Advanced Cryptography

Spring Semester 2025

Homework 2

- This homework contains one question: Dinstinguishing Attacks on CROSS
- 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 **teams of two**. If you work in a team, please register it on Moodle and **indicate both teammates' name on the report**. Feel free to ask questions to the T.A.
- We expect all answers to be **formally justified** in order to get full points. Please pay attention to the **rigour** and **clarity** of your answers.
- 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 **May 19th, 2025** at 23 : 59.

1 Distinguishing Attacks on CROSS

In this exercise, we will look at the zero-knowledge property of the CROSS protocol in the version 2.0
We use this document for reference: `https://www.cross-crypto.com/CROSS_SecurityDetails_v2.0.pdf` and follow all of its notations.

CROSS is a digital signature protocol, based on an identification protocol that has been submitted to the NIST additional call for digital signature. It relies on the hardness of the restricted syndrome decoding problem with a subgroup.

Let $\mathbb{E}$ denotes a cyclic subgroup of the multiplicative group $\mathbb{F}_p^*$ with generator g and order some z. We denote by $\star$ the component wise multiplication in $G \leq \mathbb{E}^n$. We define $G = \langle a_1, ..., a_m \rangle := \{a_1^{\bar{u}_1} \star ... \star a_m^{\bar{u}_m} | \bar{u}_i \in \mathbb{F}_z\}$.

Definition 1 (Restricted Syndrome Decoding Problem with a subgroup)**.** Let $G = \langle a_1, ..., a_m \rangle$ for $a_i \in \mathbb{E}^n$, $H \in \mathbb{F}_p^{(n-k)\times n}$ and $s \in \mathbb{F}_p^{(n-k)}$. Does there exists a vector $e \in G$ with $eH^T = s$.

We introduce below the CROSS identification protocol as in the v2.0 of the security document.The protocol corresponds to Figure 4. of the security specifications. It proves knowledge of the following relation

$$\mathcal{R}((s, H), e | s = eH^t, e \in G)$$

for a public $G \subseteq \mathbb{E}^n$. We have that (s, H) is the statement with $s \in \mathbb{F}_p^{n-k}$ and $H \in \mathbb{F}_p^{(n-k)\times n}$ and $e \in G$.

1.1 Understanding the protocol

Question 1

What is the advantage of sending digest_y over y directly? Why do we send Seed as the response in the $\mathsf{chall}_2 = 1$ case?

Question 2

Can you informally explain the role of commitment cmt_0 and commitment cmt_1 with respect to the relationship proven in the protocol?

Question 3

In a Fiat-Shamir fashion, propose a way to make this protocol non-interactive. Be careful, you have two rounds of challenges to take care of.

You do **not** have to prove the security of the resulting protocol.

1.2 Analysis

We recall the definition of Honest Verifier Zero-knowledge used in the security specification (Definition 19).

Definition 2. (Honest-verifier zero-knowledge). Let $\Pi = (P, V)$ be an interactive proof system for an hard relation $R \subseteq X \times Y$. We say that Π is honest-verifier zero-knowledge if there exists a probabilistic polynomial time algorithm S, called the simulator, such that the following two distribution ensembles are indistinguishable:

$$\{(x, y, \mathsf{transcript}(P(x,y), V(x)))|(x,y) \xleftarrow{\$} R\}$$

and

$$\{(x, y, S(x))|(x,y) \xleftarrow{\$} R\}$$

where $\mathsf{transcript}(P(x,y), V(x))$ denotes a transcript of an honest execution between a prover, knowing both x and y, and a verifier, knowing only x.

In this definition, x stands for the statement and y for the witness.

We recall below the proof HVZK and the proposed simulator as per Proposition 24 of their specifications.

Simulator S starts by sampling a random bit chall_2. Then, depending of the value of chall_2, S does the following:

- $\mathsf{chall}_2 = 0$: The simulator picks a random $\mathsf{chall}_1 \in \mathbb{F}_p^*$ then computes $e^* \in \mathbb{F}_p^n$ such that $e^* H^T = s$. Then, S selects a random $v^* \in G$ and a vector $u^* \in \mathbb{F}_p^n$, and computes $u'^* = v^{*-1} \star e^*$. Finally, it computes $s^{*'} = u^* H^T$ and $\mathsf{cmt}_0 = \mathsf{Hash}(s^{*'}, v^*)$. Then, S computes $y^* = u'^* + \mathsf{chall}_1 e^{'*}$. Finally, S set cmt_1 as a random binary string with length 2λ. Since $\mathsf{chall}_2 = 0$ this commitment is never revealed, and thus, in the Random Oracle Model, this has the same statistical distribution as an honestly computed com_1. It is easy to see that the transcript produced by S (i.e., the values y^* and v^*) follows the same statistical distribution as those of an honestly produced transcript. Indeed, in an honest execution, y is uniformly random over $\mathbb{F}_p^*$ because u' is uniformly random over $\mathbb{F}_p^n$. This guarantees that $u' + \mathsf{chall}_1 e'$ is uniformly random over $\mathbb{F}_p^n$, and the same holds after multiplying with v. Finally, in an honest execution of the protocol, v is uniformly distributed over G. Indeed, for any $e' \in G$ there is a unique $v \in G$ such that $v \star e' = e$. If e' is uniformly random over G, then v also follows the same distribution.
- $\mathsf{chall}_2 = 1$: in this case, the simulator simply executes the protocol by sampling the seed and computing cmt_1 analogously to what the honest prover P would do. For the other commitment, cmt_0, it is enough to use a random binary string again.

Question 4

Show that the protocol is not honest-verifier zero-knowledge according to Definition 2 by exhibiting a distinguisher D.

Hint: Observe that, according to Definition 2 the distinguisher is given access to both the statement and the witness.

Question 5

Identify which variant of zero-knowledge the protocol actually satisfies. Give a formal definition of that variant and prove your statement.

Private Key $\mathbf{e} \in G$

Public Key $G \subseteq \mathbb{E}^n$, $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\mathbf{s} = \mathbf{e}\mathbf{H}^\top \in \mathbb{F}_p^{n-k}$

```
PROVER                                                                 VERIFIER

// Sampling Seed to compute $\mathbf{e}', \mathbf{u}'$
$\mathsf{Seed} \xleftarrow{\$} \{0,1\}^\lambda$
$(\mathbf{e}', \mathbf{u}') \leftarrow \mathsf{CSPRNG}(\mathsf{Seed})$ // with co − domain $G \times \mathbb{F}_p^n$

// Computing $\mathbf{v}, \mathbf{u}, \mathbf{s}'$
$\mathbf{v} \leftarrow \mathbf{e} \star (\mathbf{e}')^{-1}$
$\mathbf{u} \leftarrow \mathbf{v} \star \mathbf{u}'$
$\mathbf{s}' \leftarrow \mathbf{u}\mathbf{H}^\top$

// Computing commitments
$\mathtt{cmt}_0 \leftarrow \mathsf{Hash}(\mathbf{s}'|\mathbf{v})$
$\mathtt{cmt}_1 \leftarrow \mathsf{Hash}(\mathbf{u}'|\mathbf{e}')$
                                  $\xrightarrow{\mathtt{cmt}_0, \mathtt{cmt}_1}$
                                      // Sampling first challenge
                                  $\xleftarrow{\mathtt{chall}_1}$                 $\mathtt{chall}_1 \xleftarrow{\$} \mathbb{F}_p^*$

// Computing first response
$\mathbf{y} \leftarrow \mathbf{u}' + \mathtt{chall}_1\mathbf{e}'$
$\mathtt{digest}_\mathbf{y} \leftarrow \mathsf{Hash}(\mathbf{y})$
                                  $\xrightarrow{\mathtt{digest}_\mathbf{y}}$
                                      // Sampling second challenge
                                                                  $\mathtt{chall}_2 \xleftarrow{\$} \{0,1\}$
                                  $\xleftarrow{\mathtt{chall}_2}$

// Computing second response
If $\mathtt{chall}_2 = 0$, $\mathtt{resp} \leftarrow (\mathbf{y}, \mathbf{v})$
If $\mathtt{chall}_2 = 1$, $\mathtt{resp} \leftarrow \mathsf{Seed}$
                                  $\xrightarrow{\mathtt{resp}}$
                                      // Verification
                                      If $\mathtt{chall}_2 = 0$:
                                        $\mathbf{y}' \leftarrow \mathbf{v} \star \mathbf{y}$
                                        $\mathbf{s}' \leftarrow \mathbf{y}'\mathbf{H}^\top - \mathtt{chall}_1\mathbf{s}$
                                        Accept if:
                                          1) $\mathsf{Hash}(\mathbf{y}) = \mathtt{digest}_\mathbf{y}$
                                          2) $\mathsf{Hash}(\mathbf{s}'|\mathbf{v}) = \mathtt{cmt}_0$
                                          3) $\mathbf{v} \in G$
                                      If $\mathtt{chall}_2 = 1$:
                                        $(\mathbf{e}', \mathbf{u}') \leftarrow \mathsf{CSPRNG}(\mathsf{Seed})$ // with co − domain $G \times \mathbb{F}_p^n$
                                        $\mathbf{y} \leftarrow \mathbf{u}' + \mathtt{chall}_1\mathbf{e}'$

                                        Accept if:
                                          1) $\mathsf{Hash}(\mathbf{y}) = \mathtt{digest}_\mathbf{y}$
                                          2) $\mathsf{Hash}(\mathbf{u}'|\mathbf{e}') = \mathtt{cmt}_1$
```

Figure 1: CROSS identification protocol