Prof. Dr. Johannes Blömer
Nils Löken, Fabian Eidens

July 5th, 2016
submission due: July 12th, 2016: 11 a.m.

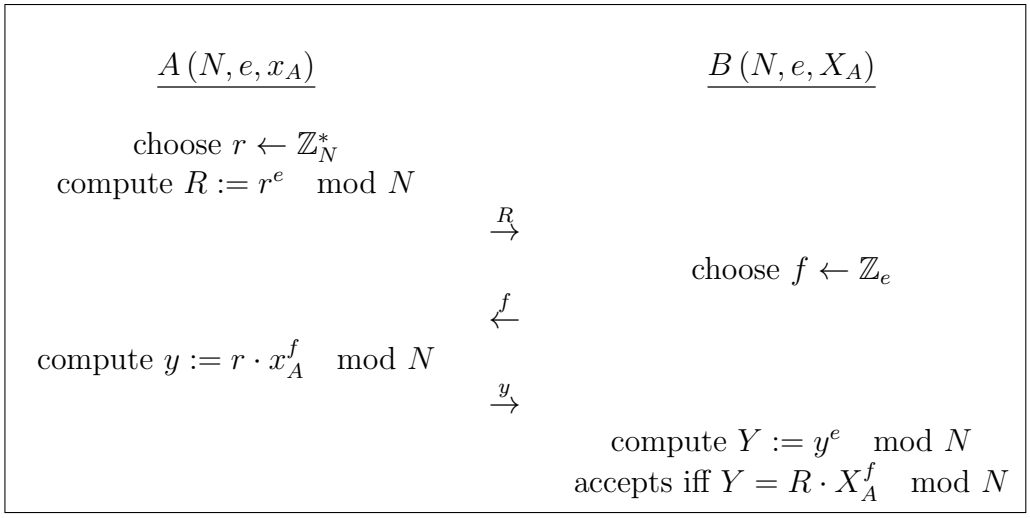
Cryptographic Protocols

SS 2016

Handout 5

Exercises marked (*) or (**) 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 (GQ-Ident) protocol
System parameters: A trusted authority (TA) chooses RSA parameters $N := p \cdot q$ and some $e \in \mathbb{Z}^*_{\phi(N)}$. The parameters (N, e) are published to all participants.
User parameters: User A chooses a private $x_A \leftarrow \mathbb{Z}^*_N$. Her public key is $X_A := x_A^e \mod N$. (Furthermore, the TA issues a certificate that X_A really is the public key of A.)
Protocol: To prove the identity to B, the user A runs the following protocol:



(Furthermore, before starting the actual protocol, A sends X_A and the certificate issued by the TA to B. They only proceed if B's verification of this certificate is successful.)
About this protocol we know:

- *Completeness:* An honest verifier B will always accept an honest interaction with an honest prover A.
- *Special soundness:* There is a probabilistic polynomial time algorithm, called *extractor*, which, given a user's public key pk and two transcripts (R, f, y), (R, f', y') with $f \neq f'$ of accepting protocol executions, computes the secret key corresponding to pk.
- *Special honest verifier zero knowledgeness:* there is a probabilistic polynomial time algorithm, called *simulator*, which, given a user's public key pk and a verifier's challenge f produces transcripts (R, f, y) with the same probability distributions as transcripts

of protocol executions between honest provers and honest verifiers and with common input pk and challenge f, where the prover uses sk corresponding to pk. Additionally, the simulator, given challenge f and a value a that is not a public key that corresponds to any private key, computes transcripts of accepting protocol executions nonetheless.

Provide a proof of the special soundness property.

Exercise 2:
Consider the following attempt to create a parallel variant of Schnorr's identification protocol.
System parameters: A trusted authority (TA) on input 1^l chooses primes p, q such that $q|p-1$ and $q > 2^l$, chooses generator $z \in \mathbb{Z}_p^*$ and sets $g := z^{(p-1)/q}$.
User parameters: User A chooses a private sk $:= (x_{A,1}, x_{A,2}) \leftarrow \mathbb{Z}_q \times \mathbb{Z}_q$. Her public key is pk $:= (X_{A,1}, X_{A,2}) := (g^{x_{A,1}} \mod p, g^{x_{A,2}} \mod p)$. Furthermore, the TA issues a certificate that $(X_{A,1}, X_{A,2})$ really is the public key of A.
Protocol: To prove the identity to B, the user A runs the following protocol:

$A\,(p,q,g,\mathrm{sk})$		$B\,(p,q,g,\mathrm{pk})$
choose $k \leftarrow \mathbb{Z}_q$		
compute $x := g^k \mod p$		
	$\xrightarrow{x}$	
		choose $r \leftarrow \{1, \ldots, 2^l\}$
	$\xleftarrow{r}$	
compute $y := k - r \cdot x_{A,1} - r^2 \cdot x_{A,2} \mod q$		
	$\xrightarrow{y}$	
		accepts iff $x = g^y \cdot X_{A,1}^r \cdot X_{A,2}^{r^2} \mod p$

- 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 $x_{A,1}$ but not $x_{A,2}$.
- Show that $x_{A,1}, x_{A,2}$ can be recovered from *three* transcripts $(x, r, y), (x, r', y'), (x, r'', y'')$ with $r \neq r', r \neq r'', r' \neq r''$.

Exercise 3 (4 points)**:**
(**) Consider the GQ-Ident protocol from the first exercise. Give a protocol that is complete, special sound and special honest verifier zero knowledge and proves knowledge (AND-composition) of a pair of secret keys sk $= (x_{A,1}, x_{A,2})$ for the same parameters (N, e). Prove that your protocol has the required properties.

Exercise 4 (4 points)**:**
(**) Let V/P be an honest verifier zero knowledge protocol and let n be the length of the input to the prover. Consider $n = \mathrm{poly}(l)$ sequential executions of V/P. Show that the sequetial composition is still honest verifier zero knowledge.

Exercise 5:
Let L be a language from $\mathcal{P}$. Show that there is a zero knowledge protocol for L.