ETH Zurich, Department of Computer Science
SS 2018

Prof. Ueli Maurer
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 Graph (Non-)Isomorphism

a) The GNI protocol from the lecture is not zero-knowledge because Vic could cheat by sending Peggy an arbitrary graph $\mathcal{K}$ and learn if $\mathcal{K}$ is isomorphic to $\mathcal{G}_0$ or $\mathcal{G}_1$.

b) The protocol is honest-verifier zero-knowledge, since in the case where the verifier follows the protocol, he chooses one bit b at random, and receives a bit $c = b$.

c) Let the three graphs be $(\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2)$. The verifier permutes each graph randomly generating $\mathcal{H}_i$ with $\mathcal{H}_i \cong G_i$ for $i \in \{0,1,2\}$, and chooses a shift uniformly at random $s \in \{0,1,2\}$. Let $\mathcal{K}_i := \mathcal{H}_{(i+s) \bmod 3}$, for $i \in \{0,1,2\}$. The verifier sends (K_0, K_1, K_2) to the prover, and the prover has to tell what s the verifier has chosen. If the prover succeeds, the verifier accepts. Otherwise, he rejects.

Completeness: If the three graphs $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2$ are not all isomorphic, the prover can tell which shift s the verifier has chosen.

Soundness: Assume that all graphs are isomorphic. In this case, the prover cannot tell which shift s the verifier has chosen. Hence, he cannot succeed with probability higher than one third.

Algorithm 1: $B(m)$ using square-root algorithm A

$r \leftarrow_R \{1, \ldots, m-1\}$
$p' \leftarrow \gcd(r, n)$
if $p' > 1$
  return p'
$a \leftarrow r^2$
$r' \leftarrow A(m, a)$
if $r' \equiv \pm r \pmod{m}$
  return $\perp$
return $\gcd(r + r', m)$

HONEST-VERIFIER ZERO-KNOWLEDGE: Intuitively, the above protocol is honest-verifier zero-knowledge because a cheating verifier chooses a random shift s, and then receives $s' = s$ from the prover.

1.3 Square Roots and Factoring

a) - By computing $1^2, 2^2, 3^2, \ldots \bmod n = 7$, one obtains $r = 3$ und $r' = 4$.
- Obviously, $r = 5$ is a root. Therefore so is $w' = 24 = 29 - 5 \equiv -w \pmod{n}$.

Generally, a number has either two square roots modulo a prime p or none. Thus, exactly half of the elements of $\mathbb{Z}_p^*$ are quadratic residues, and the other half are quadratic non-residues. For more information, see the lecture notes, Section 1.5.

Below we use that if $n = pq$ for two primes p and q, $\mathbb{Z}_n^*$ is isomorphic to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ (cf. lecture notes, Section 1.4) via the isomorphism[1]

$$\psi_n : \mathbb{Z}_n^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*, \quad x \mapsto (R_p(x), R_q(x)).$$

- Since $n = 35 = 5 \cdot 7$, we have that $\mathbb{Z}_{35}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_7^*$. Thus, it is sufficient to find the square roots of $\psi_{35}(11) = (1, 4) \in \mathbb{Z}_5^* \times \mathbb{Z}_7^*$ and see what they correspond to in $\mathbb{Z}_{35}^*$. The roots are $(\pm 1, \pm 2)$, i.e., $(1, 2)$, $(1, 5)$, $(4, 2)$, and $(4, 5)$. They correspond to $\psi_{35}^{-1}(1, 2) = 16$, $\psi_{35}^{-1}(1, 5) = 26$, $\psi_{35}^{-1}(4, 2) = 9$, and $\psi_{35}^{-1}(4, 5) = 19$ (these correspondences are obtained via the Chinese Remainder Theorem).

In the case where $n = 3 \cdot 5 \cdot 7 = 105$, $a = 4$, the square roots are $2, 23, 37, 47, 58, 68, 82, 103$. More generally, one can show that if n is the product of k distinct primes, an element $x \in \mathbb{Z}_n^*$ has either 2^k square roots or none.

b) The algorithm B is depicted above.

Recall that a quadratic residue $a \in \mathbb{Z}_m^*$ has four square roots $r, -r, r', -r'$. The idea behind factoring m given algorithm A for computing square roots modulo m, is the following: If r is chosen randomly, then conditioned on A invoked on $a = r^2$ finding some root r', we will have $r' \not\equiv \pm r \pmod{m}$ with probability $1/2$. This is due to the fact that a yields no information about which of the four roots it was computed from. If $r' \equiv \pm r \pmod{m}$, it outputs $\perp$ and fails. Otherwise, the algorithm outputs $\gcd(r + r', m)$, which actually is one of the prime factors as we show below:

Since $r^2 \equiv r'^2 \pmod{m}$, $(r - r')(r + r') \equiv 0 \pmod{m}$. Moreover, since $r \not\equiv \pm r' \pmod{m}$, m divides neither $(r - r')$ nor $(r + r')$. Therefore, either $(r - r')$ is a multiple of p and $(r + r')$ a multiple of q or vice-versa. Thus, computing $\gcd(r + r', m)$ yields one of the prime factors.

If $A(m, a)$ returns a square root of a uniformly randomly chosen quadratic residue a with probability α, then B succeeds with probability at least $\alpha/2$.

[1] $R_n(x)$ denotes the (unique) remainder when dividing x by n.