ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 1

1.1 Padlocks

a) Consider a setting where there are two combination padlocks (e.g., with three wheels with 10 positions each), which can only be opened by someone who knows the corresponding secret combinations. Vic does not know the combinations. Peggy claims that she knows the combination for one of the padlocks and would like to convince Vic of this fact while Vic should learn neither the combination nor for which padlock Peggy knows the combination. Describe a protocol that meets Peggy's requirements. Is your protocol complete and sound? Is the above task a proof of a statement or a proof of knowledge?

b) Consider 100 combination padlocks, where Vic knows the combinations for all of them. Give a protocol that allows Peggy to prove to Vic that she knows the combination for *at least one* of the padlocks (without revealing which one).

c) Consider 7 padlocks, where Vic knows the combinations for all of them. Peggy now claims that she knows the combinations to open *at least* two of them. Describe a protocol that allows Peggy to prove her claim to Vic without revealing the padlocks she knows.

HINT: Use the above proof several times for different subsets of the 7 padlocks.

1.2 Kit Kat

Peggy and Vic are exhausted after studying Cryptographic Protocols the whole afternoon. They decide to take a break and buy a Kit Kat each. After buying both Kit Kat, Peggy claims that her Kit Kat is smaller, but for Vic both Kit Kat are identical. How can Peggy prove to Vic that she can distinguish between the two Kit Kat?

a) Construct a zero-knowledge protocol to prove to Vic that she can distinguish the two KitKat. Argue (informally) why it is complete and sound.

b) Construct a zero-knowledge protocol for the case where Peggy claims that she can distinguish between all three Kit Kat.

c) Consider again three Kit Kat. Construct a zero-knowledge protocol for the case where Peggy claims that one Kit Kat is different to the other two.

HINT: Assume that Vic can use glue to stick the Kit Kat onto a round table.

1.3 Where is Waldo?

Where's Waldo? is a puzzle book that contains very detailed pictures with many different characters. The goal for each picture is to find Waldo, a predefined character.

Peggy and Vic are playing Where's Waldo?, when Peggy suddenly claims that she knows where Waldo is. However, Vic does not believe her. How can Peggy prove to Vic that she knows where Waldo is without revealing his location?

a) Construct an interactive proof that allows Peggy to prove that she knows where Waldo is without revealing his location. Argue (informally) why it is complete and sound.

b) Is the protocol zero-knowledge? What information is and what is not leaked to Vic?