# Advanced Cryptography

## Spring Semester 2021

## Homework 3

- This homework contains one question: a variant of $\Sigma$ 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 $\Sigma$ protocol

In this exercise, we will work with a variant of $\Sigma$ protocols. First, recall that a $\Sigma$ protocol must fulfills several properties like completeness, special Honest Verfier Zero-Knowledge (HVZK), special soundness, etc. (see slides 275-277). In addition, a $\Sigma$ 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 $\mathcal{A}$,

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

is negligible in $\lambda$, where HARD is the following game.

| HARD($\mathcal{A}$) |
|---|
| $(x, w') \leftarrow_\$ \mathsf{Gen}(1^\lambda)$ |
| $w \leftarrow \mathcal{A}(x)$ |
| **return** $R(x, w)$ |

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 $(R, \mathsf{Gen}, P, V)$ has adversarial special soundess if for any ppt adversary $\mathcal{A}$

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

is negligible in $\lambda$.

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

A $\Sigma$ protocol has an extractor $\mathsf{Ext}(x, a, e, z, e', z')$ that outputs $w$ s.t. $R(x, w)$ when $e \neq e' \wedge V(x, a, e, z) \wedge V(x, a, e', z')$. Thus, given a ADVSS adversary $\mathcal{A}$ one can construct a HARD adversary $\mathcal{B}$ s.t.

$$\mathsf{Adv}^{\text{advss}}_{\mathcal{A}} \leq \mathsf{Adv}^{\text{hard}}_{\mathcal{B}}$$

where $\mathcal{B}$ runs $(a, e, e', z, z') \leftarrow_\$ \mathcal{A}(x)$ and outputs $\mathsf{Ext}(a, e, z, e', z')$. Hence, if the relation is hard, the $\Sigma$ protocol fulfills *adversarial special soundness.*

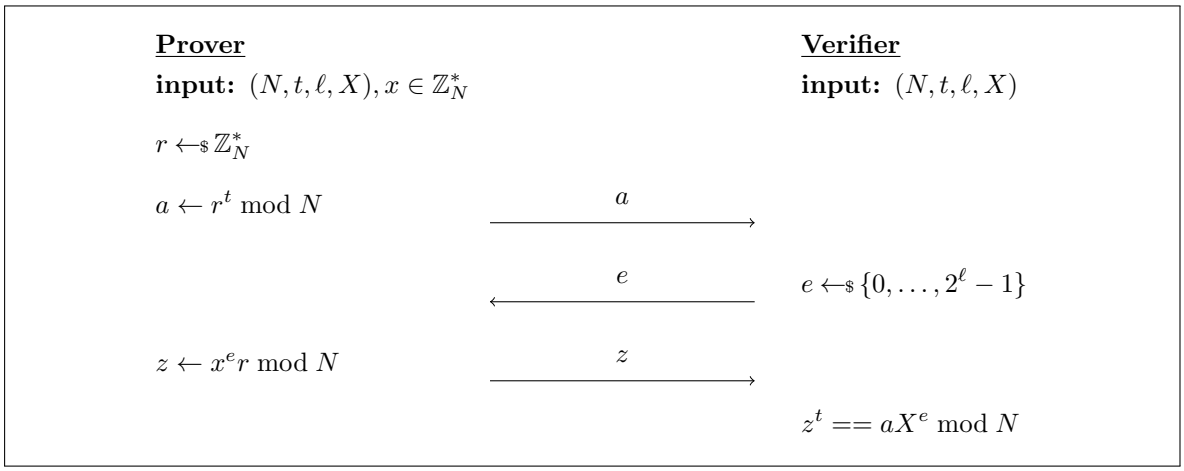


Figure 2: $\Sigma_{RSA}$ protocol. $N$ is a RSA modulus, $t$ a prime s.t. $\gcd(t, \phi(N)) = 1$, $\ell$ s.t. $2^\ell < t$ and we work in $\mathbb{Z}_N^*$. The verifier checks that messages are in correct sets. We omit these checks in the figure.

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

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

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. $\Sigma_{RSA}$ 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 $\mathsf{Gen}$ algorithm for the language, but defining it might give you a clearer view of the protocol.

1. $x = (N, t, X)$ and $w = x$.
2. $R((N, t, X), x) = 1_{x^t = X \bmod N}$.
3. Quite clear, only basic group operations are performed by $R$, $P$, $V$.

4. If the protocol is run honestly, we have

$$z^t = x^{et} r^t = X^e a \bmod N \ .$$

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 $\Sigma$ protocol $(R, \mathsf{Gen}, P, V)$ has adversarial special soundess if for any ppt adversary $\mathcal{A}$ the advantage

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

is negligible in $\lambda$.

**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 $\Sigma$ protocol $(R, \mathsf{Gen}, P, V)$ is strongly HVZK if there exists a **deterministic** simulator $\mathsf{StrSim}$ s.t. the following simulator $\mathsf{Sim}$ is a (perfect-)HVZK simulator for $\Sigma$.

$\mathsf{Sim}(x)$

$e \leftarrow\!\!\$\ \mathcal{E}$ // $\mathcal{E}$ 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 $\mathsf{Sim}$ 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 $\Sigma_{RSA}$ 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 $\Sigma_{RSA}$ 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. $a\alpha + b\beta = 1$.

First assume that we have valid transcripts with $e = e'$ but $z \neq z'$. Then,

$$z^t = aX^e = aX^{e'} = z'^t$$

and $z = z'$ (we can take the $t$-th root on both sides since $\gcd(t, \phi(N)) = 1$). This is a contradiction, therefore $e \neq e'$ and in this case STRSS is equivalent to ADVSS. Since the

relation is believed to be hard, by Question 1 it suffices to show the special soundness property to prove the STRSS property.

First, we have

$$\left(\frac{z}{z'}\right)^t = X^{e-e'} = x^{t(e-e')}$$

. Thus, $\frac{z}{z'} = x^{e-e'}$ and we also know that $X = x^t$. Since $t$ is prime and $e - e' < t$, we have $\gcd(t, e - e') = 1$ and we can find $a, b$ s.t. $at + b(e - e') = 1$. Hence,

$$\left(\frac{z}{z'}\right)^b X^a = x^{at+b(e-e')} = x$$

and we can recover a witness $x$.

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

The simulator simply sample $e \leftarrow_\$ \{0, \ldots, 2^\ell - 1\}$, $z \leftarrow_\$ \mathbb{Z}_N^*$ and computes $a \leftarrow z^t X^{-e} \bmod N$. Following a similar argument as for other $\Sigma$ protocols seen in class, it is clear the simulator has the correct distribution. In addition, we see that it fulfills the definition of strong HVZK.

**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 $\lambda$.

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

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

We can define $\mathcal{H} = (\mathsf{Gen}, H)$ as follows. $\mathsf{Gen}$ runs the generation function of the sigma protocol to get $(x, w)$ and outputs $k := x$. Then, $H(k, x_1, x_2) := \mathsf{StrSim}(x, x_1, x_2)$. In other words, $x$ is the key and $x_1$, $x_2$ correspond to $e$, $z$, respectively. Now, given a collision adversary $\mathcal{A}$, one can construct a STRSS adversary $\mathcal{B}$ s.t.

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

The adversary $\mathcal{B}(x)$ simply runs $(x_1, x_2, x_1', x_2') \leftarrow_{\$} \mathcal{A}(x)$. Now, if $\mathcal{A}$ is successful then $(x_1, x_2) \neq (x_1', x_2') \wedge a = H(x_1, x_2) = H(x_1', x_2')$. In turn, it means $(a, x_1, x_2)$ and $(a, x_1', x_2')$ are accepting transcripts of the sigma protocol (as they were output by the simulator). Hence, the condition to win the STRSS game is fulfilled and $\mathcal{B}$ wins as well.

**Question 6.** Show that the Fiat-Shamir $\Sigma$ 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. $(e, z) \neq (e', z')$...

We can use the simulator to get a valid transcript $(a, e, z)$. Then, it is easy to see that $(a, e, -z)$ is also a valid transcript. Therefore, it is easy to break the STRSS property.

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

We modify the verifier s.t. it checks that $z \in \mathbb{Z}_N^* \cap \{1, \ldots, N/2\}$. Now, both $z$ and $-z$ are not valid anymore. Now assume we can find $(a, e, z)$ and $(a, e', z')$ which are valid transcripts with $(e, z) \neq (e', z')$.
If $e \neq e'$ it is as in the course, we can use the extractor to get a witness. Since the relation is believed to be hard it is not possible.
If $e = e'$ and $z \neq z'$, we have $z'^2 = z^2$ but $z \in \{z', -z'\}$. It follows that $\gcd(z - z', n)$ holds a non-trivial factor of $N$. Since factoring is believed to be hard, it is not possible either.