Advanced Cryptography

Spring Semester 2021

Homework 3

- This homework contains one question: a variant of Σ protocols.
- You will submit a **report** that will contain all your answers and explanations. The report should be a PDF document. You can use any editor to prepare the report, but Latex is usually the best choice for typesetting math and pseudocode.
- We ask you to **work alone or in groups of 2**. No collaborations are allowed outside of the group you registered for HW1. Please contact the T.A. if you have a good reason to change group. Feel free to ask questions to the T.A.
- We might announce some typos for this homework on Moodle in the news forum. Everybody is subscribed to it and does receive an email as well. If you decided to ignore Moodle emails we recommend that you check the forum regularly.
- The homework is due on Moodle on Friday, 14$^{\text{th}}$ of May at 23h59. Please submit 1 report per group.

ADVSS($\mathcal{A}$)	STRSS($\mathcal{A}$)
$(x, w) \leftarrow\!\!\$\ \mathsf{Gen}(1^\lambda)$	$(x, w) \leftarrow\!\!\$\ \mathsf{Gen}(1^\lambda)$
$(a, e, e', z, z') \leftarrow \mathcal{A}(x)$	$(a, e, e', z, z') \leftarrow \mathcal{A}(x)$
return $e \neq e' \wedge V(x, a, e, z) \wedge V(x, a, e', z')$	**return** $(e, z) \neq (e', z') \wedge V(x, a, e, z) \wedge V(x, a, e', z')$

Figure 1: Adversarial special soundess and strong special soundness games.

1 A variant of Σ protocol

In this exercise, we will work with a variant of Σ protocols. First, recall that a Σ protocol must fulfills several properties like completeness, special Honest Verfier Zero-Knowledge (HVZK), special soundness, etc. (see slides 275-277). In addition, a Σ protocol is defined over a relation R defining a language $L = \{x : \exists w\ R(x, w)\}$. For this exercise, we assume we have in addition a randomized generating function $(x, w) \leftarrow\!\!\$\ \mathsf{Gen}(1^\lambda)$ that outputs x, w s.t. $R(x, w)$.

Definition 1 (Hard relation)**.** We say a relation R is hard if for any ppt adversary $\mathcal{A}$,

$$\Pr[\mathrm{HARD}(\mathcal{A}) \Rightarrow 1]$$

is negligible in λ, where HARD is the following game.

$$\begin{array}{l} \underline{\mathrm{HARD}(\mathcal{A})} \\ (x, w') \leftarrow\!\!\$\ \mathsf{Gen}(1^\lambda) \\ w \leftarrow \mathcal{A}(x) \\ \textbf{return } R(x, w) \end{array}$$

I.e. it is hard to find a witness w s.t. $R(x, w)$.

We also define a variant of special soundness that we call *adversarial special soundness.*

Definition 2 (Adversarial special soundess)**.** We consider the game on the left in Figure 1. A protocol (R, Gen, P, V) has adversarial special soundess if for any ppt adversary $\mathcal{A}$

$$\Pr[\mathrm{ADVSS}_\Sigma(\mathcal{A}) \Rightarrow \textbf{true}]$$

is negligible in λ.

Question 1. Show that a Σ protocol (which fulfills *special soundness*) over a hard relation also fulfills *adversarial special soundness.*

We consider the protocol in Figure 2, which we call Σ_{RSA}. Details about the parameters can be found in the legend.

Question 2. Show that Σ_{RSA} is a Σ protocol (except the HVZK and special soundness for now). Here is a list of what you need to show:

Prover		**Verifier**
input: $(N, t, \ell, X), x \in \mathbb{Z}_N^*$		**input:** (N, t, ℓ, X)
$r \leftarrow_{\$} \mathbb{Z}_N^*$		
$a \leftarrow r^t \bmod N$	$\xrightarrow{\quad a \quad}$	
	$\xleftarrow{\quad e \quad}$	$e \leftarrow_{\$} \{0, \ldots, 2^\ell - 1\}$
$z \leftarrow x^e r \bmod N$	$\xrightarrow{\quad z \quad}$	
		$z^t == aX^e \bmod N$

Figure 2: Σ_{RSA} protocol. N is a RSA modulus, t a prime s.t. $\gcd(t, \phi(N)) = 1$, ℓ s.t. $2^\ell < t$ and we work in $\mathbb{Z}_N^*$. The verifier checks that messages are in correct sets. We omit these checks in the figure.

1. Identify which parameters correspond to the *instance* and which correspond to the *witness.*
2. Define a relation (i.e. a language) R for this protocol. Σ_{RSA} should be an interactive proof of *knowledge of a plaintext corresponding to a RSA ciphertext (in $\mathbb{Z}_N^*$).*
3. Show that R, P, V are polynomially computable.
4. Prove the *correctness* property.
5. You do **not** have to provide a Gen algorithm for the language, but defining it might give you a clearer view of the protocol.

We now define a stronger variant of special soundness and HVZK, called *strong special soundness* and *strong HVZK*, respectively.

Definition 3 (Strong special Soundness)**.** We consider the game on the right in Figure 1. A Σ protocol (R, Gen, P, V) has adversarial special soundess if for any ppt adversary $\mathcal{A}$ the advantage

$$\mathsf{Adv}^{\text{strss}}_{\mathcal{A},\Sigma} := \Pr[\text{STRSS}_\Sigma(\mathcal{A}) \Rightarrow \textbf{true}]$$

is negligible in λ.

Note: The only difference between both special soundness notions defined in this exercise is the winning condition ($e \neq e'$ required in ADVSS and $(e, z) \neq (e', z')$ in STRSS).

Definition 4 (Strong HVZK)**.** A Σ protocol (R, Gen, P, V) is strongly HVZK if there exists a **deterministic** simulator StrSim s.t. the following simulator Sim is a (perfect-)HVZK simulator for Σ.

$\underline{\mathsf{Sim}(x)}$

$e \leftarrow_\$ \mathcal{E}$ // $\mathcal{E}$ is the domain of e's
$z \leftarrow_\$ \mathcal{Z}$ // $\mathcal{Z}$ is the domain of z's
$a \leftarrow \mathsf{StrSim}(x, e, z)$
return (a, e, z)

Here we say that Sim is a (perfect-)HVZK simulator if the transcript (a, e, z) of the execution $P \overset{x}{\leftrightarrow} V$ has the same distribution as $\mathsf{Sim}(x)$.

Question 3. Show that Σ_{RSA} fulfills *strong special soundness* if the RSA problem is hard. (We assume the RSA public-key in the RSA problem follows the same distribution as (N, t) in the protocol.)
Hint: First prove that Σ_{RSA} fulfills the *special soundness* notion of the course and then show that it fulfills *adversarial special soundness*. Conclude by showing that *adversarial special soundness* implies *strong special soundness* in this case. **Hint2:** Remember that if you have $\gcd(\alpha, \beta) = 1$, the extended gcd algorithm gives you a, b s.t. $a\alpha + b\beta = 1$.

Question 4. Show that Σ_{RSA} is *strong HVZK*.
Hint: Again, it might be easier to first prove that Σ_{RSA} fulfills special HVZK and then show that *strong* HVZK follows.

Definition 5 (2-inputs CR hash functions)**.** A family of 2-inputs hash functions is a tuple $\mathcal{H} = (\mathsf{Gen}, H)$, where $H(k, x_1, x_2)$ is a function parametrized by a key $k \leftarrow_\$ \mathsf{Gen}(1^\lambda)$ that hashes two inputs x_1, x_2. Such a family $\mathcal{H}$ is collision resistant if for all ppt adversary $\mathcal{A}$, the advantage

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A},\mathcal{H}} := \Pr[(x_1, x_2) \neq (x_1', x_2') \wedge H(x_1, x_2) = H(x_1', x_2') : (x_1, x_2, x_1', x_2') \leftarrow_\$ \mathcal{A}(k); k \leftarrow_\$ \mathsf{Gen}(1^\lambda)]$$

is negligible in λ.

Question 5. Show that one can construct a 2-inputs CR hash function family from **any** Σ protocol that is *strongly HVZK* **and** fulfills *strong special soundness*. That is, you should specify the Gen algorithm and the H function. Then, prove that for any $\mathcal{A}$ one can build $\mathcal{B}$ s.t.

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathcal{A},\mathcal{H}} \leq \mathsf{Adv}^{\mathrm{strss}}_{\mathcal{B},\Sigma} .$$

Question 6. Show that the Fiat-Shamir Σ protocol (slide 290) does not fulfill strong special soundness.
Hint: Given a valid transcript (a, e, z), it might be is easy to obtain a second valid transcript (a, e', z') s.t. $(e, z) \neq (e', z')$...

Question 7. Explain how you could modify the FS Σ protocol s.t. it has strong special soundness. Explain in a few sentences why your modified protocol fulfills *strong special soundness*.