Homework 2: Report

Lecturer: Dr. Adi Akavia Student(s): Yara Shamali, Samih Warwar, Maias Omar

Abstract

In this article we take a deeper look into a a popular cryptographic tool called One Time Truth Table or OTTT , that is used to ensure secure communication between multiple parties .

1 Introduction

In the field of information security, ensuring the confidentiality and integrity of sensitive data is of utmost importance. Cryptography is an effective method for achieving this,one of the ways it can be applied is by the One-Time Truth Table.

Motivation. The motivation behind this technique is to enable secure communication between parties by ensuring that both parties have a shared understanding of the cryptographic algorithm or function being used for encryption or decryption without uncovering private data .

Secure Computation Technique. here we will explore and implement a secure two-party protocol for computing the function specified in the euqation below using the passively secure One-Time Truth-Table (OTTT) protocol.

Application. we implemented OTTT to solve the boolean equation down below , using key techniques that include : an offline phase which is the process of generating the truth table for a specific cryptographic function or algorithm before any communication or encryption takes place.
online phase : which is the process of using the precomputed truth table to encrypt or decrypt the data in real-time.

$$f_{a,4}(x) = \begin{cases} 1 & \text{if } ax \geq 4 \\ 0 & \text{otherwise} \end{cases}$$

2 Protocols

The protocol utilized the One-Time Truth Table (OTTT) technique to develop a user-friendly system that enables efficient and secure data sharing while protecting each party's confidentiality.

To achieve this, the following steps were taken:

2.1 Offline Phase

parties : trusted dealer D with truth table T.

1. we begin with a truth table that inputs all possibilities for a and x .
2. Draw random row/col shifts: $r, c \in 1, \ldots, 2n$.
3. Draw a random $2^n X 2^n$ Boolean matrix M_B.
4. Compute:$M_A[i,j] = M_B[i,j] \oplus T[i–r \mod 2n, j–c \mod 2n]$.
5. output (r, M_A) to party I,and (c, M_B) to party II.

2.2 Online Phase

Parties: Party I A with (r, M_A)(from offline phase) and input x, Party II B with (c, M_B)(from offline phase) and input a.

1. Party I computes $u = x + r \mod 2n$, and sends u to Party II.
2. Party II computes $v = a + c \mod 2n$,$z_B = M_B[u, v]$,and sends $(v, Z_B)$to Party I.
3. Party I outputs $z = M_A[u, v] \oplus z_B$.

3 Implementation

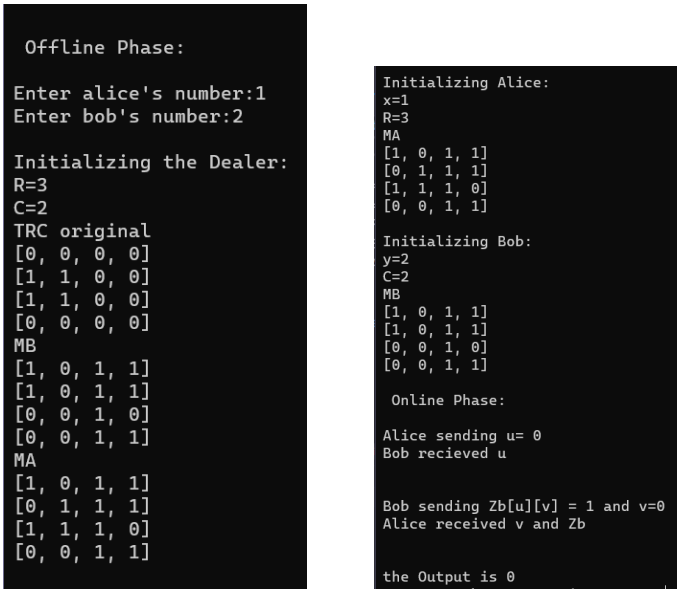
• Party I (Alice) has input $x \in 0, 1, 2, 3$.
• Party II (Bob) has input $a \in 0, 1, 2, 3$.

Truth table for Equation 2:

xa	0	1	2	3
0	0	0	0	0
1	0	0	0	0
2	0	0	1	1
3	0	0	1	1

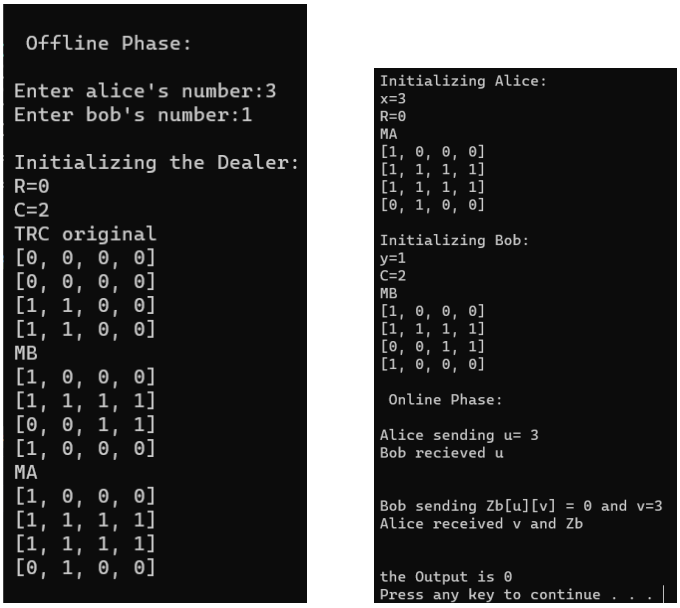
• online phase : (Alice(x = 1, r = 3) and Bob(a = 2, c = 2)):
• Alice computes $u = x + r \mod 4 = 1 + 3 \mod 4 = 0$, and sends u to Bob.
• Bob computes $v = a + c \mod 4 = 2 + 2 \mod 4 = 0$, and $z_B = M_B[u, v] = M_B[0, 0] = 1$,and sends $(v, Z_B) = (0, 1)$ to Alice.
• Alice outputs:$z = M_A[u, v] \oplus z_B$, $= M_A[0, 0] \oplus 1$, $= 1 \oplus 1 = 0$.

4 Empirical Evaluation



(a) (b)

Figure 1: here we have an examples where is Alice chose 1 and Bob chose 2



(a) (b)

Figure 2: here we have an examples where is Alice chose 3 and Bob chose 1

5 Conclusions

In summary, this article presented an implementation of the One-Time Truth Table (OTTT) technique for solving a boolean equation in a secure and efficient manner. The protocol was implemented using the OTTT tool, which generated a shared truth table between the parties and performed the comparison operation in a privacy-preserving manner.

The importance of this work lies in its contribution to the field of secure computation, where privacy-preserving protocols are essential for protecting sensitive data.

The results of our empirical evaluation showed that the OTTT technique is a viable solution for solving a boolean Problem, with a low computational overhead and high level of security. The protocol was implemented using Python and the results were evaluated using the OTTT tool, which demonstrated the efficiency and practicality of the technique.