TD 1 Advanced cryptography

Léo Colisson Palais

Exercice 1: Exercises from the course

Do the exercises from the course, notably:

- Show that the Fiat-Shamir transform is not secure when we hash commitments one by one, i.e. the i-th challenge is obtained from the i-th commitment.
- Show that there exists a ZK protocol that is secure when applied sequentially but not in parallel (see hint from the course).

Exercice 2: Practicality of ZK proofs based on the Hamiltonian path problem

Alice wants to prove to Bob that she knows the preimage of a given y by the hash function $\mathsf{SHA256}$. For this, she plans to use the ZK protocol based on he Hamiltonian path problem, but she first wants to estimate how realistic this is.

1. As a first step, Alice wants to estimate the number of variables n_v and clauses $n_c = n_{c,1} + n_{c,2} + n_{c,3}$ (where $n_{c,i}$ is the number of clauses involving i literals) needed to encode in a SAT instance a circuit with $n_\wedge$ AND gates, $n_\vee$ OR gates, and $n_\neg$ NOT gates.
   (a) Recall briefly how to convert a circuit to a SAT instance. How many variables do you have for a circuit with n_{in} input bits and g gates?
   (b) Show that:
      - adding a NOT gate adds 2 clauses involving 2 variables each,
      - adding an AND or OR gate adds 3 clauses, 2 of them involving 2 variables each, and one involving 3 variables.

   (c) Express $n_{c,1}$, $n_{c,2}$, $n_{c,3}$ and n_v in function of n_{in}, $n_\wedge$, $n_\vee$, and $n_\neg$.
   (d) Alice finds in `http://stevengoldfeder.com/projects/circuits/sha2circuit.html` a circuit to compute $\mathsf{SHA256}$ (256 output bits), on inputs of size 512, involving 22 272 AND gates, 91 780 XOR gates, and 2 194 NOT gates. Compute $n_{c,1}$, $n_{c,2}$, $n_{c,3}$ and n_v based on these numbers.
2. In a second step, Alice needs to compute the size of the directed graph G encoding the SAT instance as a problem of Hamiltonian path finding. How many nodes n_n and edges n_e are contained in the graph? (Express this both analytically and compute it for the case of $\mathsf{SHA256}$, and do the same in all follow up questions.)
3. Alice wants to prove that she knows a Hamiltonian path in G in a ZK way. Based on the protocol seen in the course (involving commitments of all entries of the adjacency matrix of G), what is the number of commitments that Alice needs to send to Bob? If she commits with $\mathsf{SHA256}$ (having 256 output bits), how large is the message sent to Bob for one round of communication?
4. How many rounds do you need to run to obtain a probability of cheating for Alice of $1/10^9$?
5. Since the graph G is mostly sparse, can you propose a better solution than committing to the whole adjacency matrix? Is this safe irrespective of the ordering of the new message? How large is the message sent from Alice to Bob with this optimized version?
6. How can you make this protocol non-interactive, so that Alice sends a single message to Bob? What is the size of the resulting message?

Exercice 3: Schnorr's signature

- Prove that Schnorr's signature is not secure if the nonce (r in the course) of the prover is used more than once.
- We saw (previous exercise) that the Fiat-Shamir transform is not secure when the hash is applied on each round separately. Yet, Schnorr's signature can be seen s a Fiat-Shamir on a single round, i.e. it coincides with the case where the Fiat Shamir transform is applied on each round separately. Why can't you apply the same attack here?
- Prove (if not done in the course) that the Schnorr's signature is a secure ZK proof (sound and ZK).
- Prove that it is a proof of knowledge (ZKPoK) protocol.

Exercice 4

ZK proofs of graph coloring Alice wants to prove, in a ZK way, that she knows the 3-coloring of a graph (an assignment of one color amount 3 for each vertex, such that no neighboring vertices have the same color).

1. Alice comes up with the idea of the following protocol:

   (a) First, Alice sends for each vertex a commit of its color (Bob knows the mapping vertex $\leftrightarrow$ commit).

   (b) Then, Bob challenges Alice to reveal the colors of one random edge in the graph.

   (c) Alice open the commitments of the two vertices on this edge and Bob checks they are different.

   Is this protocol correct? Sound? ZK? If not, show an explicit attacker against the ZK property.

2. Propose a fix to the above protocol, and show that it is correct, sound, and ZK.
3. Propose a naive "attack" against one round of your protocol, i.e. a method that allows Alice to pass the test without knowing a 3-coloring. What is the probability of cheating? How many rounds do you need to reduce the probability of attacking the scheme to 2^{-80}?

Exercice 5

ZK proof of graph isomorphism Alice wants to prove that she knows an isomorphism between two graphs G_0 and G_1 without revealing the isomorphism. Can you find such a protocol? Prove that it is a ZK proof of knowledge.

Hint: consider a third graph G' isomorph to both G and G'.