Prof. Dr. Johannes Blömer
Nils Löken

June 14th, 2017
submission due: July 25th, 2017: 11 a.m.

Cryptographic Protocols

SS 2017

Handout 5

Exercises marked (*) will be checked by tutors.
We encourage submissions of solutions by small groups of up to four students.

Exercise 1:
Consider the Guillous-Quisquater identification protocol
Parameters: Choose RSA modulus $N := p \cdot q$ and some prime $e \in \mathbb{Z}^*_{\phi(N)}$. Chose private key $x \leftarrow \mathbb{Z}^*_N$. The corresponding public key is $(N, e, X = x^e \mod N)$.
Protocol: To prove her identity to V, the prover P runs the following protocol:

$P\,(N, e, x)$		$V\,(N, e, X)$
choose $r \leftarrow \mathbb{Z}^*_N$		
compute $R := r^e \mod N$		
	$\xrightarrow{R}$	
		choose $f \leftarrow \mathbb{Z}_e$
	$\xleftarrow{f}$	
compute $y := r \cdot x^f \mod N$		
	$\xrightarrow{y}$	
		compute $Y := y^e \mod N$
		accepts iff $Y = R \cdot X^f \mod N$

We know that this protocol is correct, a special honest-verifier zero-knowledge proof of knowledge, and has the special soundness property.

a) Transform the GQ identification protocol to into a signature scheme: Employ the Fiat-Shamir heuristic in your construction to get rid of the interaction.

b) Prove the correctness of your construction.

Exercise 2:
Consider the Fiat-Shamir identification protocol. Show that the protocol is witness indistinguishable and witness hiding. Provide an adequate assumption for your proof.

Exercise 3 (4 points)**:**
(*) Consider relation R_{GI} with $R_{\text{GI}}((G_1, G_2), (\pi_1, \pi_2)) = 1 \Leftrightarrow \pi_1(G_1) = \pi_2(G_2)$, where $G_1 = (V, E), G_2 = (V, E')$ are graphs, $\pi_1, \pi_2 \in S_{|V|}$ are permutations and $\pi_1(G_1) = \pi_2(G_2)$ holds if and only if for all nodes $u, v \in V$ we have $\{u, v\} \in E \Leftrightarrow \{\pi_1(\pi_2^{-1}(u)), \pi_1(\pi_2^{-1}(v))\} \in E'$.
Protocol: A prover P proves knowledge of witness (π_1, π_2) for (G_1, G_2) to verifier V by running the following protocol:

$P\,(G_1, G_2, \pi_1, \pi_2)$		$V\,(G_1, G_2)$
$\pi_c \leftarrow S_{\lvert V\rvert}$		
$G := \pi_1(G_1)$		
$H := \pi_c(G)$		
	$\xrightarrow{H}$	
		$b \leftarrow \{1, 2\}$
	$\xleftarrow{b}$	
$\pi_r := \pi_c \circ \pi_b$		
	$\xrightarrow{\pi_r}$	
		accepts iff $\pi_r(G_b) = H$

Prove, that this protocol is witness indistinguishable.

Hint: Assume that the automorphism groups of all relevant graphs only contain the identity, i. e. for graph G and permutation π $\pi(G) = G$ implies $\pi = 1_{S_{|V|}}$.

For an example of a graph that does not have such a trivial automorphism group, consider the graph $G = (V, E)$ with $V = \{1, 2, 3, 4, 5\}$, $E = \{\{3, 4\}, \{4, 5\}\}$. The automorphism group of G contains four permutations: nodes 1 and 2, as well as 3 and 5 can be exchanged with without changing the graph.

Exercise 4 (4 points)**:**
(*) Consider the following attempt to an AND-composition of two instances of Schnorr's identification protocol.
Parameters: On input 1^l choose primes p, q such that $q|p-1$ and $q > 2^l$, choose generator $z \in \mathbb{Z}_p^*$ and set $g := z^{(p-1)/q}$, choose a private key $sk := (x_1, x_2) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q$ and set public key $pk = (p, q, g, Y_1 = g^{x_1} \mod p, Y_2 = g^{x_2} \mod p)$.
Protocol: Prover P proves her identity to verifier V by running the the following protocol:

$P\,(sk)$		$V\,(pk)$
choose $k \leftarrow \mathbb{Z}_q$		
compute $a := g^k \mod p$		
	$\xrightarrow{a}$	
		choose $c \leftarrow \{1, \ldots, 2^l\}$
	$\xleftarrow{c}$	
compute $r := k - c \cdot x_1 - c^2 \cdot x_2 \mod q$		
	$\xrightarrow{r}$	
		accepts iff $a = g^r \cdot Y_1^c \cdot Y_2^{c^2} \mod p$

- Show that this protocol is complete and special honest verifier zero knowledge.
- Explain why special soundness does not hold for this protocol.

  Hint: consider an prover who knows x_1 but not x_2.

- Show that x_1, x_2 can be recovered from *three* transcripts $(a, c, r), (a, c', r'), (a, c'', r'')$ with $c \neq c', c \neq c'', c' \neq c''$.

Exercise 5 (4 points)**:**
(*) Design a protocol for the AND-composition of two instances of Schnorr's identification protocol, i. e. a Σ-protocol that proves knowledge of discrete logarithms $x_1, x_2 \in \mathbb{Z}_q$ for public values $g^{x_1} \mod p, h^{x_2} \mod p$ with $g, h \in \mathbb{Z}_p^*, g \neq h$.

Prove that your protocol is complete, special honest verifier zero-knowledge and has the special soundness property.