Prof. Dr. Johannes Blömer
Nils Löken

June 30th, 2017
submission due: July 11th, 2017: 11 a.m.

Cryptographic Protocols

SS 2017

Handout 3

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 (GQ) identification protocol which is based on RSA.
System parameters: Choose 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 $X_A := x_A^e \mod N$.
Protocol: To prove the identity to B, the user A runs the following protocol:

$A\,(N, e, x_A)$		$B\,(N, e, X_A)$
choose $r \leftarrow \mathbb{Z}^*_N$ compute $R := r^e \mod N$		
	$\xrightarrow{R}$	
		choose $f \leftarrow \mathbb{Z}_e$
	$\xleftarrow{f}$	
compute $y := r \cdot x_A^f \mod N$		
	$\xrightarrow{y}$	
		compute $Y := y^e \mod N$ accepts iff $Y = R \cdot X_A^f \mod N$

Show that the GQ-protocol from the previous exercise is a Σ-protocol for some relation P:

a) Give the relation P.

b) Correctness: Prove the protocol's completeness for P.

c) Special soundness: Present an extractor that, given two transcripts $(R, f, y), (R, f', y')$ with $f \neq f'$ computes x_a.

d) SHV-ZK: Present a simulator that generates transcripts of protocol executions for given public keys (N, e, X_A) and challenge f. Prove that the simulated transcripts are indistinguishable from transcripts of real protocol executions.

Exercise 2 (4 points)**:**
Consider the GQ-protocol from the previous exercise. Show that some party C can successfully impersonate A if she knows B's challenge f before the protocol starts.
Note that this implies the existence of a $1/e$-forger which guesses f and successfully impersonates A if the guess was correct.

Exercise 3 (4 points)**:**
(*) Consider the Fiat-Shamir identification protocol modified as follows.
System parameters: Choose RSA modulus $N := p \cdot q$. N is published to all participants.
User parameters: User A chooses a private $s_A \leftarrow \mathbb{Z}_N^*$. Her public key is $v_A := s_A^2 \mod N$.
Protocol: To prove the identity to B, the user A runs the following protocol:

$\underline{A\,(N, s_A)}$		$\underline{B\,(N, v_A)}$
choose $r \leftarrow \mathbb{Z}_N^*$, compute $r_1 := r^2 \mod N$ and $r_2 := 25 \cdot r^2 \mod N$		
	$\xrightarrow{r_1, r_2}$	
		choose $b_1, b_2 \leftarrow \{0, 1\}$
	$\xleftarrow{b_1, b_2}$	
compute $t_1 := r \cdot s_A^{b_1} \mod N$ and $t_2 := 5 \cdot r \cdot s_A^{b_2} \mod N$		
	$\xrightarrow{t_1, t_2}$	
		accepts iff $t_1^2 = r_1 \cdot v_A^{b_1} \mod N$ and $t_2^2 = r_2 \cdot v_A^{b_2} \mod N$

Show that:

a) Correctness: If both A and B are honest, B will accept A's identity.

b) After running this protocol B can compute the secret key of A efficiently if B chooses the bits b_1, b_2 appropriately.

Exercise 4 (4 points)**:**
(*) Consider the stateful signature scheme presented on Slide 3 of the respective slide set. Prove the scheme's existential unforgeability under chosen-message attacks:

a) Provide an appropriately modified definition of security against existential unforgeability under chosen-message attacks.

b) Prove the signature scheme's security in the security model from (a) based on the security of the underlying one-time signature scheme.

Hint: Consult a book on Part (a).