ETH Zurich, Department of Computer Science — Dr. Jonathan Bootle
HS 2023 — Karen Klein, Varun Maram, Antonio Merino Gallardo

Zero-Knowledge Proofs
Exercise 12

12.1 Feasibility of Non-Interactive Zero-Knowledge

Explain why the argument in the lectures (that if L has a non-interactive zero-knowledge proof *without a CRS*, then $L \in BPP$) does not apply when the NIZK has adaptive zero-knowledge *with CRS*, as defined in the lectures.

12.2 Non-Interactive Proofs of Quadractic Non-Residuosity

Given an odd prime integer p, recall that the Legendre symbol of $a \in \mathbb{Z}_p^*$, denoted $\left(\frac{a}{p}\right) \in \{-1, 1\}$, is computed as $a^{(p-1)/2} \bmod p$ and indicates whether a is a quadratic residue modulo p (i.e., whether there exists $b \in \mathbb{Z}_p^*$ such that $a = b^2 \bmod p$).

Let n be the product of two distinct primes p and q. The set of quadratic residues modulo n is further denoted QR_n. The Jacobi symbol of $a \in \mathbb{Z}_n^*$, denoted $J_n(a)$, is defined as $\left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) \in \{-1, 1\}$. Note that a Jacobi symbol can be computed in polynomial time. Denote by J_n^+ the subset of Z_n^* of elements of Jacobi symbol 1 and J_n^- the subset of elements of Jacobi symbol -1.

a) Show that $|J_n^+| = |J_n^-|$ if $p = q = 3 \bmod 4$ (i.e., n is a so-called Blum integer).

An integer z is said to be *regular* if we have $|J_z^+| = |J_z^-|$. A regular integer is said to be *k-regular*, for $k \geq 1$, if it is the product of k distinct primes. We denote by $R(k)$ the set of k-regular integers. The previous question shows that all Blum integers are 2-regular.

Let $L_{2,\overline{\mathrm{QR}}}$ denote the set

$$\left\{(n, a) \in \mathbb{Z}_{\geq 0}^2 \colon n \in R(2) \wedge a \in J_n^+ \wedge a \notin \mathrm{QR}_n\right\}.$$

Deciding whether a pair (n, a) is in this language is not a trivial task as a standard computational assumption in cryptography is precisely if n is a Blum integer, then it is hard to distinguish quadratic residues (modulo n) from non-quadratic residues with Jacobi symbol 1.

Let $(n, a) \in L_{2,\overline{\mathrm{QR}}}$.

b) Show that if $r \in J_n^+$, then either r or ar is a quadratic residue modulo n.

This observation suggests the following non-interactive proof system for $L_{2,\overline{\mathrm{QR}}}$.

- The prover and the verifier are given as input a pair $(n, a) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_n^*$ (set $\lambda := \lfloor \log n \rfloor + 1$) as well as a uniformly random λ^3-bit reference string $r_1 r_2 \cdots r_{\lambda^2}$ with each r_i of length λ.
- For $i \in [\![\lambda^2]\!]$, if $r_i \in J_n^+$ (the bit string r_i is identified with the integer it represents), then the prover computes and sends a uniformly random value y_i such that $r_i = y_i^2 \bmod n$ or $ar_i = y_i^2 \bmod n$.

– Upon receiving the proof, the verifier proceeds as follows.
  1. If $r_i \in J_n^+$ for less than 3λ indices i then accept.
  2. If n is not odd or $a \notin J_n^+$ then reject.
  3. If n is a perfect square then reject.
  4. If n is a prime power then reject.
  5. If $r_i = y_i^2 \bmod n$ or $ar_i = y_i^2 \bmod n$ for each y_i received from the prover then accept, otherwise reject.

  To check whether n is a prime power, assuming the existence of a randomized (with a random tape of the same length as the input tape) primality-test algorithm $\mathsf{PrimeTest}$ with perfect correctness and soundness error $3/8$[1], the verifier can proceed as follows.
  1. Compute the largest integer α such that $n = m^\alpha$ for some positive integer m. The verifier need only loop over the value $\{1, \ldots, \lfloor \log n \rfloor + 1\}$ for α, and do a binary search to find m, should it exist.
  2. Let z be such that $z^\alpha = n$.
  3. If $\mathsf{PrimeTest}(z; r_i) = 1$ for all $i \in [\![\lambda^2]\!]$, reject.

c) Show that the protocol has negligible (in λ) completeness error.

d) What is the probability that the last check from the verifier succeeds if n is 2-regular but $a \in \mathrm{QR}_n$?

e) Show that an odd integer is regular if and only if it is *not* a perfect square.

f) What is the probability that the third check of the verifier succeeds if n is not regular?

g) Consider a binary relation $\sim$ over $\mathbb{Z}_n^*$ defined as $a_1 \sim a_2$ if and only if $a_1 a_2 \in \mathrm{QR}_n$. Show that it is an equivalence relation.

h) Show that an odd integer n is k-regular for $k \geq 1$ if and only if it is regular and $\mathbb{Z}_n^*$ is partitioned in 2^k $\sim$ equivalence classes of the same cardinality.

i) What is the probability that the fourth check of the verifier succeeds if n is 1-regular?

j) For any fixed (n, a) such that n is k-regular for $k \geq 3$, show that for each $r_i \in J_n^+$, r_i or ar_i is in QR_n with probability at most $1/2$.

k) Show that the last check of the verifier succeeds with probability at most $2^{-\lambda}$ if n is k-regular for $k \geq 3$.

l) Conclude that the proof has negligible soundness error.

m) Show that the proof is zero-knowledge by designing a polynomial-time simulator that computes a common-reference string (after getting the instance as input) with the same distribution as in the proof system and can thereby compute proofs with the same distribution as those of the prover.

[1] That is, the probability that it declares a composite number to be prime is at most $3/8$.