Assignment 1

Graded

Group

PRASAD VIJAY JAWARE
PRADUMNA AWASTHI
KARTIKEYA SHUKLA
...and 3 more
View or edit group

Total Points

48 / 50 pts

Question 1

Derivation

10 / 10 pts

✓ **+ 10 pts** A valid derivation showing that a linear model suffices to solve the problem.

− 2 pts Minor mistakes

+ 0 pts Completely wrong or else unanswered

Question 2

Code

34 / 35 pts

+ 0 pts No rubric -- see comments for mark breakup

+ 34 pts GROUP NO: 27

Grading scheme for code:
Dimensionality dd: dd < 550 (5 marks), 550 <= dd < 1000 (4 marks), dd >= 1000 (3 marks)
Train time tt (in sec): tt < 5 (10 marks), 5 <= tt < 10 (9 marks), 10 <= tt < 20 (8 marks), 20 <= tt < 50 (7 marks), tt >= 50 (6 marks)
Map time mt (in sec): mt < 0.1 (10 marks), 0.1 <= mt < 0.2 (9 marks), 0.2 <= mt < 0.5 (8 marks), 0.5 <= mt < 1 (7 marks), mt >= 1 (6 marks)
Error rate ee: ee < 0.1 (10 marks), 0.1 <= ee < 0.2 (8 marks), ee > 0.2 (6 marks)

dd = 528.0 : 5 marks
tt = 2.162 sec : 10 marks
mt = 0.145 sec : 9 marks
ee = 0.006 : 10 marks
TOTAL: 34 marks

Question 3

Report

4 / 5 pts

✓ **+ 5 pts** Description of the hyperparameters in the chosen method and how the hyperparameters were tuned.

− 2 pts Insufficient or missing details of hyperparameters e.g. missing grid values if grid search was used.

+ 0 pts Completely wrong or else unanswered.

− 1 pt -1 for not specifying method for hyperparameter tuning

No questions assigned to the following page.

CS771A Introduction to Machine Learning
Assignment 1

Group Member(s)

Ayush Pandey
200248
apandey20@iitk.ac.in

Navneet Singh
200626
navneets20@iitk.ac.in

Prasad Jaware
208070705
prasadvj20@iitk.ac.in

Md Sameer Idris
200578
sameer20@iitk.ac.in

Kartikeya Shukla
220506
kartikeyas22@iitk.ac.in

Pradumna Awasthi
200693
pradumna20@iitk.ac.in

Question 1:

By giving a detailed mathematical derivation (as given in the lecture slides), show how a CAR-PUF can be broken by a single linear model. Give derivations for a map ϕ : $\{0,1\}^{32} \rightarrow \mathbb{R}^D$ mapping 32-bit 0/1-valued challenge vectors to D-dimensional feature vectors (for some D > 0) so that for any CAR-PUF, there exists a D-dimensional linear model $W \in \mathbb{R}^D$ and a bias term $b \in \mathbb{R}$ such that for all CRPs (**c**,r) with $c \in \{0,1\}^{32}, r \in \{0,1\}$, we have

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

Solution 1:

First we will find a linear model to break a single PUF.
An Attacker can see responses on a few challenges and use ML to predict responses on other challenges. It does not if using 32 bit or 64 bit challenges.

t_i^u : time at which the upper signal leaves the i^{th} - MUX.
t_i^l : time at which the lower signal leaves the i^{th} - MUX.

t_1^u and t_1^l depend on $t_0^u, t_0^l, p_1, q_1, r_1, s_1$ and c_1.
c_1 dictates which previous delay t_0^u and t_0^l will get carried forward and p_1, q_1, r_1, s_1 gives us delay introduce in the i^{th} - MUX itself.

$$t_1^u = (1 - c_1).(t_0^u + p_1) + c_1.(t_0^l + s_1)$$
$$t_1^l = (1 - c_1).(t_0^l + q_1) + c_1.(t_0^u + r_1)$$

let us use shorthand $\Delta = t_i^u - t_i^l$ denotes lag.
All that matter is, for a single PUF whether Δ_{31} is less then 0 or not.

$$\begin{aligned}\Delta_1 &= (1 - c_1).(t_0^u + p_1 - t_0^l - q_1) + c_1.(t_0^l + s_1 - t_0^u - r_1)\\ &= (1 - 2c_1).\Delta_0 + (q_1 - p_1 + s_1 - r_1).c_1 + (p_1 - q_1)\end{aligned}$$

No questions assigned to the following page.

$$\Delta_1 = \Delta_0.d_1 + \alpha_1.d_1 + \beta_1$$

$$where, \alpha_1 = \frac{(p_1 - q_1 + r_1 - s_1)}{2} \quad \& \quad \beta_1 = \frac{(p_1 - q_1 + r_1 - s_1)}{2}$$

$$d_i = (1 - 2c_i) \Rightarrow d_i = \{-1, 1\}$$

$$\Delta_i = d_i.\Delta_{i-1} + \alpha_i.d_i + \beta_i \qquad ...[\Delta_{-1} = 0]$$

$$\Delta_0 = \alpha_0.d_0 + \beta_0$$

$$\Delta_1 = \alpha_0.d_2.d_1.d_0 + (\alpha_1 + \beta_0).d_2.d1 + (\alpha_2 + \beta_1).d_2 + \beta_2$$

A pattern begins can be seen in these equations:

$$\begin{aligned} \Delta_{31} &= w_0.x_0 + w_1.x_1 + ... + w_{31}.x_{31} + \beta_{31} \\ &= w^T X + b \end{aligned}$$

$$\begin{aligned} x_i &= d_i.d_{i+1}.d_{i+2}...d_{31} \\ w_i &= \alpha_i + \beta_{i-1} \quad for \quad (i > 0) \\ w_0 &= \alpha_0 \end{aligned}$$

If $\Delta_{31} < 0$, upper signal wins and answer is 0. And if $\Delta_{31} > 0$, then the lower signal wins and the answer is 1.

$$\Rightarrow \frac{sign(w^T X + b) + 1}{2}$$

This means if we find w, b parameters then we can predict response to any challenge.
Similarly, we can show the proof for the 2^{nd} PUF (reference PUF).

For working PUF, let us assume $(\Delta w)_{31}$
For reference PUF, let us assume $(\Delta r)_{31}$

In the given question, we require a linear model to break two PUF whose time difference $|(\Delta w)_{31} - (\Delta r)_{31}|$ is smaller than some unknown $\tau > 0$

$$\Rightarrow |(\Delta w)_{31} - (\Delta r)_{31}| < \tau$$

So, now we will prove Melbo wrong and give a single linear model to break such combination of PUF.

$$\begin{aligned} (\Delta w)_{31} &= w_0.x_0 + w_1.x_1 + ... + w_{31}.x_{31} + \beta_{31} \\ &= w^T X + b \qquad ...[b = \beta_{31}] \end{aligned}$$

$$\Rightarrow \begin{pmatrix} w_0 & w_1 & w_2 & \cdots & w_{31} & \beta_{31} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{31} \\ 1 \end{pmatrix}$$

$$w_i = \alpha_i + \beta_{i-1} \quad for \quad (i > 0, I \in I)$$

α_i & β_i are system constant for working PUF.

No questions assigned to the following page.

$$
\begin{aligned}
(\Delta r)_{31} &= v_0.x_0 + v_1.x_1 + ... + v_{31}.x_{31} + \beta_{31} \\
&= v^T X + b \qquad ...[b = B_{31}]
\end{aligned}
$$

$$\Rightarrow \begin{pmatrix} v_0 & v_1 & v_2 & \cdots & v_{31} & B31 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{31} \\ 1 \end{pmatrix}$$

$$v_i = A_i + B_{i-1} \quad for \quad (i > 0, i \in I)$$

A_i & B_i are system constant for reference PUF.

given -

$$|(\Delta w) - (\Delta r)| \leq \tau \rightarrow 1$$

$$|(\Delta w) - (\Delta r)| > \tau \rightarrow 0$$

From the lecture notes we know :

$$(\Delta w) = u^T.x + P$$

$$(\Delta r) = v^T.x + Q$$

$$|(\Delta w) - (\Delta r)| = |(u - v)^T.x + (P - Q)|$$

$$|(\Delta w) - (\Delta r)| - \tau = |(u - v)^T.x + (P - Q)| - \tau$$

as far as bit is concerned, it will be :

$$\frac{1 + sign(|(u - v)^T.x + (P - Q)| - \tau)}{2}$$

So we can see that above expression is for a genearalized linear model

Now, we can prove that $sign(|a| - b)$ is same as $sign(a^2 - b^2)$

So, we can say that

$$sign(|(u - v)^T.x + (P - Q)| - \tau) = sign(((u - v)^T.x + (P - Q))^2 - \tau^2)$$

let $(u - v) \rightarrow \alpha$ & $(P - Q) \rightarrow \beta$

$$\Rightarrow sign((\alpha^T.x + \beta)^2 - \tau^2)$$

$\alpha^T.x =$ can be expanded as $\rightarrow (\alpha_1.x_1 + \alpha_2.x_2 + \alpha_3.x_3 + \cdots + \alpha_{32}.x_{32})$

$\Rightarrow$ sign(($\alpha_1^2.x_1^2 + \alpha_2^2.x_2^2 + \alpha_3^2.x_3^2 + \cdots + \alpha_{32}^2.x_{32}^2$) + C)

also value of $(x_1, x_2 \cdots x_{32})$ is either (1 or -1) so value of $(x_1^2, x_2^2 \cdots x_{32}^2)$ will be 1 only

So Now,

$$\Rightarrow sign(\sum_{\substack{i,j=1 \\ i \neq j}}^{32} \alpha_i.\alpha_j.x_i.x_j + \text{C})$$

No questions assigned to the following page.

Question 3:

LinearSVC		
Loss	Accuracy	time
Hinge	98.93	51s
Squared hinge	99.19	1m 1s

Table 1: Changing the loss hyperparameter in LinearSVC (hinge vs squared hinge)

c	LinearSVC	
	Accuracy	Time
100	99.2	1m 38s
1	99.16	1m 1s
0.01	98.65	6s

c	Logistic Regression	
	Accuracy	Time
100	99.31	3s
1	99.07	3s
0.01	96.35	2s

Table 2: Changing the c hyperparameter in LinearSVC and LogisticRegression to high/low/medium values

tol	LinearSVC	
	Accuracy	Time
High	97.21	25s
Medium	99.04	59s
Low	99.19	1m 18s

tol	Logistic Regression	
	Accuracy	Time
High	99.07	1s
Medium	99.07	2s
Low	99.07	3s

Table 3: Changing the tol hyperparameter in LinearSVC and LogisticRegression to high/low/medium values

Penalty	LinearSVC		Logistic Regression	
	Accuracy	Time	Accuracy	Time
l1	99.1425	12m 40s	N/A	N/A
l2	99.19	1m	99.07	2s

Table 4: Changing the penalty (regularization) hyperparameter in LinearSVC and LogisticRegression (l2 vs l1)