Notes for Lecture 25 (draft)

Summary

Today we show that the graph isomorphism protocol we defined last time is indeed a zero-knowledge protocol. Then we discuss the *quadratic residuosity problem* modulo a composite, and define a protocol for proving quadratic residuosity. (We shall prove that the protocol is zero knowledge next time.)

1 The Graph Isomorphism Protocol

Last time we considered the following protocol for the graph isomorphism protocol.

- Verifier's input: two graphs $G_1 = (V, E_1)$, $G_2 = (V, E_2)$;
- Prover's input: G_1, G_2 and permutation π^* such that $\pi^*(G_1) = G_2$; the prover wants to convince the verifier that the graphs are isomorphic
- The prover picks a random permutation $\pi_R : V \to V$ and sends the graph $G := \pi_R(G_2)$
- The verifier picks at random $b \in \{1, 2\}$ and sends b to the prover
- The prover sends back π_R if $b = 2$, and $\pi_R(\pi^*(\cdot))$ otherwise
- The verifier cheks that the permutation π received at the previous round is such that $\pi(G_b) = G$, and accepts if so.

In order to prove that this protocol is zero knowledge, we to show the existence of an efficient simulator.

Theorem 1 *For every verifier algorithm V^* of complexity t there is a simulator algorithm S^* of expected complexity $\leq 2t + O(n^2)$ such that, for every two isomorphic graphs G_1, G_2, and for every isomorphism π between them, the distributions of transcripts*

$$P(\pi, G_1, G_2) \leftrightarrow V^*(G_1, G_2) \tag{1}$$

and

$$S^*(G_1, G_2) \tag{2}$$

are identical.

2 The Quadratic Residuosity Problem

We review some basic facts about quadratic residuosity modulo a composite.

If $N = p \cdot q$ is the product of two distinct odd primes, and $\mathbb{Z}_N^*$ is the set of all numbers in $\{1, \ldots, N-1\}$ having no common factor with N, then we have the following easy consequences of the Chinese remainder theorem:

- $\mathbb{Z}_N^*$ has $(p-1) \cdot (q-1)$ elements, and is a group with respect to multiplications;
- If $r = x^2 \bmod N$ is a quadratic residue, and is an element of $\mathbb{Z}_N^*$, then it has exactly 4 square roots in $\mathbb{Z}_N^*$
- Precisely $(p-1) \cdot (q-1)/4$ elements of $\mathbb{Z}_N^*$ are quadratic residues
- Knowing the factorization of N, there is an efficient algorithm to check if a given $y \in \mathbb{Z}_N^*$ is a quadratic residue and, if so, to find a square root.

It is, however, believed to be hard to find square roots and to check residuosity modulo N if the factorization of N is not known.

Indeed, we can show that from any algorithm that is able to find square roots efficiently mod N we can derive an algorithm that factors N efficiently

3 The Quadratic Residuosity Protocol

We consider the following protocol for proving quadratic residuosity.

- Verifier's input: an integer N (product of two unknown odd primes) and a integer $r \in \mathbb{Z}_N^*$;
- Prover's input: N, r and a square root $x \in Z_N^*$ such that $x^2 \bmod N = r$.
- The prover picks a random $y \in Z_N^*$ and sends $a := y^2 \bmod N$ to the verifier
- The verifier picks at random $b \in \{0, 1\}$ and sends b to the prover
- The prover sends back $c := y$ if $b = 0$ or $c := y \cdot x \bmod N$ if $b = 1$
- The verifier cheks that $c^2 \bmod N = a$ if $b = 0$ or that $c^2 \equiv a \cdot r \pmod N$ if $b = 1$, and accepts if so.

We show that:

- If r is a quadratic residue, the prover is given a square root x, and the parties follow the protocol, then the verifier accepts with probability 1;
- If r is not a quadratic residue, then for every cheating prover strategy P^*, the verifier rejects with probability $\geq 1/2$.

Next time we shall prove that the protocol is zero knowledge.