CS771 Assignment 1

VIVEK RAJ, SHUBHAM JANGID, ABHIJEET KUMAR, KUSHAL MAHESHWARI, KUNAL SAINI

TOTAL POINTS

53 / 60

QUESTION 1

1 Simple XORRO PUF 10 / 10

✓ **+ 10 pts** *A valid derivation showing how the simple XORRO PUF can be cracked using a single linear model*

- 3 pts Minor mistakes in derivation or else not enough details in the derivation.

+ 0 pts Completely wrong or else unanswered

QUESTION 2

2 Advanced XORRO PUF 10 / 10

✓ **+ 10 pts** *A valid derivation showing how the advanced XORRO PUF can be cracked using a collection of linear models*

- 3 pts Minor mistakes in derivation or else not enough details in the derivation.

+ 0 pts Completely wrong or else unanswered

QUESTION 3

3 Coding marks 30 / 35

+ 0 pts Enter marks directly using point adjustment

+ 30 *Point adjustment*

GROUP NO: 44

Grading scheme for code:

Training time tt (in sec): tt < 2 (7 marks), 2 <= tt < 4 (6 marks), 4 <= tt < 8 (5 marks), tt > 8 (4 marks)

Inference time ti (in sec): ti < 2 (10 marks), 2 <= ti < 4 (8 marks), 4 <= ti < 8 (6 marks), ti > 8 (4 marks)

Model size ms (in KB): ms < 50 (8 marks), 50 <= ms < 100 (7 marks), 100 <= ms < 200 (6 marks), ti > 200 (5 marks)

Accuracy ac: ac > 0.99 (10 marks), 0.95 <= ac < 0.99 (8 marks), 0.90 <= ac < 0.95 (6 marks), ac < 0.90 (4 marks)

tt = 1.56 sec : 7 marks

ti = 1.948 sec : 10 marks

ms = 87.22 KB : 7 marks

ac = 0.9415 : 6 marks

TOTAL: 30 marks

QUESTION 4

4 Hyperparameter Experiments 3 / 5

+ 5 pts Reporting effect of at least two hyperparameter changes on training time and test accuracy as asked in the assignment problem statement (see page 7 of assn1.pdf)

+ 3 pts Effect of at only one hyperparameter change is reported

- 1 pts Minor issues with reporting the results e.g. graphs with unclear axis labels, ambiguous figures, etc

+ 0 pts Completely wrong or else unanswered

✓ **+ 3 pts** *only one of either change on training time or test accuracy in reported*

Assignment-1

Abhijeet Kumar(190020) **Shubham Jangid(19817831)** **Vivek Raj(190989)**

Kushal Maheshwari(190452) **Kunal Saini(190448)**

1 Mathematical derivation to break simple break a simple XORRO PUF by a single linear model.

For breaking simple XORRO by a single linear model In this, we have to find the parameters for the individual XORRO.

$$Let\ \delta_{00}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 00\ ,$$
$$Let\ \delta_{01}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 01\ ,$$
$$Let\ \delta_{11}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 11\ ,$$
$$Let\ \delta_{10}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 10\ ,$$

Let a_i be the challenge bit for the i^{th} XOR gate and let D_i be the input bit for the i^{th} XOR gate.

Let $t_i^{D_i,U}$ be the time taken by the $i^{\text{th}}XORRO$ when the input bit is D_i for the UPPER XORRO for the first cycle,

$t_i^{D_i,U} \quad = \quad t_{i-1}^{D_i,U} \ + \ \delta_{00}^{U,i}\left(1-a_i\right)\left(1-D_i\right) \ + \ \delta_{10}^{U,i}a_i\left(1-D_i\right) \ + \ \delta_{01}^{U,i}\left(1-a_i\right)D_i \ \ +\delta_{11}^{U,i}D_ia_i$ ...eq-1
Let $t_i^{D_i',U}$ be the time taken by the $i^{\text{t}}\ XORRO$ when the input bit is D_i' for the UPPER XORRO for the Second cycle,

$t_i^{D_i',U} = t_{i-1}^{D_i',U} + \delta_{00}^{U,i}\left(1-a_i\right)\left(1-D_i'\right) + \delta_{10}^{U,i}a_i\left(1-D_i'\right) + \delta_{01}^{U,i}\left(1-a_i\right)D_i' + \delta_{11}^{U,i}D_i'a_i$ ...eq-2

Since the output bit for the ith XOR gate in the first round will be complement of the output bit for the ith XOR gate in the second round and so we can write the following relation:

Adding equation 1 and 2, we get total time taken for one oscillation by the upper XORRO as:
$t_i^U = t_{i-1}^U + \delta_{00}^{U,i}\left(1-a_i\right) + \delta_{10}^{U,i}a_i + \delta_{01}^{U,i}\left(1-a_i\right) \ + \delta_{11}^{U,i}a_i$ ...eq-3

$t_i^U = t_{i-1}^U + \delta_{00}^{U,i} + + \delta_{01}^{U,i} - \delta_{00}^{U,i}a_i + \delta_{10}^{U,i}a_i - \delta_{01}^{U,i}a_i + \delta_{11}^{U,i}a_i$ ...eq-4

$t_i^U = t_{i-1}^U + \delta_{00}^{U,i} + \delta_{01}^{U,i} + (-\delta_{00}^{U,i} + \delta_{10}^{U,i} - \delta_{01}^{U,i} + \delta_{11}^{U,i})a_i$ ...eq-5

Similarly we can write the equation for the time taken for one oscillation by the lower XORRO as:

$t_i^L = t_{i-1}^L + \delta_{00}^{L,i} + \delta_{01}^{L,i} + (-\delta_{00}^{L,i} + \delta_{10}^{L,i} - \delta_{01}^{L,i} + \delta_{11}^{L,i})a_i$ ...eq-6

$$D_i + D_i' = 1 t_i^u - t_i^L \qquad = \Delta_i$$

$$\Delta_i = \Delta_{i-1} + (1-a_i)\left[\delta_{00}^{u,i} + \delta_{01}^{u,i} - \left(\delta_{00}^{L,i} + \delta_{01}^{L,i}\right)\right] \quad + a_i\left[\left(\delta_{10}^{u,i} + \delta_{11}^{u,i}\right) - \left(\delta_{10}^{L,i} + \delta_{11}^{L,i}\right)\right]$$

Preprint. Under review.

1 Simple XORRO PUF 10 / 10

- ✓ **+ 10 pts** *A valid derivation showing how the simple XORRO PUF can be cracked using a single linear model*
- **- 3 pts** Minor mistakes in derivation or else not enough details in the derivation.
- **+ 0 pts** Completely wrong or else unanswered

Assignment-1

Abhijeet Kumar(190020) **Shubham Jangid(19817831)** **Vivek Raj(190989)**

Kushal Maheshwari(190452) **Kunal Saini(190448)**

1 Mathematical derivation to break simple break a simple XORRO PUF by a single linear model.

For breaking simple XORRO by a single linear model In this, we have to find the parameters for the individual XORRO.

$$Let\ \delta_{00}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 00\ ,$$
$$Let\ \delta_{01}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 01\ ,$$
$$Let\ \delta_{11}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 11\ ,$$
$$Let\ \delta_{10}\ be\ the\ time\ taken\ when\ both\ input\ bits\ are\ 10\ ,$$

Let a_i be the challenge bit for the i^{th} XOR gate and let D_i be the input bit for the i^{th} XOR gate.

Let $t_i^{D_i,U}$ be the time taken by the $i^{\text{th}} XORRO$ when the input bit is D_i for the UPPER XORRO for the first cycle,

$t_i^{D_i,U} \quad = \quad t_{i-1}^{D_i,U} \; + \; \delta_{00}^{U,i}\left(1-a_i\right)\left(1-D_i\right) \; + \; \delta_{10}^{U,i}a_i\left(1-D_i\right) \; + \; \delta_{01}^{U,i}\left(1-a_i\right)D_i \;\; +\delta_{11}^{U,i}D_ia_i$ ...eq-1

Let $t_i^{D'_i,U}$ be the time taken by the $i^{\text{t}}\ XORRO$ when the input bit is D'_i for the UPPER XORRO for the Second cycle,

$t_i^{D'_i,U} = t_{i-1}^{D'_i,U} + \delta_{00}^{U,i}\left(1-a_i\right)\left(1-D'_i\right) + \delta_{10}^{U,i}a_i\left(1-D'_i\right) + \delta_{01}^{U,i}\left(1-a_i\right)D'_i + \delta_{11}^{U,i}D'_ia_i$ ...eq-2

Since the output bit for the ith XOR gate in the first round will be complement of the output bit for the ith XOR gate in the second round and so we can write the following relation:

Adding equation 1 and 2, we get total time taken for one oscillation by the upper XORRO as:
$t_i^U = t_{i-1}^U + \delta_{00}^{U,i}\left(1-a_i\right) + \delta_{10}^{U,i}a_i + \delta_{01}^{U,i}\left(1-a_i\right) \; + \delta_{11}^{U,i}a_i$ ...eq-3

$t_i^U = t_{i-1}^U + \delta_{00}^{U,i} + +\delta_{01}^{U,i} - \delta_{00}^{U,i}a_i + \delta_{10}^{U,i}a_i - \delta_{01}^{U,i}a_i + \delta_{11}^{U,i}a_i$ ...eq-4

$t_i^U = t_{i-1}^U + \delta_{00}^{U,i} + \delta_{01}^{U,i} + (-\delta_{00}^{U,i} + \delta_{10}^{U,i} - \delta_{01}^{U,i} + \delta_{11}^{U,i})a_i$ ...eq-5

Similarly we can write the equation for the time taken for one oscillation by the lower XORRO as:
$t_i^L = t_{i-1}^L + \delta_{00}^{L,i} + \delta_{01}^{L,i} + (-\delta_{00}^{L,i} + \delta_{10}^{L,i} - \delta_{01}^{L,i} + \delta_{11}^{L,i})a_i$ ...eq-6

$$D_i + D'_i = 1t_i^u - t_i^L \qquad\qquad = \Delta_i$$
$$\Delta_i = \Delta_{i-1} + (1-a_i)\left[\delta_{00}^{u,i} + \delta_{01}^{u,i} - \left(\delta_{00}^{L,i} + \delta_{01}^{L,i}\right)\right] \quad +a_i\left[\left(\delta_{10}^{u,i} + \delta_{11}^{u,i}\right) - \left(\delta_{10}^{L,i} + \delta_{11}^{L,i}\right)\right]$$

Preprint. Under review.

$$\Delta_i = \Delta_{i-1} + \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i} - a_i \left[\delta_{00}^{u,i} + \delta_{01}^{u,i} - \left(\delta_{00}^{L,i} + \delta_{01}^{L,i}\right) + \delta_{10}^{u,i} + \delta_{11}^{u,i} - \delta_{10}^{L,i} - \delta_{11}^{L,i}\right]$$

$$\beta i = \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i}$$

$$-\alpha_i = \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i} + \delta_{10}^{U,i} + \delta_{11}^{U,i} - \delta_{10}^{L,i} - \delta_{11}^{L,i}$$

$$\Delta_i = \Delta_{i-1} + \beta_i + \alpha_i a_i$$

$$\Delta_{63} = \beta^0 + \beta^1 + \ldots \beta^{63} + \alpha_0 a_0 + \ldots..\alpha_{63} a_{63}$$

If
$Delta_{63}$ > 0 then the output is 1 else it is 0 and hence the output depends only on the sign of $Delta_{63}$ hence output can be written as :

$$Y = W^\top X + B$$

2 To extend the above linear model to crack an Advanced XORRO PUF

Using the linear model above, that is, logistic regression, we can further extend it to crack Advanced XORRO PUF as the multiplexers choose two XORRO from the given, select bits of length 4 four each. Now after the XORRO gets chosen, the problem becomes same as Simple XORRO PUF. Now there will be $\binom{16}{2}$ = 120 combinations possible, which is equal to 120 Simple XORRO PUFs as 2^4 is 16 so there is 16 XORRO PUFS thus $\binom{16}{2}$. So we can train 120 linear models to crack Advanced XORRO PUF.

3 Code is submitted

4 Outcome of experiment

For this machine learning problem we use only sklearn as our main library. We also numpy library to manipulate data. Since this is a classification problem we used linear classifier SVC , RC, Logistic regression,etc. Since the bit prediction equation comes out same as the hypothesis used in logistic regression we predicted logistic regression will be best for the data modelling. The accuracy on training data and cross-validation came out be as

	Training	CV
RC	92	81
LR	98	9389
SVC	94	83.22

We also tried tuning other parameters in logistic regression such as solver, C value, Class Weights but changing this value was diverting away from the accuracy we got using default values.

2 Advanced XORRO PUF 10 / 10

✓ **+ 10 pts** *A valid derivation showing how the advanced XORRO PUF can be cracked using a collection of linear models*

- 3 pts Minor mistakes in derivation or else not enough details in the derivation.

+ 0 pts Completely wrong or else unanswered

3 Coding marks 30 / 35

+ 0 pts Enter marks directly using point adjustment

+ 30 *Point adjustment*

GROUP NO: 44

Grading scheme for code:

Training time tt (in sec): tt < 2 (7 marks), 2 <= tt < 4 (6 marks), 4 <= tt < 8 (5 marks), tt > 8 (4 marks)

Inference time ti (in sec): ti < 2 (10 marks), 2 <= ti < 4 (8 marks), 4 <= ti < 8 (6 marks), ti > 8 (4 marks)

Model size ms (in KB): ms < 50 (8 marks), 50 <= ms < 100 (7 marks), 100 <= ms < 200 (6 marks), ti > 200 (5 marks)

Accuracy ac: ac > 0.99 (10 marks), 0.95 <= ac < 0.99 (8 marks), 0.90 <= ac < 0.95 (6 marks), ac < 0.90 (4 marks)

tt = 1.56 sec : 7 marks

ti = 1.948 sec : 10 marks

ms = 87.22 KB : 7 marks

ac = 0.9415 : 6 marks

TOTAL: 30 marks

$$\Delta_i = \Delta_{i-1} + \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i} - a_i \left[\delta_{00}^{u,i} + \delta_{01}^{u,i} - \left(\delta_{00}^{L,i} + \delta_{01}^{L,i}\right) + \delta_{10}^{u,i} + \delta_{11}^{u,i} - \delta_{10}^{L,i} - \delta_{11}^{L,i}\right]$$

$$\beta i = \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i}$$

$$-\alpha_i = \delta_{00}^{u,i} + \delta_{01}^{u,i} - \delta_{00}^{L,i} - \delta_{01}^{L,i} + \delta_{10}^{U,i} + \delta_{11}^{U,i} - \delta_{10}^{L,i} - \delta_{11}^{L,i}$$

$$\Delta_i = \Delta_{i-1} + \beta_i + \alpha_i a_i$$

$$\Delta_{63} = \beta^0 + \beta^1 + \ldots \beta^{63} + \alpha_0 a_0 + \ldots..\alpha_{63} a_{63}$$

If
$Delta_{63}$ > 0 then the output is 1 else it is 0 and hence the output depends only on the sign of $Delta_{63}$ hence output can be written as :

$$Y = W^\top X + B$$

2 To extend the above linear model to crack an Advanced XORRO PUF

Using the linear model above, that is, logistic regression, we can further extend it to crack Advanced XORRO PUF as the multiplexers choose two XORRO from the given, select bits of length 4 four each. Now after the XORRO gets chosen, the problem becomes same as Simple XORRO PUF. Now there will be $\binom{16}{2}$ = 120 combinations possible, which is equal to 120 Simple XORRO PUFs as 2^4 is 16 so there is 16 XORRO PUFS thus $\binom{16}{2}$. So we can train 120 linear models to crack Advanced XORRO PUF.

3 Code is submitted

4 Outcome of experiment

For this machine learning problem we use only sklearn as our main library. We also numpy library to manipulate data. Since this is a classification problem we used linear classifier SVC , RC, Logistic regression,etc. Since the bit prediction equation comes out same as the hypothesis used in logistic regression we predicted logistic regression will be best for the data modelling. The accuracy on training data and cross-validation came out be as

	Training	CV
RC	92	81
LR	98	9389
SVC	94	83.22

We also tried tuning other parameters in logistic regression such as solver, C value, Class Weights but changing this value was diverting away from the accuracy we got using default values.

4 Hyperparameter Experiments 3 / 5

+ 5 pts Reporting effect of at least two hyperparameter changes on training time and test accuracy as asked in the assignment problem statement (see page 7 of assn1.pdf)

+ 3 pts Effect of at only one hyperparameter change is reported

- 1 pts Minor issues with reporting the results e.g. graphs with unclear axis labels, ambiguous figures, etc

+ 0 pts Completely wrong or else unanswered

✓ **+ 3 pts** *only one of either change on training time or test accuracy in reported*