CSCI 3907-83/6907-81 February 17, 2020

Homework Assigment 2

Due Feb. 26

Please answer each of the below questions. Remember, you may work together, but everyone MUST write up and understand their own solutions. Additionally, you may reference other sources such as papers, lecture notes, etc., but solutions that appear copied will be considered a violation of the academic honesty code. Also, you must list all people you work with and cite any references used.

Note, this homework is challenging, so please start early and feel free to email me if you have questions.

1. **Security vs. Additive Attacks**

   Recall that in class we learned that the (semi-honest) Damgard-Nielsen protocol is vulnerable to an *additive attack*. That is, an adversary can introduce an arbitrary additive term into the result of a multiplication gate (i.e., the adversary can choose a value δ, and then cause the output of a multiplication gate $c = ab + \delta$ instead of just ab).

   Chida et al. [1] show how to overcome this attack by using a random MAC key α and computing on pairs $([x], [\alpha x])$ and $([y], [\alpha y])$. Consider a circuit consisting of a single multiplication gate. Show that if an adversary is able to use an additive attack successfully to break security of Chida et al. (i.e., he is able to produce a validly MACed output), then he can compute the value α. That is, show that for an additive attack to succeed, the adversary must guess the value of α.

2. **Linear Attacks**

   We mentioned in class that an *additive attack* on the (semi-honest) Damgard-Nielsen protocol does not break the privacy of the protocol (i.e., it does not allow the malicious adversary to learn anything about the inputs or intermediary values). Explain why this is so. Specifically, consider how an adversary can cause an additive attack and explain why this does not help him learn any secret values.

   DO NOT DO THE SECOND PART OF PROBLEM 2

   Now, consider a stronger variant of an additive attack called a *linear attack* where instead of adding an arbitrary value of his choice, an adversary can add a value that depends on an input he does not know. Specifically, suppose we wish to compute $z = x \cdot y$. Now, consider an adversary whose input is y and suppose that this adversary is able to mount a linear attack so instead of $[z]$, the protocol computes $[z'] = [x \cdot y + x]$. Show, how this adversary can learn the value of x. (Assume that the output of the computation is opened to both parties).

3. **Garbled Circuits**

   In class, we described how to garble a Boolean gate, that is a gate that takes two bits as input and outputs a bit. Now consider an ADD mod 3 gate. This is a gate that inputs two numbers $a, b \in \{0, 1, 2\}$ and outputs $c \in \{0, 1, 2\}$ such that $[c = a + b \bmod 3]$.

(a) Describe how you could garble an ADD mod 3 gate directly. That is, do not convert it to a circuit of standard Boolean gates, but directly build a garbled table for this gate. (Hint: Think of how you would garble the "truth table" of this gate.)

(b) Show how to generalize the free-XOR technique to get free-ADD mod 3. Specifically, describe how we should choose the wire labels to make additions gates free.

4. **Dual-Execution Garbled Circuits**

Consider the following attempt to make garbled circuits maliciously secure for 2-party computation between P_1 and P_2. To evaluate a circuit C, we run two copies of the garbled circuit protocol (on the same circuit C), where in copy 1, P_1 is the garbler and P_2 is the evaluator and, in copy 2, P_2 is the garbler and P_1 is the evaluator. Now, before revealing the output (i.e., the mapping between the output wire label and the output value), the parties check (via a secure comparison) whether the outputs in the two executions are the same. If they are, then open the output, and if they are not, then abort.

Is this protocol secure against a malicious adversary corrupting one of the parties? Why or why not?

References

[1] Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, and Ariel Nof. Fast large-scale honest-majority MPC for malicious adversaries. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 34–64. Springer, 2018.