Data Innovators - Report for Assignment 1 - CS771

1. Kshitij Bhardwaj - 230580

2. Harsh Gupta - 230445

3. Priyanka Arora - 230799

4. Parnika Mittal - 230736

5. Harshit Agarwal - 230458

1

There are two possibilities for the time upper signal of i^{th} Multiplexer takes:

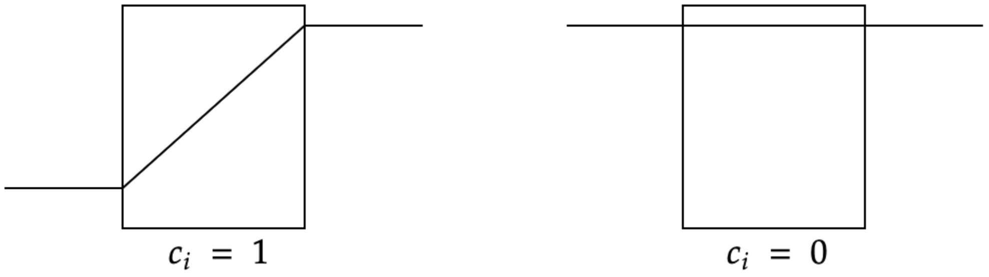
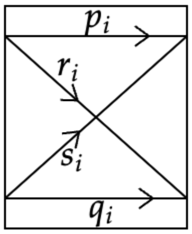


Figure 1: Defines the possible values of c for i'th Multiplexer and corresponding Multiplexer Configuration

For a Multiplexer, time delays $p_i,\ q_i, r_i,\ s_i$ are defined as:



Preprint. Under review.

$t_i^u = [(1-c_i)p_i + c_i r_i] + t_{i-1}^u$ (if the signal started upper at (*i-1*)th Multiplexer)

$t_i^u = [(1-c_i)q_i + c_i s_i] + t_{i-1}^l$ (if the signal started lower at (*i-1*)th Multiplexer)

where t_i^u refers to the signal that comes out as upper signal at last Multiplexer

Since we need the time of the signal that reaches as the upper signal we can think of it like finding out the time of the signal that starts out as upper but with the reverse challenge input given to us. So if the number of interchanges of signal from the last to the i^{th} Multiplexer is even then we need the time of the signal that enters the ith Multiplexer as the upper signal otherwise it cannot reach as upper signal and if it's odd then the lower signal at ith Multiplexer turns out to be the final upper signal

In order to know whether the final upper signal is UPPER or LOWER at the i^{th} Multiplexer, we can use the expression:

$$\textstyle\prod_{i=i}^{31}(1-2c_i)$$

Hence the time that the final UPPER signal takes at i^{th} Multiplexer would be:

$$\begin{aligned} t_i^u = {} & [(1-c_i)p_i + c_i r_i][\frac{1+\prod_{i=i}^{31}(1-2c_i)}{2}] \\ & + [(1-c_i)q_i + c_i s_i][\frac{1-\prod_{i=i}^{31}(1-2c_i)}{2}] \end{aligned} \tag{1}$$

which can be written as:

$$\begin{aligned} t_i^u = {} & \frac{(1-2c_i)}{2}\frac{(p_i+q_i-r_i-s_i)}{2} + \frac{(p_i+q_i+r_i+s_i)}{4} \\ & + [\frac{\prod_{i=i+1}^{31}(1-2c_i)}{2}][\frac{(p_i-q_i-r_i+s_i)}{2}] \\ & + [\prod_{i=i}^{31}(1-2c_i)][\frac{(p_i-q_i+r_i+-s_i)}{4}] \end{aligned} \tag{2}$$

Using the Following Substitutions:

$$\begin{aligned} \alpha_i &= \tfrac{p_i-q_i+r_i-s_i}{4} \\ \beta_i &= \tfrac{p_i-q_i-r_i+s_i}{4} \\ \gamma_i &= \tfrac{p_i+q_i-r_i-s_i}{4} \\ b_i &= \tfrac{p_i+q_i+r_i+s_i}{4} \\ d_i &= (1-2c_i) \end{aligned}$$

(i=0,1,2,...31)

$$w_i = \alpha_i + \beta_{i-1} \text{ (i=1,2,...31)}$$

$$w_0 = \alpha_0 \text{ (i=0)}$$

$$x_i = d_{31}.d_{30}...d_{i+1}.d_i$$

Total Time (summation of time taken at each Multiplexer) would be:

$$T_{31}^u = \textstyle\sum_{i=0}^{31}(d_i\gamma_i + b_i + w_i x_i) + \frac{p_{31}-q_{31}-r_{31}-s_{31}}{4}$$

$$T_{31}^u = \sum_{i=0}^{31}(d_i\gamma_i + b_i + w_i x_i) + \beta_{31} \tag{3}$$

This can be written as $W^T\phi(c) + b$:

$$w_i = \alpha_i + \beta_{i-1} \text{ (i=1,2,...30)}$$

$$w_0 = \alpha_0$$

$$w_{31} = \alpha_{31} + \beta_{31} + \gamma_{31}$$

$$w_i = \gamma_{i-32} \text{ (for i=32, 33,... 62)}$$

$$\phi_i = x_i \text{ (for i=0, 1,... 31)}$$

$$\phi_i = d_{i-32} \text{ (for i=32, 33,... 62)}$$

$$b = \textstyle\sum_{i=0}^{31} b_i + \frac{p_{31}-q_{31}-r_{31}+s_{31}}{4}$$

$$\Rightarrow W^T\phi(c) + b$$

2

Dimensionality = 63
As 63 Linearly Independent terms are included in Linear Model **W**

3

$$\begin{aligned} T_i &= t_i^u + t_i^l \\ &= \sum_{i=0}^{i}[(p+q)(1-c_i) + (r+s)(c_i)] \\ &= \sum_{i=0}^{i}[(p+q-r-s)(\frac{1-2c_i}{2}) + \frac{p+q+r+s}{2}] \end{aligned} \tag{4}$$

$$t_i^u = \sum_{i=0}^{i}[(1-2c_i)(\frac{p_i+q_i-r_i-s_i}{4}) + \frac{p_i+q_i+r_i+s_i}{4} + \prod_{i=i}^{31}(1-2c_i)(\frac{p_i-q_i+r_i-s_i}{4}) + \prod_{i=i+1}^{31}(1-2c_i)(\frac{p_i-q_i-r_i+s_i}{4})] \quad (5)$$

$$t_i^l = T_i - t_i^u = \sum_{i=0}^{i}[(1-2c_i)(\frac{p_i+q_i-r_i-s_i}{4}) + \frac{p_i+q_i+r_i+s_i}{4} - \prod_{i=i}^{31}(1-2c_i)(\frac{p_i-q_i+r_i-s_i}{4}) - \prod_{i=i+1}^{31}(1-2c_i)(\frac{p_i-q_i-r_i+s_i}{4})] \quad (6)$$

For PUF0, delays remain the same, p_i, q_i, r_i, s_i
For PUF1, corresponding delays are denoted as $p_i^{'}, q_i^{'}, r_i^{'}, s_i^{'}$
(for the $i^{'}th$ Multiplexer)
Hence for Response0, if sign of $t_{31}^{l'} - t_{31}^{l}$ is positive, Response0 will be 1

Therefore, it can be written as:

$$\frac{1+sign(t_{31}^{l'}-t_{31}^{l})}{2}$$

Here

$$t_{31}^{l'} - t_{31}^{l} = \sum_{i=0}^{31}[d_i(\gamma_i^{'}-\gamma_i) + b_i^{'} - b_i - (w_i^{'}x_i - w_i x_i)] - \beta_{31}^{'} + \beta_{31} \quad (7)$$

This can be written as $W^T\phi(c) + b$:
(ϕ has the same meaning as before)

$$w_i = \alpha_i + \beta_{i-1} - \alpha_i^{'} - \beta_{i-1}^{'} \text{ (i=1,2,...30)}$$

$$w_0 = \alpha_0 - \alpha_0^{'}$$

$$w_{31} = \alpha_{31} + \beta_{31} + \gamma_{31} - \alpha_{31}^{'} - \beta_{31}^{'} - \gamma_{31}^{'}$$

$$w_i = \gamma_{i-32} - \gamma_{i-32}^{'} \text{ (for i=32, 33,... 62)}$$

$$\phi_i = x_i \text{ (for i=0, 1,... 31)}$$

$$\phi_i = d_{i-32} \text{ (for i=32, 33,... 62)}$$

$$b = \sum_{i=0}^{31}(b_i - b_i^{'}) + \beta_{31} - \beta_{31}^{'}$$

$$\Rightarrow W^T\phi(c) + b$$

(All Other Notations are same as in Q1)

And For Response 1: sign of $t_{31}^{u} - t_{31}^{u'}$ decides the response
Here

$$t_{31}^{u} - t_{31}^{u'} = \sum_{i=0}^{31}[d_i(\gamma_i - \gamma_i^{'}) + b_i - b_i^{'} + (w_i x_i - w_i^{'} x_i)] + \beta_{31} - \beta_{31}^{'} \quad (8)$$

This can be written as:

$$\Rightarrow W^T\phi(c) + b$$

(All Notations are same as above)

4

Dimensionality for Response 0 = **63**
Dimensionality for Response 1 = **63**

6

Here we will discuss the model performance of LinearSVC and LogisticRegression considering the metrics:
(1) my_fit Time : Time taken by the my_fit() function in seconds
(2) 1 - Accuracy (Response 0) : Accuracy Losses for the Response 0 Arbiter PUF
(3) 1 - Accuracy (Response 1) : Accuracy Losses for the Response 1 Arbiter PUF

For all the above mentioned metrics, the lower the output values, the better the model performance

(a) changing the loss hyperparameter in LinearSVC (hinge vs squared hinge)

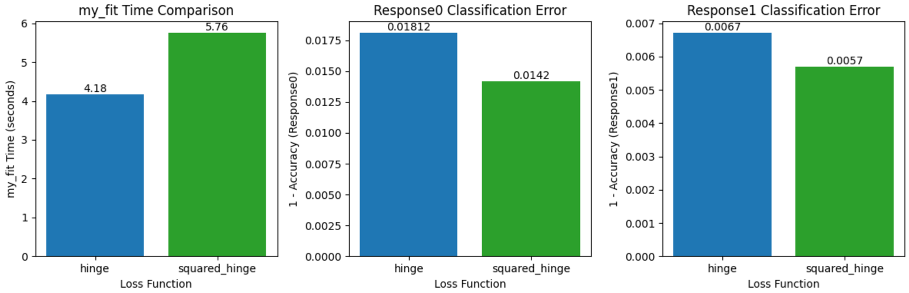


Figure 2:

(b) setting C in LinearSVC and LogisticRegression to high/low/medium values

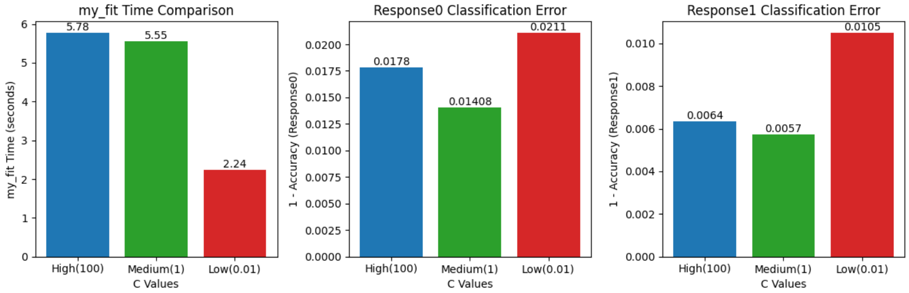


Figure 3: LinearSVC model statistics with varying hyperparameter C (inverse regularization)

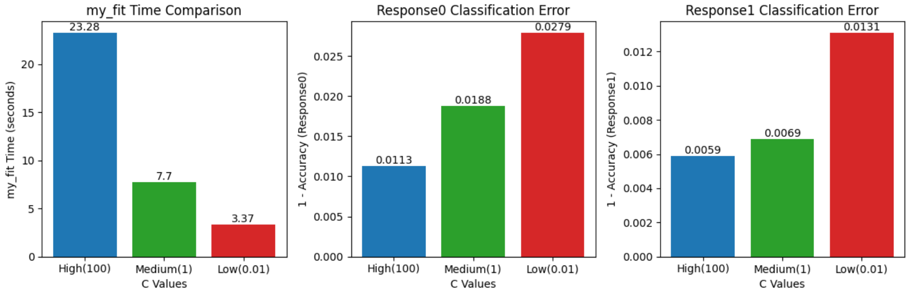


Figure 4: Logistic Regression model statistics with varying hyperparameter C (inverse regularization)

(c) changing tol in LinearSVC and LogisticRegression to high/low/medium values

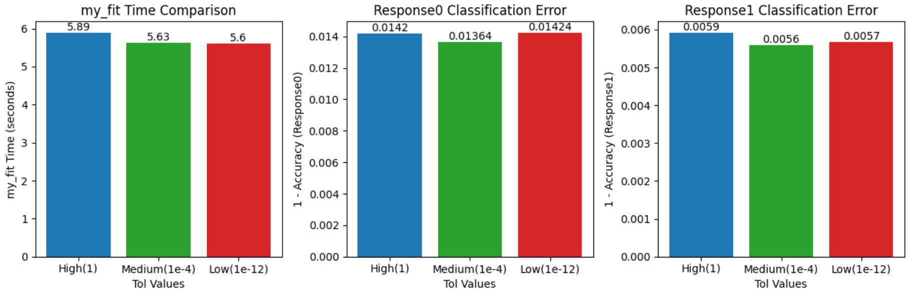


Figure 5: LinearSVC model statistics with varying Tolerance

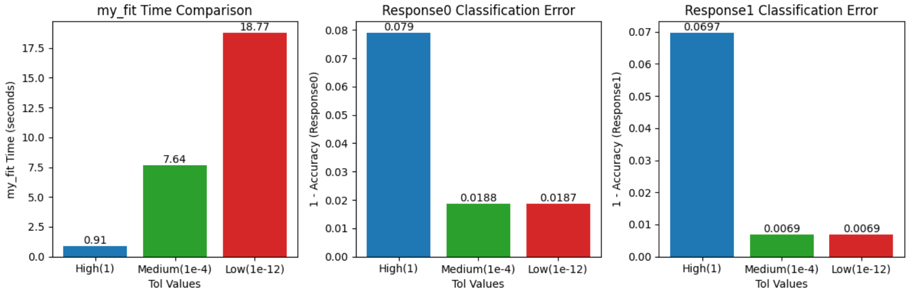


Figure 6: Logistic Regression model statistics with varying Tolerance

(d) changing the penalty (regularization) hyperparameter in LinearSVC and LogisticRegression (l2 vs l1)

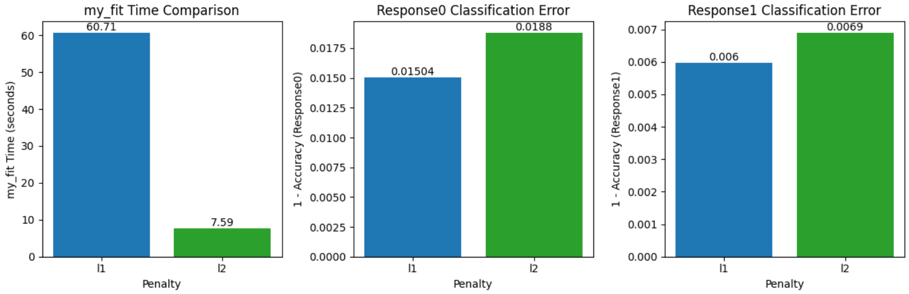


Figure 7: LinearSVC model statistics with varying norms used in penalization

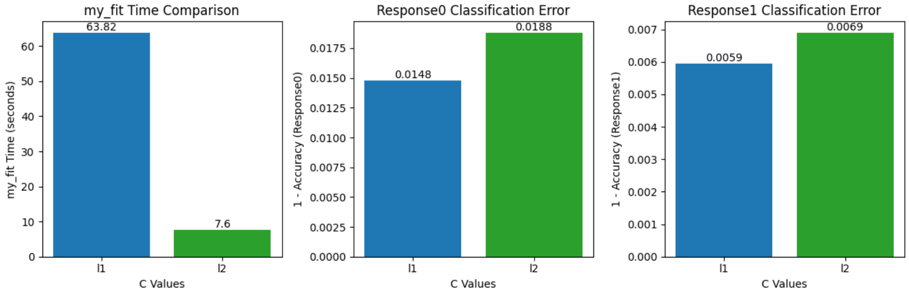


Figure 8: LinearSVC model statistics with varying norms used in penalization

7 References

1. Khatri-Rao Product - Wikipedia
2. matplotlib Documentation
3. scikit-learn Documentation
4. Modelling Delay-based Physically Unclonable Functions through Particle Swarm Optimization - *Nimish Mishra, Indian Institute of Technology Kharagpur, Kuheli Pratihar, Indian Institute of Technology Kharagpur, Anirban Chakraborty, Indian Institute of Technology Kharagpur, Debdeep Mukhopadhyay, Indian Institute of Technology Kharagpur*