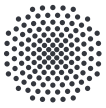

University of Stuttgart
Institute of
Information Security

Security and Privacy
Summer Term 2018
Prof. Dr. Ralf Küsters

Homework 3

Submission into the *red SEC mailbox* in front of Room 2.041 until June 19, 2018, 14:00.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants (see ILIAS for contact information).
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk losing points.

Remark

Some of the following tasks require you to prove properties of languages $L \subseteq \{0,1\}^*$ that are in $\mathcal{NP}$. Recall that the set $\mathcal{NP}$ is defined as follows:
$L \in \mathcal{NP} \Leftrightarrow \exists$ relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ that is decidable in polynomial time and $\exists$ polynomial q such that: $L = \{x : \exists\, w, |w| \leq q(|x|)$ and $(x,w) \in R\}$ (w is called a witness for $x \in L$).

Problem 1: Sum of negligible functions (4 points)

Show that the sum of two negligible functions ν and ν' is also a negligible function (see Slide Set 04, Slide 19).

Problem 2: Deterministic verifier in IPS (4 points)

Let $L \in \mathcal{IP}$. Show the following: If there is an interactive proof system (IPS) (P,V) with deterministic verifier V for the language L, then it holds true that $L \in \mathcal{NP}$.

Hint: First show that if there is an IPS (P,V) with a deterministic verifier V, then it is possible to convince V with a deterministic prover. Then show how one can construct a witness for $x \in L$ from the transcript of a conversation between such a deterministic prover and V. Don't forget to show that, in your construction, there are no witnesses for $x \notin L$!

Problem 3: Anonymous credentials and IPS (4 points)

Let $E(x,k,r)$ $(x \in X, k, r \in \{0,1\}^*)$ be a (symmetric) encryption scheme, i.e., E upon input of a plaintext x, key k, and randomness r outputs a ciphertext. We assume that E runs in polynomial time in $|x|$ and that $|x| \leq |E(x,\cdot,\cdot)|$.

In the following, we consider a setting where users have several credentials that can be used to get access to different services. For the sake of an example, we consider the credentials *name*, *age*, *residence*. Because a user wants to keep his credentials secret, he encrypts them with a secret key k. To be more precise, he encrypts the message $m =$ "Name: *name*, Age: *age*, Residence: *residence*" and obtains a ciphertext c (italic strings denote the actual values of the corresponding credentials).

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

Now consider a service that requires its users to be of age at least 18. In other words, upon input of some ciphertext c the service only allows access if c is in the following language:

$$L = \{c : \exists name, residence \in \{0,1\}^*, age \in \mathbb{N}, k, r \in \{0,1\}^* \text{ such that } E(m,k,r) = c \wedge age \geq 18\},$$

where m is defined as above.

1. Show: $L \in \mathcal{NP}$.
2. Give an IPS for L and prove its properties.

Hint: Note that your IPS does not have to be ZK, allowing for quite simple constructions.

Remark: By a result that we will show in the lecture, there also exists a ZK proof for this language because $L \in \mathcal{NP}$. Thus, using such a ZK proof, a user is able to prove that he is at least 18 years old without revealing any of his credentials (including the actual age)!

Problem 4: Equivalent definition of computational ZK (4 points)

Prove that if we replace the random variable $\{\langle P, V^* \rangle(x)\}_{x \in L}$ with the random variable $\{view^P_{V^*}(x)\}_{x \in L}$ in the definition of computational zero knowledge, then we obtain an equivalent definition.

Remark: Note that this requires you to show two directions: One the one hand, if we can simulate the view of V^*, then we can simulate the overall output of V^*. On the other hand, if we can simulate the overall output of V^*, we can also simulate the view of V^*.

Problem 5: Reducing the error probability 1 ★ (4 points) bonus

Let L be some language. In this task, we want to show that we can lower the probability of a verifier accepting an interactive proof for some $x \notin L$. For this purpose, show that the following two statements are equivalent:

(i) There is an interactive proof system (IPS) for L with completeness bound 1 and soundness bound $\frac{1}{3}$.

(ii) For every polynomial $p(\cdot)$ there is an IPS for L with completeness bound 1 and soundness bound $2^{-p(\cdot)}$ (i.e., $\forall x \notin L, \forall B$ connected to $V : \Pr[\langle B, V \rangle(x) = 1] \leq 2^{-p(|x|)}$).

Remark: It is also possible to show a stronger result where the completeness bound is arbitrary (instead of 1) as long as it is larger than the soundness bound.