Prof. Dr. Johannes Blömer
Nils Löken, Fabian Eidens

June 24th, 2016
submission due: July 5th, 2016: 11 a.m.

# Cryptographic Protocols

## SS 2016

## Handout 4

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

**Exercise 1** (4 points)**:**
(**) Consider the Guillous-Quisquater identification 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:

| $\underline{A\,(N, e, x_A)}$ | | $\underline{B\,(N, e, X_A)}$ |
|---|---|---|
| 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 $Y = R \cdot X_A^f \mod N$ |

(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:

- *Correctness:* 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.

Now, show that this protocol is *special honest verifier zero knowledge*, i. e. 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.

**Exercise 2:**
We apply the *Fiat-Shamir Heuristic*: Consider a signature scheme that is based on the Guillous-Quisquarter identification protocol. The signature scheme works as follows:

- $\mathrm{Gen}(1^n)$ computes RSA parameters $(N, e)$, and chooses $\mathrm{sk} \leftarrow \mathbb{Z}_N^*$ and $\mathrm{pk} = \mathrm{sk}^e$. params $:= (N, e)$ and pk) are published and sk is kept private. We assume a hash function $H : \{0,1\}^* \to \mathbb{Z}_e$ to be publicly known.
- $\mathrm{Sign}_{\mathrm{sk}}(m)$ picks $r \leftarrow \mathbb{Z}_N^*$. Let $R := r^e$, $f := H(R, m)$ and $y := r \cdot \mathrm{sk}^f \mod N$. Output $(f, y)$.
- $\mathrm{Vrfy}_{\mathrm{pk}}(m, \sigma)$ parses $\sigma = (f, y)$. It outputs 1 if $f = H(y^e \cdot \mathrm{pk}^{-f} \mod N, m)$ and 0 otherwise.

Show that

a) the signature scheme is correct.

b) if the hash function $H$ is modelled as a random oracle, then the signature scheme is existentially unforgeable under an adaptive chosen message attack.

Hint: The properties from Exercise 1 might help proving correctness and unforgeability.

**Exercise 3** (4 points)**:**
(**) An undirected graph $G = (V, E)$ consists of the set of $n$ vertices $V = \{1, \ldots, n\}$ and a set $E$ of unordered pairs $\{i, j\} \subseteq V$ called edges. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are called isomorphic if there exists a bijective mapping $\pi : V_1 \to V_2$ such that for every edge $\{i, j\} \in E_1$ we have that $\{\pi(i), \pi(j)\} \in E_2$ and for every edge $\{i, j\} \in E_2$ we have that $\{\pi^{-1}(i), \pi^{-1}(j)\} \in E_1$. In this case we write $G_1 = \pi(G_2)$ or $G_1 \simeq G_2$. Else they are non-isomorphic.
Let $G_1, G_2$ be two graphs. We consider the following two problems:

$$\mathrm{GI} := \{(G_1, G_2) | G_1 \simeq G_2\}$$

and

$$\mathrm{GNI} := \{(G_1, G_2) | G_1 \not\simeq G_2\}.$$

a) Which of the following pairs of graphs are in GI or in GNI? ($V_1 = V_2 = \{1, 2, 3, 4\}$)
   - $E_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$ and $E_2 = \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\}$
   - $E_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$ and $E_2 = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

b) Give a interactive proof system for GI (not necessarily zero-knowledge).

   Hint: The decision variant of GI is in $\mathcal{NP}$. Consequently, a powerful person can compute a witness that two graphs are isomorphic and everyone can verify this.

c) Give an interactive proof system for GNI.

Hint: Look at the protocol for QNR ("quadratic non-residues") from the lecture.

d) Give a (honest verifier) zero-knowledge interactive proof system for GI.

Hint: Recall the Fiat-Shamir protocol. It's a proof system for QR ("quadratic residues"). Furthermore, note that applying a random permutation to some graph gives you a random isomorphic graph.