta_2$$
$$\Delta_2 = d_2 \cdot \Delta_1 + \alpha_2 \cdot d_2 + \beta_2$$
$$\Delta_3 = d_3 \cdot \Delta_2 + \alpha_3 \cdot d_3 + \beta_3$$

Using Induction we get:

$$t_{32}^u - t_{32}^l = \Delta_{32} = \sum_{i=1}^{32} (\alpha_i d_i + \beta_i) \prod_{j=i+1}^{32} (d_j)$$

Substituting values of α_i , β_i and d_i we get:

$$t_{32}^u - t_{32}^l = \sum_{i=1}^{32} ((1-c_i)(p_i - q_i) - c_i(r_i - s_i)) \prod_{j=i+1}^{32} (1 - 2c_j) \tag{iv}$$

Adding equation (iii) and (iv) we get expression for t_{32}^u ,

$$t_{32}^u = \frac{1}{2} \sum_{i=1}^{32} [(1-c_i)(p_i + q_i) + c_i(r_i + s_i) + \prod_{j=i+1}^{32} (1 - 2c_j)((1-c_i)(p_i - q_i) - c_i(r_i - s_i))]$$

After substituting

- c_i = (1 - d_i)/2
- $p_i + q_i - r_i - s_i = A_i$
- $p_i - q_i + r_i - s_i = B_i$

we get:

$$t_{32}^u = \frac{1}{4} \sum_{i=1}^{32} [2p_i + 2q_i - A_i + d_i A_i + \prod_{j=i+1}^{32} d_j (2p_i - 2q_i - B_i + d_i B_i)]$$

Substitute

- $2p_i + 2q_i - A_i = p_i + q_i + r_i + s_i = C_i$
- $2p_i - 2q_i - B_i = p_i - q_i - r_i + s_i = D_i$

we get:

$$t_{32}^u = \frac{1}{4} \sum_{i=1}^{32} [C_i + d_i A_i + \prod_{j=i+1}^{32} d_j (D_i + d_i B_i)]$$

Now to convert this equation in the form $W^\top \phi(c) + b = t_u(c)$ we take

$$b = \sum_{i=1}^{32} \frac{C_i}{4}$$

where ,

$$\phi(c) = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ \vdots \\ d_{32} \\ d_1 d_2 d_3 ....d_{32} \\ d_2 d_3 ....d_{32} \\ \vdots \\ \vdots \\ d_{31} d_{32} \end{pmatrix}$$

$$W = \frac{1}{4} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \vdots \\ A_{32} + B_{32} + D_{31} \\ B_1 \\ B_2 + D_1 \\ \vdots \\ \vdots \\ B_{31} + D_{30} \end{pmatrix}$$

Question 2

We calculate the dimension of the linear model using

$$\phi(c) = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ \vdots \\ d_{32} \\ d_1 d_2 d_3 .... d_{32} \\ d_2 d_3 .... d_{32} \\ \vdots \\ \vdots \\ d_{31} d_{32} \end{pmatrix}$$

We can easily see that $\phi(c)$ is a **[63 x 1]** dimensional vector. Therefore the dimension of the model is **[63 x 1]**

Question 3

A COCO-PUF uses 2 arbiter PUFs, say PUF0 and PUF1 – each PUF has its own set of multiplexers with possibly different delays. In this system lower signal from PUF0 compete with the lower signal from PUF1 using an arbiter called Arbiter0 to generate a response called Response0. If the signal from PUF0 reaches first, Response0 is 0 else if the signal from PUF1 reaches first, Response0 is 1. Similarly, the upper signal from PUF0 compete with the upper signal from PUF1 using a second arbiter called Arbiter1 to generate a response called Response1. If the signal from PUF0 reaches first, Response1 is 0 else if the signal from PUF1 reaches first, Response1 is 1.
Using the derivations from previous solution we have following equations:

$$t_{32}^{u_1} = \frac{1}{2}\sum_{i=1}^{32}[(1-c_i^1)(p_i^1+q_i^1)+c_i^1(r_i^1+s_i^1)+\prod_{j=i+1}^{32}(1-2c_j^1)((1-c_i^1)(p_i^1-q_i^1)-c_i^1(r_i^1-s_i^1))] \tag{1}$$

$$t_{32}^{u_2} = \frac{1}{2}\sum_{i=1}^{32}[(1-c_i^2)(p_i^2+q_i^2)+c_i^2(r_i^2+s_i^2)+\prod_{j=i+1}^{32}(1-2c_j^2)((1-c_i^2)(p_i^2-q_i^2)-c_i^2(r_i^2-s_i^2))] \tag{2}$$

Where:

- $t_{32}^{u_1}$ is the time taken by upper signal of PUF0 to reach.
- $t_{32}^{u_2}$ is the time taken by upper signal of PUF1 to reach.

Similarly we have equation for lower signal as follows:

$$t_{32}^{l_1} = \frac{1}{2}\sum_{i=1}^{32}[(1-c_i^1)(p_i^1+q_i^1)+c_i(r_i^1+s_i^1)-\prod_{j=i+1}^{32}(1-2c_j)((1-c_i)(p_i^1-q_i^1)-c_i(r_i^1-s_i^1))] \tag{3}$$

$$t_{32}^{l_2} = \frac{1}{2}\sum_{i=1}^{32}[(1-c_i)(p_i^2+q_i^2)+c_i(r_i^2+s_i^2)-\prod_{j=i+1}^{32}(1-2c_j)((1-c_i)(p_i^2-q_i^2)-c_i(r_i^2-s_i^2))] \tag{4}$$

Calculating Response 1 *i.e.* $t_{32}^{u_2}$ - $t_{32}^{u_1}$ using the equations derieved in Question 1 :

$$t_{32}^{u_2} - t_{32}^{u_1} = \frac{1}{4}\sum_{i=1}^{32}[C_i^2 - C_i^1 + d_i(A_i^2 - A_i^1) + \prod_{j=i+1}^{32}(d_j(D_i^2 - D_i^1 + d_i(B_i^2 - B_i^1)))]$$

Where:

- c_i = (1 - d_i)/2
- $p_i^k + q_i^k - r_i^k - s_i^k = A_i^k$
- $p_i^k - q_i^k + r_i^k - s_i^k = B_i^k$
- $2p_i^k + 2q_i^k - A_i^k = p_i^k + q_i^k + r_i^k + s_i^k = C_i^k$

- $2p_i^k - 2q_i^k - B_i^k = p_i^k - q_i^k - r_i^k + s_i^k = D_i^k$

for k = *1,2*

Let:

- $A_i^2 - A_i^1 = \alpha_i$
- $B_i^2 - B_i^1 = \beta_i$
- $C_i^2 - C_i^1 = \gamma_i$
- $D_i^2 - D_i^1 = \delta_i$

We have:

$$t_{32}^{u_2} - t_{32}^{u_1} = \frac{1}{4}\sum_{i=1}^{32}[\gamma_i + d_i(\alpha_i) + \prod_{j=i+1}^{32}(d_j(\delta_i + d_i\beta_i))]$$

Now to convert this equation in the form $t_{32}^{u_2} - t_{32}^{u_1} = \tilde{W}^\top\tilde{\phi}(c) + \tilde{b}$ we take

$$\tilde{b} = \sum_{i=1}^{32}\frac{\gamma_i}{4}$$

where ,

$$\tilde{\phi}(c) = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ \vdots \\ d_{32} \\ d_1d_2d_3....d_{32} \\ d_2d_3....d_{32} \\ \vdots \\ \vdots \\ d_{31}d_{32} \end{pmatrix}$$

$$\tilde{W} = \frac{1}{4}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_{32} + \beta_{32} + \delta_{31} \\ \beta_1 \\ \beta_2 + \delta_1 \\ \vdots \\ \vdots \\ \beta_{31} + \delta_{30} \end{pmatrix}$$

We can predict Response1 by following formula :

$$\frac{1+\text{sign}(\tilde{W}^\top \tilde{\phi}(c)+\tilde{b})}{2} = r_1(c)$$

We can predict Response0 similarly,

$$t_{32}^{l_2} - t_{32}^{l_1} = \frac{1}{4}\sum_{i=1}^{32}[(1-c_i)(p_i^2+q_i^2-p_i^1-q_i^1)+c_i(r_i^2+s_i^2-r_i^1-s_i^1)+$$

$$\prod_{j=i+1}^{32}((1-2c_j)((1-c_i)(p_i^2-q_i^2-p_i^1+q_i^1)-c_i(r_i^2-s_i^2-r_i^1+s_i^1))]$$

Substituting following :
Where:

- c_i = (1 - d_i)/2
- $(p_i^2-p_i^1)+(q_i^2-q_i^1)-(r_i^2-r_i^1)-(s_i^2-s_i^1)=\alpha_i$
- $(p_i^2-p_i^1)-(q_i^2-q_i^1)+(r_i^2-r_i^1)-(s_i^2-s_i^1)=\beta_i$
- $(p_i^2-p_i^1)+(q_i^2-q_i^1)+(r_i^2-r_i^1)+(s_i^2-s_i^1)=\gamma_i$
- $(p_i^2-p_i^1)-(q_i^2-q_i^1)-(r_i^2-r_i^1)+(s_i^2-s_i^1)=\delta_i$

We have:

$$t_{32}^{l_2} - t_{32}^{l_1} = \frac{1}{4}\sum_{i=1}^{32}[\gamma_i + d_i(\alpha_i) + \prod_{j=i+1}^{32}(d_j(\delta_i+d_i\beta_i))]$$

Now to convert this equation in the form $t_{32}^{l_2} - t_{32}^{l_1} = \tilde{W}^\top\tilde{\phi}(c)+\tilde{b}$ we take

$$\tilde{b} = \sum_{i=1}^{32}\frac{\gamma_i}{4}$$

where ,

$$\tilde{\phi}(c) = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ \vdots \\ d_{32} \\ d_1d_2d_3....d_{32} \\ d_2d_3....d_{32} \\ \vdots \\ \vdots \\ d_{31}d_{32} \end{pmatrix}$$

$$\tilde{W} = \frac{1}{4} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_{32} + \beta_{32} + \delta_{31} \\ \beta_1 \\ \beta_2 + \delta_1 \\ \vdots \\ \vdots \\ \beta_{31} + \delta_{30} \end{pmatrix}$$

Response0 is given by following formula :

$$\frac{1 + \mathrm{sign}(\tilde{W}^\top \tilde{\phi}(c) + \tilde{b})}{2} = r_0(c)$$

Question 4

Since both models are similar in structure, both the models will have same **Dimensionality** .

$$\tilde{W} = \frac{1}{4} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_{32} + \beta_{32} + \delta_{31} \\ \beta_1 \\ \beta_2 + \delta_1 \\ \vdots \\ \vdots \\ \beta_{31} + \delta_{30} \end{pmatrix}$$

We can easily see that $\tilde{W}$ is a **[63 x 1]** dimensional vector. Therefore the dimension of both models for predicting Response0 and Response1 is **[63 x 1]**