CS 600.442 – Modern Cryptography November 9, 2015

Lecture 21: NIZK - II

Instructor: Abhishek Jain *Scribe: Michael Shavit*

In the previous lecture we showed how to construct an NIZK in the CRS model given an NIZK in the hidden bit model. We will now construct an NIZK in the hidden bit model.

1 Hamiltonian graph problem and notation

Definition 1 (Hamiltonian cycle) *A Hamiltonian cycle on a graph is a cycle that covers each vertex exactly once.*

Definition 2 (Hamiltonian Graph) *A Hamiltonian graph is a graph that contains a Hamiltonian cycle, that is a graph $G = (V, E)$ st $|v| = n$ is Hamiltonian iff $\exists$ a labeling $(x_1, ..., x_n)$ st $(x_i, x_{i+1}) \in E$.$\forall i \in [n]$.*

Remark 1 *The Hamiltonian Graph problem is NP-Complete.*
The set of edges of a Hamiltonian cycle is a sufficient witness for a Hamiltonian Graph.

Since the Hamiltonian graph problem is in NP-Complete, constructing an NIZK proof system for that problem is sufficient for constructing an NIZK proof system for all problems in NP.

Definition 3 (Adjacency matrix) *A graph $G = (V, E)$ with $|v| = n$ can be represented as a $N \times N$ adjacency matrix M_G of boolean values s.t $M_G(i, j) = 1$ iff $(i, j) \in E$.*

Definition 4 (Cycle matrix) *A cycle matrix is a matrix that corresponds to a graph $G = (V, E)$ that contains a Hamiltonian cycle and no edges outside the cycle's edges. In other words $\exists$ a labeling $(x_1, ..., x_n)$ st $M_G(x_i, x_j) = 1$ iff $i = j - 1(mod n)$ or $i = j + 1(mod n)$.*

Definition 5 (Permutation matrix) *A permutation matrix is a boolean matrix s.t each row and each column has exactly one entry equal to 1.*

2 NIZK proof system construction

Theorem 1 *There exists a NIZK proof system for the Hamiltonian graph problem in the Hidden Bit model (which requires no cryptographic assumption).*

Construction. Let r be the hidden random string and suppose that r represents an $N \times N$ cycle matrix M_c.
Let $G = (V, E)$ be the shared input with a Hamiltonian cycle $(x_1, ..., x_n)$ known to the prover P.

1. P can choose a random mapping $\phi : V \to \{1, ..., n\}$ s.t $M_c[\phi(x_i), \phi(x_{i+1})] = 1 \, \forall$ edges (x_i, x_{i+1}) in G's Hamiltonian cycle.

2. P sends (ϕ, I) to the verifier where $I = \{(\phi(u), \phi(v)) : (u, v) \in V \times V \setminus E\}$.

3. r's bits that correspond to the entries $M_c[a, b]$ st $(a, b) \in I$ are revealed to the verifier. The verifier accepts the proof iff $M_c[\phi(u), \phi(v)] = 0 \; \forall (u, v) \in V \times V \setminus E$.

Proof.

Completeness: By construction M_c is a cycle matrix st $M_c[\phi(u), \phi(v)] = 1$ iff (u, v) is an edge in P's Hamiltonian cycle, thus only if $(u, v) \in E$. Therefore $M_c[\phi(u), \phi(v)] = 0 \; \forall (u, v) \in V \times V \setminus E$.

Soundness: Note that $\forall M_c[\phi(u), \phi(v)]$ equal to 1 then $(u, v) \in E$ or else the proof is rejected. Furthermore note that if there exists a mapping ϕ s.t $(u, v) \in E \; \forall M_c[\phi(u), \phi(v)]$ equal to 1 then the graph G is a Hamiltonian graph. Indeed the edges (u, v) which map to 1 entries in the cycle graph are precisely the edges of a Hamiltonian cycle.
Thus if G is not a Hamiltonian graph then there doesn't exist such a mapping. Given a non Hamiltonian graph G, for any mapping ϕ, $\exists (u, v) \notin E$ s.t $M_c[\phi(u), \phi(v)] = 1$ and the proof would get rejected.

Zero knowledge: Briefly: we can build a simulator that chooses an arbitrary permutation ϕ and reveals only 0s in the random string (recall that the simulator can control the random string). Recall that for the honest prover, ϕ is a random mapping onto a random cycle graph (that is hidden) and is thus indistinguishable from a random permutation.

■

3 Distribution of the random string r

In the previous section, the proof assumed that r represents an $N \times N$ cycle matrix M_c.
We now consider how one can sample cycle matrices from $R \overset{\$}{\leftarrow} \{0, 1\}^*$.

Construction. Let R be a random string of length $l = (3 * \log_2 n) * n^4$.
Intuitively this string can be though of as n^4 blocks, each of length $3 * \log_2 n$.
Given R, we can generate a string R' of length n^4 s.t $R'_i = 1$ iff $chunk_i(R) = 1^{3 * \log_2 n}$, where $chunk_i(R)$ is the i^{th} chunk of length $3 * \log_2 n$ in R.

Lemma 2 *$P[R'_i = 1] \approx 1/n^3$ for any R'_i. The proof for this lemma is left as an exercise to the reader.*

Let R' represent a matrix M of size $n^2 * n^2$. We can establish a cycle matrix of size $n * n$ in the following fashion:

1. Establish that M has exactly n 1s. Fail otherwise.

   Lemma 3 *This step succeeds with probability $p \approx \theta(1/n)$. The proof for this lemma is left as an exercise to the reader.*

2. Establish that the n 1s occur in different rows and collumns, i.e no row or column contains more than a single 1 entry, i.e the matrix contains a permutation sub-matrix of size $n * n$. Fail otherwise.

   Lemma 4 *This step succeeds with probability $p > 1/n$. The proof for this lemma is left as an exercise to the reader.*

3. Establish that the permutation sub-matrix is a Hamiltonian cycle.

   Lemma 5 *This step succeeds with probability $p = 1/n$.*
   Indeed observe that there are $n!$ possible permutation matrices of size $n*n$ and $(n-1)!$ possible cycle matrices of size $n * n$. A random $n * n$ permutation matrix is thus a cycle matrix with probability $p = (n-1)!/n! = 1/n$.

The construction above thus succeeds with probability $p \approx (1/n) * (1/n) * (1/n) = 1/n^3$. Using amplification n^4 times, we obtain P["At least one trial yields a cycle matrix"] $= 1 - (1 - 1/n^3)^{n^4} \approx 1 - e^{-n}$.

4 Modified NIZK proof given a string $R \overset{\$}{\leftarrow} \{0,1\}^*$

Given R, let $M_1, ..., M_L$ be $L = n^4$ matrices of size $n^2 * n^2$ (each built per the previous construction). $\forall i \in [L]$:

1. The prover checks if M_i contains a cycle sub-matrix. If not then the prover reveals M_i. Otherwise the prover sends the NIZK proof using the cycle sub-matrix, revealing the remaining $n^4 - n^2$ bits in M_i that are not part of that cycle sub-matrix. By construction those $n^4 - n^2$ bits are all 0s.

2. If M_i is completely revealed, the verifier must check that M_i indeed does not contain a cycle graph.
   For partially revealed M_is, the verifier checks that the initial $n^4 - n^2$ bits revealed are 0. The verifier then verifies the proof received assuming the remaining portion of M_i is the cycle matrix M_c.

Since at least one of the M_i contains a cycle sub-matrix, then at least of the proofs sent must have been conducted with a cycle matrix M_c as desired, thus providing soundness. Completeness and Zero knowledge naturally flow from that of section 2.