University of Stuttgart
Institute of
Information Security

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

Homework 4

Submission into the *red SEC mailbox* in front of Room 2.041 until July 3, 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.

Problem 1: Transitivity of computational indistinguishability (4 points)

Let D_x, D'_x, and D''_x ($x \in L$ for some language L) be three probability distributions such that D_x is computationally indistinguishable from D'_x and D'_x is computationally indistinguishable from D''_x.

Show that D_x is also computationally indistinguishable from D''_x.

Problem 2: Check for $e = 0$ in the Fiat-Shamir identification protocol (4 points)

In this task we want to investigate why the verifier in the Fiat-Shamir identification protocol needs to check whether the commitment x was constructed in a suitable way, i.e., why the case $e = 0$ is necessary.

For this purpose, we consider a modified version of the protocol. Namely, we replace the verifier V with V' where V' behaves just as V except that it always sends the challenge $e = 1$. Show that (P, V') is not an IPS since the soundness property is not fulfilled. That is, provide an ITM B and an input $x \notin L$ such that $\langle B, V' \rangle (x)$ *always* accepts. Prove your statement.

Remark: Consider $x \notin L$ as used in Slide Set 04, Slide 39. We suggest using a small number for n to make it easier to show that a given element $v \in \mathbb{Z}_n^*$ is not a square.

Problem 3: Pedersen commitment scheme without randomness (4 points)

Let (Gen, com) be the Pedersen commitment scheme as defined in the lecture. In this task we consider a slight variation of this commitment scheme that drops the random element h^r.

More specifically, we define a new commitment algorithm com' as follows:

function $\text{COM'}((\mathcal{G}, q, g, h), v \in \mathbb{Z}_q)$
  return g^v
end function

Show that the commitment scheme (Gen, com') is computationally binding but not computationally hiding.

Hint: You do not have to perform a reduction to show the binding property. It holds unconditionally.

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

Problem 4: Schnorr's protocol - proof of knowledge (4 points)

In this problem we take a look at Schnorr's protocol for proving knowledge of the discrete logarithm. More precisely, the protocol works for the following $\mathcal{NP}$ relation and its induced language:

$$R_{DL} = \{((\mathcal{G}, q, g, h), w) \mid q \text{ prime},\ \mathcal{G} \text{ cyclic group},\ |\mathcal{G}| = q,\ g, h \in \mathcal{G},\ g \neq 1,\ g^w = h\}.$$

Now, let $t > 0$ be a fixed constant (which will be used to determine the length of the challenge from the verifier).

Schnorr's protocol for parameter t is defined as follows:

Common input: $(\mathcal{G}, q, g, h)$ where $q \geq 2^t$

P:

1. Compute $w \in \mathbb{Z}_q$ such that $g^w = h$
2. Choose $r \xleftarrow{\$} \mathbb{Z}_q$
3. Compute $a = g^r$
4. Send a
5. Receive e
6. Compute $z = r + e \cdot w \bmod q$
7. Send z

V:

1. Receive a
2. Choose $e \xleftarrow{\$} \{0,1\}^t$
3. Send e
4. Receive z
5. **if** $|\mathcal{G}| = q, q$ prime, $g, h \in \mathcal{G}, g \neq 1$, and $g^z = a \cdot h^e$ **then** output 1, **otherwise** output 0.

We note that Schnorr's protocol is an IPS (in particular, the language is decidable in polynomial time without knowing the witness, so V just checks membership of the language locally).

Your task is to show that Schnorr's protocol is a proof of knowledge with knowledge error $\kappa = \frac{1}{2^t}$.

Hints

- You can extract a witness similar to what we did in the Fiat-Shamir identification protocol. More precisely, as part of your proof you should show how you can compute a witness if you have accepting responses z_0, z_1 for different challenges e_0, e_1 but the same commitment x. Then use this to construct a good knowledge extractor.
- Note that, given some commitment x, there might be only very few challenges e that a prover can answer successfully (depending on the probability of convincing V).
- Note that t is a constant that is independent of the input. This might be useful for showing the runtime bound of your knowledge extractor.