CS771 Assignment 1

Supervised Learners

In this assignment, we were to show that Cross Connection Arbiter PUF (COCO PUF) are also vulnerable by showing that there exist a single linear model. Here we constructed two linear models, one giving the difference of time taken by the upper and lower signal and other one giving the sum of time taken by the upper and the lower signal. Adding these two would give twice the time taken by upper signal and subtracting them carefully would give twice the time taken by lower signal. Now using these times, we can get response 0 and response 1

Task 1

We are given a simple arbiter PUF. As learned in class, the time lag between the upper and the lower signal i.e. $\Delta_{31} = t^u_{31} - t^l_{31}$ can be predicted by a linear model $\mathbf{w}^\intercal\mathbf{x} + b = \Delta_{31}$ where $b \in \mathbb{R}$, x is a map $x\colon \{0,1\}^{32} \to \mathbb{R}^{32}$ mapping 32-bit 0/1-valued challenge vectors to 32-dimensional feature vectors and $\mathbf{w}$ is 32-dimensional linear model $\mathbf{w} \in \mathbb{R}^{32}$.

Similarly we can calculate $\delta_{31} = t^u_{31} + t^l_{31}$

$$t^u_1 = (1 - c_1)(t^u_0 + p_1) + c_1(t^l_0 + s_1)$$
$$t^l_1 = (1 - c_1)(t^l_0 + q_1) + c_1(t^u_0 + r_1)$$

$$\begin{aligned}\delta_1 &= (1 - c_1)(t^u_0 + p_1 + t^l_0 + q_1) + c_1(t^l_0 + s_i + t^u_0 + r_1)\\ &= (1 - c_1)(\delta_0 + p_1 + q_1) + c_1(\delta_0 + s_1 + r_1)\end{aligned}$$

$$\therefore \delta_1 = \delta_0 + c_1(s_1 + r_1 - p_1 - q_1) + (p_1 + q_1)$$

To make notation simpler, let $\gamma_1 = s_1 + r_1 - p_1 - q_1$ and $\epsilon_1 = p_1 + q_1$

$$\delta_1 = \delta_0 + c_1.\gamma_1 + \epsilon_1$$

We can see that a similar relation holds for any stage

$$\delta_i = \delta_{i-1} + c_i.\gamma_i + \epsilon_i \tag{1}$$

where $\gamma_i = s_i + r_i - p_i - q_i$ and we can assume $t^u_{-1}, t^l_{-1} = 0$.

We can keep on going recursively

$$\begin{aligned}\delta_0 &= c_0.\gamma_0 + \epsilon_0, && \text{as } \delta_{-1} = 0\\ \delta_1 &= \delta_0 + c_1.\gamma_1 + \epsilon_1\\ \delta_1 &= c_0.\gamma_0 + c_1.\gamma_1 + \epsilon_0 + \epsilon_1\\ \delta_2 &= \delta_1 + c_2.\gamma_2 + \epsilon_2\\ \delta_2 &= c_0.\gamma_0 + c_1.\gamma_1 + c_2.\gamma_2 + \epsilon_0 + \epsilon_1 + \epsilon_2\end{aligned}$$

We can begin to see a pattern here. Hence, we have

$$\delta_i = c_0.\gamma_0 + c_1.\gamma_1 +, \ldots, +c_{31}.\gamma_{31} + \epsilon_0 + \epsilon_1 +, \ldots, +\epsilon_{31} = \gamma^\intercal\theta + \epsilon \tag{2}$$

where $\gamma = \begin{bmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_{31} \end{bmatrix}$ is the weight vector, $\theta = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{31} \end{bmatrix}$ and $\epsilon = \sum_{i=0}^{31} \epsilon_i \in \mathbb{R}$.

Now, we have a linear model that can predict $t^u_{31} + t^l_{31}$. Using this we can devise a new linear model that gives us the t^u_{31}

$$
\begin{aligned}
t^u_{31} &= \frac{\Delta_{31} + \delta_{31}}{2} = \frac{t^u_{31} - t^l_{31} + t^u_{31} + t^l_{31}}{2} \\
t^u_{31} &= \frac{\mathbf{w}^\mathsf{T}\mathbf{x} + b + \gamma^\mathsf{T}\theta + \epsilon}{2}
\end{aligned}
$$

Defining $\widetilde{\mathbf{w}} = \frac{\mathbf{w}}{2}$, $\widetilde{b} = \frac{b}{2}$, $\widetilde{\epsilon} = \frac{\epsilon}{2}$, $\widetilde{\gamma} = \frac{\gamma}{2}$ for simplicity

$$t^u_{31} = \widetilde{\mathbf{w}}^\mathsf{T}\mathbf{x} + \widetilde{b} + \widetilde{\gamma}^\mathsf{T}\theta + \widetilde{\epsilon}$$

Defining $\mathbf{W}$, ϕ and $\mathbf{b}$ for the final model

$$
\begin{aligned}
\mathbf{W} &= \begin{bmatrix} \widetilde{\mathbf{w}} \\ \widetilde{\gamma} \end{bmatrix} \in \mathbb{R}^{64} \\
\phi &= \begin{bmatrix} \widetilde{\mathbf{x}} \\ \widetilde{\theta} \end{bmatrix} \in \mathbb{R}^{64} \\
\mathbf{b} &= \widetilde{b} + \widetilde{\epsilon}
\end{aligned}
$$

where

$$
\phi = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{31} \\ c_0 \\ c_1 \\ \vdots \\ c_{31} \end{bmatrix} \in \mathbb{R}^{64}
$$

$$
\mathbf{W} = \frac{1}{2} \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{31} \\ \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{31} \end{bmatrix} \in \mathbb{R}^{64}
$$

Giving us $\mathbf{W}^\mathsf{T}\phi(\mathbf{c}) + \mathbf{b} = t^u(\mathbf{c})$

Task 2

The dimensionality of the linear model needed to predict the arrival time of the upper signal is $2(32) = 64$ as bias term is not included in the feature vector.

Task 3

Using the model $t^u(\mathbf{c})$ derived in part 1, we can get the difference between the upper signals of PUF1 and PUF0, thus we can calculate $t_1^u - t_0^u$ and get Response1 by $\frac{1+sign(t_1^u - t_0^u)}{2}$
Similarly, we can find $t_1^l - t_0^l$ to calculate Response0 using the same model $t_{31}^u = \frac{\delta_{31}-\Delta_{31}}{2} = \frac{t_{31}^u + t_{31}^l - t_{31}^u + t_{31}^l}{2}$.

Task 4

The dimensionality of the linear models needed to predict Response0 and Response1 is also $2(32) = 64$, as they are derived from predicting the arrival times and then combining these to get the Responses.

Task 6

Analysis for LinearSVC with different C values:

C value	Model train time(s)	Accuracy0	Accuracy1
Low	3.330	0.924	0.991
Medium	3.543	0.925	0.996
High	3.442	0.924	0.998

Analysis for LogisticRegression with different C values:

C value	Model train time(s)	Accuracy0	Accuracy1
Low	3.108	0.925	0.987
Medium	3.206	0.925	0.996
High	3.175	0.925	0.998

Performance of LinearSVC with different loss functions:

Loss Function	Model train time(s)	Accuracy0	Accuracy1
Hinge	3.628	0.925	0.995
Squared Hinge	3.206	0.925	0.996

Effect of tolerance for LinearSVC:

Tolerance	Model train time(s)	Accuracy0	Accuracy1
Low	3.506	0.924	0.996
Medium	3.543	0.925	0.996
High	3.278	0.924	0.991

Effect of tolerance for LogisticRegression:

Tolerance	Model train time(s)	Accuracy0	Accuracy1
Low	5.73	0.925	0.995
Medium	3.206	0.925	0.996
High	3.127	0.924	0.821

TEAM MEMBERS:

Prithvi Mehta	**220819**	**prithvim22@iitk.ac.in**
Aditi Singh	**220062**	**aditisi22@iitk.ac.in**
Abhishek Srivastava	**220051**	**srivabhi22@iitk.ac.in**
Aayush Gautam	**220020**	**aayushg22@iitk.ac.in**
Guguloth Pavani Priya	**220415**	**gppriya22@iitk.ac.in**