

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.

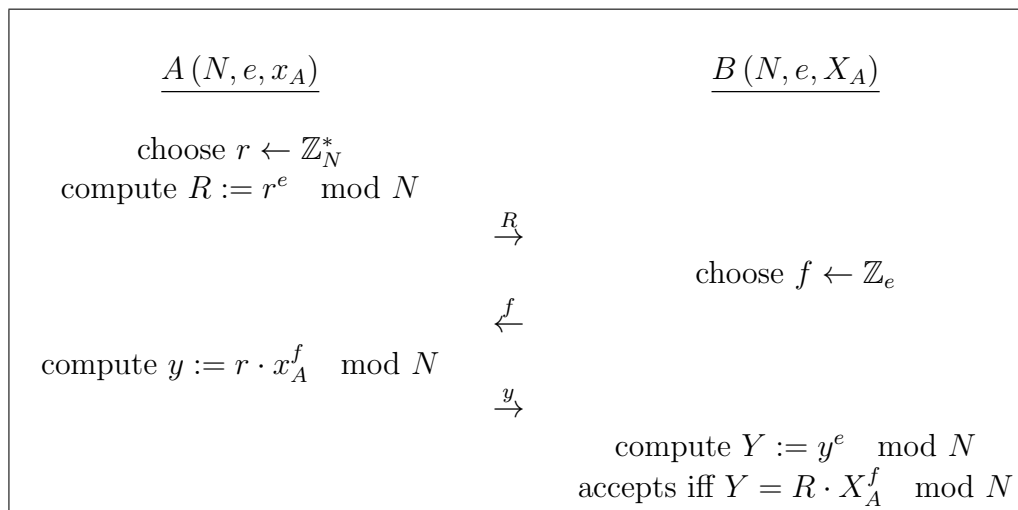
Exercise 1:

Consider the Guillou-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 $X_A := x_A^e \pmod N$.

Protocol: To prove the identity to B , the user A runs the following protocol:



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.

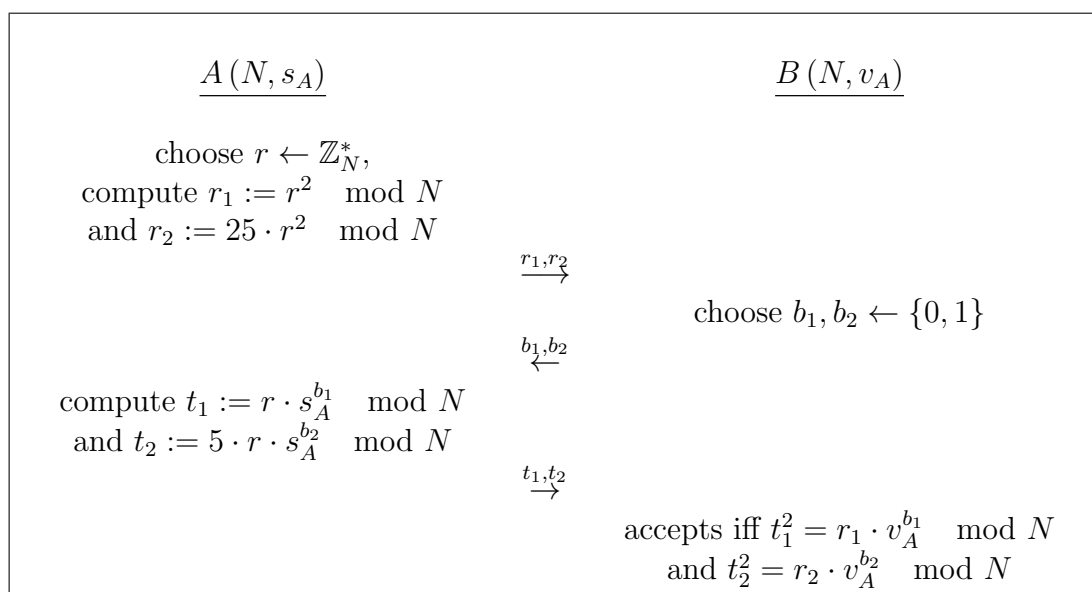
Exercise 3 (4 points):

(*) 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 $v_A := s_A^2 \pmod N$.

Protocol: To prove the identity to B , the user A runs the following protocol:



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).