ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 1

1.1 Padlocks

a) Vic hands Peggy both closed padlocks and looks away. Peggy locks one with the other (forming a chain) and shows the chain to Vic; if she succeeds, then she has proved that she can open one of the padlocks. The protocol is trivially complete: if Peggy knows the combination, she always succeeds. Intuitively, the protocol is also sound, as there does not seem to be any way of succeeding without opening at least one of the padlocks.

The task is a proof of knowledge, i.e., knowledge of the combination.

b) As Vic knows all the combinations, he can construct two chain rings of 50 padlocks each, such that padlock i, for $0 \leq i < 50$, is "chained" to padlocks $i-1$ and $i+1$ (mod 50) forming the first ring, and padlocks $50+i$, for $0 \leq i < 50$, form the second ring similarly. Vic gives the rings to Peggy and looks away. Peggy, to prove that she knows the combination for opening at least one of the padlocks, opens one of the rings (by opening the padlock whose combination she knows), interlock the two rings together, and shows the result to Vic. Vic accepts if the two chain rings are interlocked together.

Completeness, soundness, and zero-knowledge are readily verified.

c) Observe that Peggy knows the combination to at least two padlocks out of seven if and only if she knows the combination to one padlock out of any subset of six padlocks.

Hence, Peggy can use the above protocol to prove sequentially that she knows one out of six padlocks, for every possible set of six padlocks.

Completeness, soundness, and zero-knowledge are readily verified.

1.2 Kit Kat

a) Peggy gives Vic both Kit Kat. Vic holds a Kit Kat in each hand. At this point, Peggy can see which hand holds which Kit Kat. Then, Vic hides both Kit Kats behind his back and, with probability one half, he switches the Kit Kats. He then shows both hands to Peggy. Peggy then has to say whether Vic switched the position of the Kit Kats or not.

Completeness: If Peggy can distinguish the Kit Kats, she can always tell whether Vic changed the positions or not. Hence, Vic is convinced.

Soundness: If Peggy cannot distinguish the Kit Kats, she can only guess whether Vic switched the position of the Kit Kats, succeeding with probability one half. The protocol can be repeated to decrease the cheating probability of Peggy.

Zero-Knowledge: The protocol is intuitively zero-knowledge, since Vic does not learn any information about the Kit Kats beyond the fact that they are different.

b) Peggy gives Vic the three Kit Kat. Vic puts the three Kit Kats in a row. At this point Peggy can see which Kit Kat is in which position. Then, when Peggy looks away, he permutes the three Kit Kats uniformly at random. After that, Peggy sees the new configuration and has to tell which permutation Vic has executed.

Completeness: If Peggy can distinguish between the three Kit Kat, she can always tell how Vic changed the position of the Kit Kats. Hence, Vic is convinced.

Soundness: If Peggy cannot distinguish all three Kit Kats, she fails with probability at least one half. If the Kit Kats are not pairwise different, there is a pair of Kit Kats that Peggy cannot distinguish. Then, any permutation Vic chooses, Peggy cannot tell how the two identical Kit Kats where permuted, so Peggy can succeed with probability at most one half. The protocol can be repeated to decrease the cheating probability of Peggy.

Zero-Knowledge: The protocol is intuitively zero-knowledge, since Vic does not learn any information about the Kit Kats beyond the fact that they are pairwise different.

c) Peggy gives Vic the three Kit Kat. Vic glues the three Kit Kats on a round table symmetrically. At this point, Peggy can see which Kit Kat is in which position. Then, when Peggy looks away, Vic rotates uniformly at random the round table by 0, 120 or 240 degrees. After that, Peggy sees the new configuration and has to tell which rotation Vic has executed.

Completeness: If Peggy can distinguish one Kit Kat from the other two, she can always tell how much Vic has rotated the round table. Hence, Vic is convinced.

Soundness: If Peggy cannot distinguish any Kit Kat from the other two, she cannot tell how much Vic has rotated the table, and hence only succeeds with probability one third. The protocol can be repeated to decrease the cheating probability of Peggy.

Zero-Knowledge: The protocol is intuitively zero-knowledge, since Vic does not learn any information about the Kit Kats beyond the fact that there is one that is different to the others.

1.3 Where is Waldo?

a) Peggy and Vic use a large piece of cardboard (at least twice as large as the picture in each dimension) with a small rectangle hole in the middle. In order for Peggy to prove that she knows where Waldo is, she puts the rectangle hole on top of Waldo while Vic is not looking. At this point, Vic is able to see Waldo through the hole. However, Peggy could have placed a fake picture under the cardboard. To avoid that, Peggy also has to demonstrate that she has the correct Waldo picture (and hasn't changed the picture). Therefore, she covers the hole of the cardboard (e.g., with a post-it), and pulls the picture beneath the cardboard in front of Vic's eyes. Hence, Vic concludes that Peggy knows where Waldo is.

The protocol is trivially complete: if Peggy knows where Waldo is, Vic is convinced, since he sees Waldo through the rectangle, and then sees Peggy take the correct picture out of the cardboard. The protocol is also sound, because if Peggy does not know the location of Waldo, she cannot reveal Waldo through the rectangle hole of the cardboard and also prove that the Waldo picture is correct.

b) The protocol does not leak the location of Waldo, but still is not zero-knowledge. On one hand, since the cardboard is large enough to cover the picture (no matter where Waldo is), Vic learns nothing else about the location of Waldo in the picture. Also, when Peggy pulls out the picture out of the cardboard, she covers the rectangle hole so that no information about the place from which she is pulling the picture is revealed. On the other hand, some information is leaked during the execution of the protocol. For example, Vic not only sees Waldo through the rectangle, but also sees its immediate surroundings. Vic also learns information about Waldo in the picture. For example, the pose of Waldo in the picture, his face expression, etc.