CS771 Report

Question 1:

Theorem 1. *For any arbiter PUF, there exists a linear model* $(\mathbf{w}, b) \in \mathbb{R}^{32} \times \mathbb{R}$ *such that the delay* Δ *of the PUF on the challenge* $\mathbf{c}$ *is given by*

$$\Delta = \mathbf{w}^T\mathbf{x} + b$$

where $\mathbf{x} \in \mathbb{R}^{32}$ *is the feature vector defined by:*

$$x_i = (1 - 2c_i)(1 - 2c_{i+1})(1 - 2c_{i+2}) \ldots (1 - 2c_{32})$$

for each $i = 1, 2, \ldots, 32$.

We show how to extend this to the 2-arbiter case.

Theorem 2. *For a CAR-PUF, there exists a linear model* $(\mathbf{W}, b) \in \mathbb{R}^{528} \times \mathbb{R}$ *such that the response of the CAR-PUF on challenge* $\mathbf{c}$ *is given by:*

$$y = \frac{1 + \operatorname{sgn}\left(\mathbf{W}^T \phi(c) + b\right)}{2}$$

Where,

$$\phi(\mathbf{c}) = (z_{1,1}, z_{1,2} \ldots z_{1,32}, z_{2,2}, \ldots, z_{2,32}, \ldots, z_{32,32})$$

And

$$z_{i,j} = \prod_{l=i}^{j} (1 - 2c_l)$$

Proof. By Theorem 1, there must exist models $(\mathbf{u}, p), (\mathbf{v}, q)$ which perfectly model the response of the working and reference PUFs exactly.

Thus, we can predict the difference of their delays by a linear model as follows:

$$\Delta_w - \Delta_r = \mathbf{u}^T\mathbf{x} + p - \mathbf{v}^T\mathbf{x} - q = (\mathbf{u} - \mathbf{v})^T x + (p - q) = \mathbf{m}^T x + r$$

where $\mathbf{m} = \mathbf{u} - \mathbf{v}$ and $r = p - q$.

Now, notice that the response of the CAR-PUF is 1 exactly when

$$|\Delta_w - \Delta_r| > \tau \iff (\Delta_w - \Delta_r)^2 - \tau^2 > 0$$

Simplifying this expression:

$$\begin{aligned}
(\Delta_w - \Delta_r)^2 - \tau^2 &= \left(\mathbf{m}^T\mathbf{x} + r\right)^2 - \tau^2 \\
&= \left(\sum_{i=1}^{32} m_i x_i + r\right)^2 - \tau^2 \\
&= \left(\sum_{i=1}^{32} m_i x_i\right)^2 + 2r\left(\sum_{i=1}^{32} m_i x_i\right) + r^2 - \tau^2 \\
&= \sum_{i=1}^{32} m_i^2 x_i^2 + 2\sum_{1 \le i < j \le 32} m_i m_j x_i x_j + 2r\left(\sum_{i=1}^{32} m_i x_i\right) + r^2 - \tau^2
\end{aligned}$$

Since $x_i \in \{-1, 1\}, x_i^2 = 1$.

$$= \sum_{i=1}^{32} m_i^2 + 2\sum_{1 \le i < j \le 32} m_i m_j x_i x_j + 2r\left(\sum_{i=1}^{32} m_i x_i\right) + r^2 - \tau^2$$

Let $z_{i,j} = \prod_{l=i}^{j} (1 - 2c_l)$, for all $j \ge i$. Then, we note the following:

$$x_i = z_{i,32}$$

And,

$$\begin{aligned} x_i x_j &= \prod_{l=i}^{32}(1-2c_l)\prod_{l=j}^{32}(1-2c_l) \\ &= \prod_{l=i}^{j-1}(1-2c_l)\prod_{l=j}^{32}(1-2c_l)^2 \\ &= \prod_{l=i}^{j-1}(1-2c_l) \\ &= z_{i,j-1} \end{aligned}$$

Thus, letting $\alpha_{i,j-1} = 2m_i m_j, \alpha_{i,32} = 2rm_i, \gamma = \sum_{i=1}^{32} m_i^2 + r^2 - \tau^2$, we have:

$$\begin{aligned} (\Delta_w - \Delta_r)^2 - \tau^2 &= \sum_{1\le i<j\le 32} 2m_i m_j x_i x_j + \sum_{i=1}^{32} 2rm_i x_i + \sum_{i=1}^{32} m_i^2 + r^2 - \tau^2 \\ &= \sum_{1\le i<j\le 32} \alpha_{i,j-1} z_{i,j-1} + \sum_{1\le i\le 32} \alpha_{i,32} z_{i,32} + \gamma \\ &= \sum_{1\le i\le j\le 31} \alpha_{i,j} z_{i,j} + \sum_{1\le i\le 32} \alpha_{i,32} z_{i,32} + \gamma \\ &= \sum_{1\le i,j\le 32} \alpha_{i,j} z_{i,j} + \gamma \end{aligned}$$

Which is a linear model in $\phi(\mathbf{c})$. There are $\binom{32}{2} + 32 = 528$ $z_{i,j}$'s. For the linear model $(\mathbf{W}, b)$ defined by $\alpha_{i,j}$'s and γ, the response for a challenge is precisely $\frac{1+\text{sgn}\left(\mathbf{W}^T\phi(\mathbf{c})+b\right)}{2}$. $\square$

Question 3:

a

LinearSVC		
loss hyperparameter	Accuracy	Time (sec)
hinge	0.98864	15.700767
squared hinge	0.99116	17.999646

b

i

Changing C		
LinearSVC		
C Value	Accuracy	Time (sec)
0.1	0.98990	20.783399
1.0	0.99172	17.527513
10.0	0.98974	17.341398
100.0	0.98996	17.572503

ii

LogisticRegression		
C Value	Accuracy	Time (sec)
0.1	0.98710	2.004277
1.0	0.99070	2.509324
10.0	0.99220	2.880717
100.0	0.99310	4.015238

d

i

Changing Penalty/Regularization		
LinearSVC		
Penalty	Accuracy	Time (sec)
l1	0.99124	163.014093
l2	0.99190	17.716546

ii	LogisticRegression		
	Penalty	Accuracy	Time (sec)
	l1	0.99180	246.677855
	l2	0.99070	3.020177