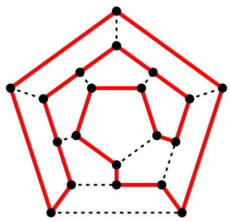
Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2021

Prof. Christian Cachin
Jovana Mićić

Exercise 5

5.1 Proving in zero-knowledge that a graph has a Hamiltonian cycle (4pt)

A *Hamiltonian cycle* in a graph $G = (V, E)$ is a closed path that contains every vertex exactly once. Deciding whether a graph on n vertices has a Hamiltonian path is NP-complete; finding such a cycle is difficult. Here is a Hamiltonian cycle in the edge graph of a Dodecahedron[1]:



In this problem, we develop a zero-knowledge proof for a prover P to convince a verifier V that a given graph G has a Hamiltonian cycle C, without giving away more information. We write $C \subset V$, i.e., the cycle is represented by a set of vertices.

Recall the zero-knowledge proof protocol for graph isomorphism (GI): The first message sent by P (the so-called commitment) was a randomly chosen graph H, isomorphic to the two graphs given for GI. It would be appealing to reuse this idea, but this does not work here because P would have to reveal too much of the mapping from G to H.

Consider the following protocol (due to Blum):

1. P chooses a random permutation π of V, computes $H = (V, F) = \pi(G)$, i.e., a random permutation of G, and $D = \pi(C)$. Notice that D is a Hamiltonian cycle in H. Then P obtains a list of commitments:

   i. a commitment to π, i.e., $c_\pi = \mathsf{Com}(\pi, r_\pi)$;

   i. for every pair $v, w \in V$, a commitment to whether an edge (v, w) exists in H, i.e.,

   $$c_{v,w} = \begin{cases} \mathsf{Com}(0, r_{v,w}) & \text{if} (v, w) \notin F \\ \mathsf{Com}(1, r_{v,w}) & \text{if} (v, w) \in F \end{cases}$$

   P sends c_π and $\{c_{v,w}\}$ for $v, w \in V$ to V.

2. V flips a coin, i.e., chooses a random bit $b \overset{R}{\leftarrow} \{0, 1\}$, sends b to P.

3. If $b = 0$, then P shows the correspondence between G and H by sending π and the openings of all commitments; if $b = 1$, then P shows that H contains a Hamiltonian cycle by sending D and the opening of the commitments for all edges (v, w) in D.

4. If $b = 0$, then V verifies that all commitments have been opened correctly and that $H = \pi(G)$; if $b = 1$, then V checks that the openings of all commitments for D are 1 (thus, D is a Hamiltonian cycle in H).

Show that this protocol satisfies the completeness, soundness, and zero-knowledge properties.

[1] Wikipedia, CC BY-SA 3.0, `https://en.wikipedia.org/wiki/Hamiltonian_path`

5.2 Proving knowledge of an RSA-inverse (6pt)

A third party T generates and publishes an RSA public key (N, e) and keeps the corresponding secret key d for itself. A party P registers with T and receives from T value $h \in \mathbb{Z}_N$ and an RSA pre-image w of h, i.e., a number $w \in \mathbb{Z}_N$ such that

$$w^e \equiv h \pmod{N}.$$

Later, P may prove to a verifier V that it knows an e-th root of h modulo N using the following zero-knowledge proof of knowledge (due to Guillou and Quisquater):

1. P picks $r \stackrel{R}{\leftarrow} \mathbb{Z}_N$ randomly, computes the commitment $t \leftarrow r^e \textbf{ mod } N$, and sends t to V.
2. V stores t, selects the challenge $c \stackrel{R}{\leftarrow} \mathbb{Z}_e$ at random, and sends c to V.
3. P computes its response $s \leftarrow rw^c \textbf{ mod } N$ and sends s to V.
4. V checks if $s^e \stackrel{?}{\equiv} t \cdot h^c \pmod{N}$ and that $\gcd(t, N) \stackrel{?}{=} 1$.

The verifier has obtained the value h from T beforehand and associated it with an identity P. Whenever an entity completes a proof of knowledge for an RSA-inverse of h successfully, the verifier considers this entity as authenticated for P.

Show that this protocol is a (honest-verifier) zero-knowledge proof of knowledge.

For the soundness property, describe a knowledge extractor E that is given two transcripts (t, c, s) and (t, c', s'). Exploit the fact that since e is prime, $\gcd(e, c - c') = 1$ and therefore there are integers σ and τ (the Bézout coefficients) such that

$$\sigma e + \tau(c - c') = 1.$$