CS771 Project Report

Group Number: 84 (MLVisionaries)

Team Member 1:	Nitish Kumar (231110033)
Team Member 2:	Riyansha Singh (232110601)
Team Member 3:	Aman Khadoliya (231040009)

Question1.

We need to find mapping function $\phi(c) : \{0,1\}^{32} \rightarrow \mathbb{R}^D$ where D is the feature space dimension and R is the reliability parameter. All challenge-response pairs $(C, R) = (c, r)$. We know response is

$$r = \frac{1 + \text{sign}(\mathbf{w}^T \phi(c) + b)}{2},$$

and $r \in \{0, 1\}$.

Let (u, p) and (v, q) be the 2 linear models that can exactly predict the output of 2 arbitrary PUFs sitting inside the CAR-PUFs.

Challenge vectors (c) composed of bits $c_1, c_2, c_3, \ldots, c_{32}$: $c_i \in \{0, 1\}$.

Let us use d_i to create bits that take value $\{+1, -1\}$ instead of $\{0, 1\}$:

$$d_i = 1 - 2c_i.$$

Corresponding delay of PUFs are:

$$\Delta_u = u^T x + p,$$

$$\Delta_v = v^T x + q.$$

Where, x = $d_i d_{i+1} \ldots d_{32}$,
$u, v \in \mathbb{R}^{32}$,
$p, q \in \mathbb{R}$.

We know that PUF response is:

$$r = \begin{cases} 0 & \text{if } |\Delta_u - \Delta_v| \leq \tau, \\ 1 & \text{if } |\Delta_u - \Delta_v| > \tau. \end{cases}$$

$$= \begin{cases} 0 & \text{if } |\Delta_u - \Delta_v| - \tau \leq 0, \\ 1 & \text{if } |\Delta_u - \Delta_v| - \tau > 0. \end{cases} \quad \text{................(1)}$$

Also, we know response is given by:

$$r = \frac{1 + \text{sign}(\mathbf{w}^T \phi(c) + b)}{2},$$

$$r = \begin{cases} 0 & \text{if } \text{sign}(\mathbf{w}^T\phi(c) + b) = -1, \\ 1 & \text{if } \text{sign}(\mathbf{w}^T\phi(c) + b) = +1. \end{cases}$$

$$r = \begin{cases} 0 & \text{if } \mathbf{w}^T\phi(c) + b \leq 0, \\ 1 & \text{if } \mathbf{w}^T\phi(c) + b > 0. \end{cases} \quad \text{.......................(2)}$$

So, we have to equate (1) and (2), we get i.e.

$$|\Delta_u - \Delta_v| - \tau = (\mathbf{w}^T\phi(c) + b).$$

Also, we know:

$$\text{sign}(|\Delta_u - \Delta_v| - \tau) = \text{sign}((\Delta_u - \Delta_v)^2 - \tau^2).$$

We know,

$$\Delta_v = v^T x + q,$$
$$\Delta_u = u^T x + p,$$

$$\text{sign}((u - v)^T x + (p - q)) = \text{sign}(((u - v)^T x)^2 + (p - q)^2).$$

Solving it further:

$$\Rightarrow ((u - v)^T x + (p - q))^2 - \tau^2$$
$$\Rightarrow ((u - v)^T x)^2 + 2(p - q)((u - v)^T x) + (p - q)^2 - \tau^2$$
$$\Rightarrow (u - v)^T x \cdot (u - v)^T x + (u - v)^T x \cdot (p - q) + (p - q)((u - v)^T x) + (p - q)^2 - \tau^2.$$

Let:

$$u - v = z \quad \text{and} \quad p - q = m.$$

Let z be a 2D vector, $z \in \mathbb{R}^2$ so $x \in \mathbb{R}^2$:

$$z = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}, \quad \text{and} \quad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

$$z^T x \cdot z^T x + z^T x \cdot m + m z^T x + m^2 - \tau^2.$$

$$z^T x = z_1 x_1 + z_2 x_2.$$

$$\Rightarrow (z_1 x_1 + z_2 x_2)(z_1 x_1 + z_2 x_2) + (z_1 x_1 + z_2 x_2) m + m(z_1 x_1 + z_2 x_2) + m^2 - \tau^2.$$

$$\Rightarrow (z_1^2 x_1^2 + 2 z_1 z_2 x_1 x_2 + z_2^2 x_2^2) + 2m z_1 x_1 + 2m z_2 x_2 + m^2 - \tau^2.$$

We know:

$$x_i \in \{-1, 1\},$$

$$x_i^2 = 1,$$

$$\Rightarrow z_1^2 + z_2^2 + 2z_1z_2x_1x_2 + 2mz_1x_1 + 2mz_2x_2 + m^2 - \tau^2.$$

$$\Rightarrow 2z_1z_2x_1x_2 + 2mz_1x_1 + 2mz_2x_2 + z_1^2 + z_2^2 + m^2 - \tau^2.$$

$$\begin{bmatrix} z_1z_2 \\ mz_1 \\ mz_2 \end{bmatrix}^T \begin{bmatrix} 2z_1x_1 \\ 2z_1x_2 \end{bmatrix} + m^2 - \tau^2 + x_1^2 + x_2^2.$$

Compare it with the below equation:

$$\mathbf{w}^T \phi(c) + b.$$

We get:

$$\mathbf{w} = \begin{bmatrix} z_1z_2 \\ mz_1 \\ mz_2 \end{bmatrix} = \begin{bmatrix} (u_1 - v_1)(u_2 - v_2) \\ (u_1 - v_1)(p - q) \\ (u_2 - v_2)(p - q) \end{bmatrix},$$

$$\phi(c) = \begin{bmatrix} 2x_1x_2 \\ 2x_1 \\ 2x_2 \end{bmatrix} = \begin{bmatrix} 2(1 - c_1)(1 - c_2)^2 \\ 2(1 - c_1) \\ 2(1 - c_2) \end{bmatrix}.$$

And:

$$b = m^2 - \tau^2 + (u_1 - v_1)^2 + (u_2 - v_2)^2,$$

$$= (p - q)^2 - \tau^2 + (u_1 - v_1)^2 + (u_2 - v_2)^2$$

So we have taken an example of 2D Euclidean space we get terms in $\phi(c) \rightarrow 2x_1x_2, 2x_1, 2x_2$.

Therefore, for 32D Euclidean space, number of terms = $\binom{32}{2} + 32 \rightarrow 528$.

Also, we reduce ${x_i}^2$ terms as we have transformed it to possible values $\{-1, 1\}$ which implies to vanish of ${x_i}^2$ terms as it is equal to 1.

Question3.

Table 1: Effect of Hyperparameters on Test Accuracy

Model	Loss	Penalty	Test Accuracy
LinearSVC	Squared Hinge	L1	98.78%
		L2	99.19%
	Hinge	L1	not supported
		L2	99%
Logistic Regression	Cross Entropy Loss	L1	98.23%
		L2	99.07%
	Binary Logistic loss	L1	98.68%
		L2	99.42%

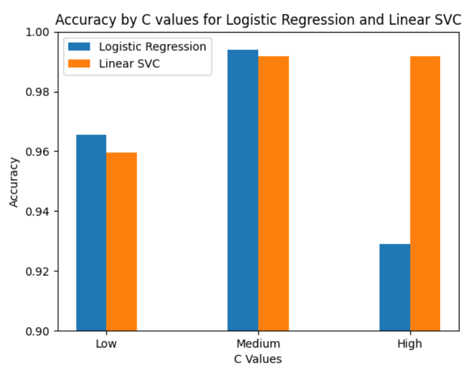

Figure 1: Accuracy plot for different **C** setting

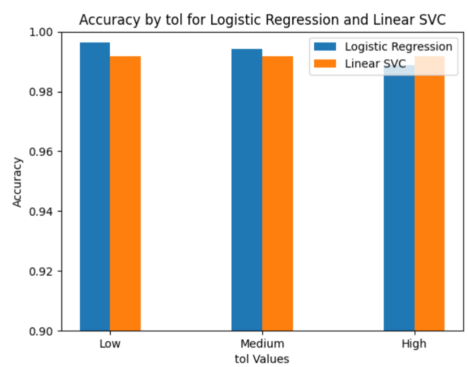

Figure 2: Accuracy plot for different **tol** setting

For the **C** setting:

- High: $C = 100$
- Medium: $C = 1$
- Low: $C = 0.001$

For the **tol** setting:

- High: $tol = 10^{-2}$
- Medium: $tol = 10^{-4}$
- Low: $tol = 10^{-6}$