CS 771 ASSIGNMENT 1

Harsh Methwani (210410)
Deshmukh Harsh Rahul (210317)
Prabhash Mishra (210730)
Divyanshu Singh (210362)
Pradeep Kumar Bagri (210734)
Tushar Dhanwani (211115)

1 Mathematical Derivations

A linear model for an Arbiter PUF looks something like this:

$$\Delta_{\mathrm{r}} = \mathrm{u}^{\mathrm{T}} \cdot \mathrm{x} + \mathrm{p}$$

Here r denotes the reference PUF. Similarly writing a linear model for working PUF:

$$\Delta_{\mathrm{w}} = \mathrm{v}^{\mathrm{T}} \cdot \mathrm{x} + \mathrm{q}$$

Now we know that :

$$\Delta_i = w_0 \cdot x_0 + w_1 \cdot x_1 + \cdots + w_i \cdot x_i + \beta_i = \mathbf{w}^\top \mathbf{x} + b \tag{1}$$

From the slides of Arbiter PUFs:

$$x_i = \prod_{j=1}^{N} (1 - 2 \cdot c_j) \tag{2}$$

The delay introduced by the i^{th} arbiter stage in the Arbiter PUF is given by $x_i = \prod_{j=1}^{N}(1-2\cdot c_j)$ where N is the number of stages. In the problem statement we have $\mathbf{N = 32}$.
Let (u, p) be the linear model for working PUF.
Let (v, q) be the linear model for reference PUF.
Hence,

$$\Delta_{\mathrm{w}} = \mathrm{u_i} \cdot \mathrm{x_i} + \mathrm{p} \tag{3}$$
$$\Delta_{\mathrm{r}} = \mathrm{v_i} \cdot \mathrm{x_i} + \mathrm{q} \tag{4}$$

If $|\Delta_{\mathrm{w}} - \Delta_{\mathrm{r}}| \leq \tau$ then we get an output of 0.
If $|\Delta_{\mathrm{w}} - \Delta_{\mathrm{r}}| > \tau$ then we get an output of 1.
Subtracting eq 3 and eq 4

$$\Delta_{\mathrm{r}} \text{ - } \Delta_{\mathrm{w}} = \sum k_i \cdot x_i \ + \ d \tag{5}$$

On Squaring,

$$(\Delta_{\mathrm{r}} \text{ - } \Delta_{\mathrm{w}})^2 = (k_i \cdot x_i \ + \ d) \cdot (k_j \cdot x_j \ + \ d) \tag{6}$$
$$(\Delta_{\mathrm{r}} \text{ - } \Delta_{\mathrm{w}})^2 = \sum_{i=1}^{32} \sum_{j=1}^{32} k_i \cdot k_j \cdot x_i \cdot x_j \ + \ \sum_{i=1}^{32} 2 \cdot d \cdot k_i \cdot x_i + d^2 \tag{7}$$

Subtracting τ^2 from both sides,

$$(\Delta_{\mathrm{r}} \text{ - } \Delta_{\mathrm{w}})^2 \text{ - } \tau^2 = \sum_{i=1}^{32} \sum_{j=1}^{32} k_i \cdot k_j \cdot x_i \cdot x_j \ + \ \sum_{i=1}^{32} 2 \cdot d \cdot k_i \cdot x_i + d^2 \text{ - } \tau^2 \tag{8}$$

Resolving the double summation,

$$(\Delta_{\mathrm{r}} \text{ - } \Delta_{\mathrm{w}})^2 \text{ - } \tau^2 = \sum_{i \neq j}^{32} \sum^{32} k_i \cdot k_j \cdot x_i \cdot x_j \ + \ \sum_{i=1}^{32} k_i^2 \cdot x_i^2 \ + \ \sum_{i=1}^{32} 2 \cdot d \cdot k_i \cdot x_i + d^2 \text{ - } \tau^2 \tag{9}$$

Now the feature vector has 32 linear terms and $\binom{32}{2}$ non-linear terms. Now total terms = **528**

Also W has $k_i \cdot k_j + k_j \cdot k_i = 2 \cdot (u_i - v_i) \cdot (u_j - v_i)$
Also we can evaluate constant $\mathbf{b}$:

$$\mathbf{b} = \sum_{i=1}^{32} k_i^2 + d^2 - \tau^2 \tag{10}$$

$$= \sum_{i=1}^{32} (u_i - v_i)^2 + (p - q)^2 - \tau^2 \tag{11}$$

Now we know that $\mathbf{W} \cdot \phi(c) + \mathbf{b} \leq 0$ then answer is 0
If $\mathbf{W} \cdot \phi(c) + \mathbf{b} > 0$ then answer is 1
Hence, CAR-PUF is ruled by,

$$\mathbf{r} = (1 + sign(\mathbf{W} \cdot \phi(c) + \mathbf{b}))/2 \tag{12}$$

Table 1: Result Table Penalty parameter is $\mathbf{l}_2$

Mean Fit Time	Param C	Param Loss	Mean Test Score	Std Test Score
9.526624123	1	squared_hinge	0.989824989	0.000302427
8.978476922	65	hinge	0.989524982	0.000582341
8.936356703	20	squared_hinge	0.989499996	0.000162262
9.320908308	100	squared_hinge	0.98945001	0.000565506
9.217669646	5	squared_hinge	0.989424991	0.000428895
8.965493282	60	hinge	0.98932499	0.00041709
8.952638865	69	squared_hinge	0.989324971	0.001056221
9.120128393	10	squared_hinge	0.989299978	0.000637731
9.277629296	10	hinge	0.989249986	0.000778017
9.306614796	75	squared_hinge	0.989174969	0.000879987
8.816924651	65	squared_hinge	0.989149989	0.000337605
8.929155986	69	hinge	0.989099992	0.000314527
9.421221415	100	hinge	0.98902499	0.000308572
9.097555319	40	squared_hinge	0.989024973	0.000921588
9.016708612	80	squared_hinge	0.988974983	0.000486427
9.035661538	41	squared_hinge	0.98892498	0.000674858
8.860201597	75	hinge	0.988924978	0.000619851
9.014125903	80	hinge	0.988849959	0.001169227
9.165065527	20	hinge	0.988824983	0.000486432
9.140021245	50	squared_hinge	0.988749987	0.000501542
8.930944602	70	squared_hinge	0.988749972	0.000864209
9.13189284	39	hinge	0.988724982	0.000528332
8.940873384	70	hinge	0.988724973	0.000761136
8.953718185	72	squared_hinge	0.988724962	0.001225589
9.389370044	5	hinge	0.988699986	0.000434819
9.020362775	30	squared_hinge	0.988599981	0.000561618
9.085398436	50	hinge	0.988549997	0.000127757
8.97807312	60	squared_hinge	0.988524976	0.000864176
9.486543576	39	squared_hinge	0.988500012	0.000467398
8.915025234	72	hinge	0.988499984	0.000521156
9.096030394	40	hinge	0.988349996	0.000358967
9.134045998	90	squared_hinge	0.988274988	0.000369492
8.942934593	90	hinge	0.988199984	0.000443406
9.064492067	30	hinge	0.988199981	0.000549265
11.4199268	0.1	squared_hinge	0.987925006	0.000317989
9.253416618	1	hinge	0.987924966	0.001102626
9.077926238	41	hinge	0.987899996	0.000358972
4.810680866	0.1	hinge	0.982775014	0.00053458
3.396004041	0.01	squared_hinge	0.981474996	0.000162449
2.575579643	0.01	hinge	0.969625002	0.000340797