RWTH AACHEN UNIVERSITY

Lecture "Privacy Enhancing Technologies for Data Science" (PETs4DS)
Winter Semester 2016/17
Informatik 5, Lehrstuhl Prof. Decker

Assignment 3

Date for exercise session : 20.12.2016

Information:

1. Participants are encouraged to present their solutions for the exercises.
2. In addition, solutions to the exercises will be presented at the exercise session and published in L2P.
3. Working on the exercises in groups is welcome.
4. The assignments of this lecture series are not graded.
5. Instead, participation in the exams depends on passing the presence exercise in January.

Execise 1: Secure Big-Data Analytics in the Cloud

(a) Shortly explain the idea of using fully homomorphic encryption (FHE) for secure cloud computing. Can you think of a reason why FHE is not a good solution for more than 2 parties?

(b) Think of possible attacks on fully homomorphic encryption and explain verifiable computation in this context.

(c) Explain which properties are provided by secure multiparty computation which are not provided by a combination of fully homomorphic encryption and verified computation.

Exercise 2: Secure Multiparty Computation (SMPC) for Exactly Three Parties

(a) Can SMPC be applied to untrusted clouds ? If yes, which circumstances have to be fulfilled ?

(b) Consider the Secure Addition Protocol for three parties from slide 42 of the lecture. Prove the correctness of the result, by showing that the sum of verification shares s_j is the same as the sum of the inputs x_i.

(c) Can the Secure Addition Protocol also be used for two parties? Explain shortly why or why not.

(d) Apply the Secure Multiplication Protocol from slide 49 for the Parties P_1 with input $a = 3$, P_2 with input $b = 15$ and P_3 with no input. The calculation should be done in $\mathbb{F}_{13}$.

(e) Consider P_3 helping P_1 and P_2 to do secure multiplication. Show that the Protocol Secure Multiplication is indeed insecure if he reveals his information to P_1 and P_2.

Exercise 3: Lagrange Interpolation and the Recombination Vector

Determine the recombination vector r for the following setting:

- Use $\mathbb{F}_7$ for the calculation.
- $t = 2$
- There are seven parties.
- Parties P_2, P_5 and P_7 are colluding.

Exercise 4: SMPC Using the Circuit Evaluation with Passive Security (CEPS) Protocol

(a) Shortly explain the four steps of the CEPS-Protocol.

(b) What is the advantage of describing a function as an arithmetic circuit?

(c) Consider the Parties P_1, P_2, P_3 with the inputs $I_1 = 4, I_2 = 1$ and $I_3 = 9$. The function $f(x) = (I_1 + I_2) * (5 * I_3)$ should be calculated in $\mathbb{F}_{11}$ and $t = 1$.

- Draw the corresponding arithmetic circuit.
- Evaluate the circuit using the CEPS protocol. Also determine the result by using the output reconstruction step.

(d) How is the interim result stored after every evaluation step ?

(e) How would you need to change the evaluation of the circuit if there is an additional fourth party P_4, independent of the changes to $f(x)$?

(f) How many nodes can be untrusted when using CEPS?

(g) Can you think of possible attacks on CEPS?