# Proofs of Security

## TUT n°3 — Zero-knowledge proofs

Léo Ackermann

*Answer all ▸ questions before looking at ⋆ questions.*

## Pedersen commitment

We start by introducing commitment schemes, a cryptographic primitive that allows one to commit to a chosen message while keeping it hidden to others, with the ability to reveal the committed value later on*.

> **Definition 1 (Commitment scheme)** *A* commitment scheme *is a collection of three algorithms* Setup*,* Commit *and* Verif *such that:*
>
> - Setup$(1^\lambda)$ *returns the public parameters* $pp$ *for the security parameter* $\lambda$*.*
> - Commit$(pp, m)$ *returns the commitment* $c$ *and the corresponding opening value* $o$*.*
> - Open$(pp, m, c, o)$ *takes a message* $m$*, commitment* $c$ *and an opening value* $o$ *and returns* $\top$ *iff* $c$ *opens to* $m$ *using* $o$*.*

Two natural security notions arise from such a scheme. The first is the *hiding* property, that morally states that any PPT adversary has no advantage in distinguishing a commitment of a value $m_0$ from a commitment of a value $m_1$, even if she chose the messages. While this property protect the person who is commiting, another ensures that a person looking at a commitment cannot be tricked and is called *binding*. Informally, it states that no PPT adversary can come up with a commitment that opens to different messages using different opening values.

▸ **Question 1.** *Formalize the* Hinding *and* Binding *properties, precising the advantage in the related games.*

▸ **Question 2.** *Show how to construct a hiding and binding commitment scheme from any* IND-CPA *cryptosystem.*

We now focus on a particular commitment scheme, introduced by Perdersen in 1991, and defined as follows.

> - Setup$(1^\lambda)$ chooses a group $G$ of prime order $q$ and outputs two random elements $(g, h)$ of $G$ as the public parameters $pp$.
> - Commit$(pp, m)$ samples $r \leftarrow_\$ \mathbb{Z}_q$ to produce the commit $c = g^m h^r$. The corresponding opening value is $r$.
> - Open$(\mathsf{pp}, m, c, o)$ returns $\top$ iff $c = g^m \cdot h^o$.

▸ **Question 3.** *Prove that the commitment scheme is hiding, and binding under the* DL *assumption.*

▸ **Question 4.** *Getting inspired by Schnorr protocol, propose an* HVZKPoK† *protocol for proving the knowledge of a message-opening couple corresponding to a commited message. What are the expected properties for such a scheme? Prove them.*

▸ **Question 5.** *Extend this protocol for additionally proving that the two handed commitments correspond to the same message.*

▸ **Question 6.** *How can those protocols be made non-interactive?*

## ZKPoK for quadratic residuosity

Let $N \in \mathbb{N}$ be the product of two odd primes. An integer $q$ is called a *quadratic residue modulo* $N$ if there exists an integer $x$ such that $x^2 \equiv q \mod N$. We recall that the set of quadratic residues modulo $N$ form a group $QR_N$.

In this exercise, Alice wants to convinces Bob that the number $x$ she is handing is a quadratic residue modulo $N$. To this end, she follows the protocol $\Pi^{\mathsf{ZKP(oK)}}_{\cdot \in QR_N}$ partially described on next page.

*For a down-to-earth analogy, one can think of predictions in magic tricks.

†In Honest-Verifier Zero-Knowledge-Proof-of-Knowledge, the Verifier is supposed to strictly follows the protocol. This can be exploited when proving the zero-knoweldge property.

The QR-ZKP(oK) protocol followed by Alice $\mathcal{A}$ and Bob $\mathcal{B}$ is the following.

**Protocol $\Pi^{\mathsf{ZKP(oK)}}_{\cdot \in QR_N}$**

1: At the beginning, $\mathcal{A}$ knows $(q, x)$ s.t. $q = x^2 \mod N$, and $\mathcal{B}$ knows $q$
2: $\mathcal{A}$ samples $r \hookleftarrow_\$ \mathbb{Z}_N^\times$ and hands $y = r^2 \mod N$ to $\mathcal{B}$
3: $\mathcal{B}$ samble an uniform random bit $b \hookleftarrow_\$ \{0, 1\}$, and hands it back to $\mathcal{A}$
4: $\mathcal{A}$ set $z = r$ if $b = 1$, $z = xr \mod N$ otherwise, and sends $z$ to $\mathcal{B}$
5: $\mathcal{B}$ checks that $\cdots$

▸ **Question 7.** *Propose a verification step for the verifier Bob.*

▸ **Question 8.** *Prove the scheme is a ZKP for quadratic residuosity.*

▸ **Question 9.** *Prove the scheme is a ZKPoK for quadratic residuosity.*

## (HV)ZKPoK over graphs

In this exercise, we focus on two undirected graphs problems, known as the graph isomorphism problem (GIP) and the 3-coloring problem (3-COL).

**Definition 2 (GIP, 3-COL)** *The graph isomorphism problem (GIP) and the 3-coloring problem (3-COL) are defined as follows:*

- ***GIP.*** *Given two isomorphic[‡] graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, that is such that there exists a mapping $\mu : V_1 \to V_2$ on vertices such that $(u, v) \in E_1$ iff $(\mu(u), \mu(v)) \in E_2$, find such a $\mu$.*
- ***3-COL.*** *Given a 3-colorable graph $G = (V, E)$, that is there is a mapping $\mu : V \to \{0, 1, 2\}$ such that for all $(u, v) \in E$ it holds that $\mu(u) \neq \mu(v)$, find such a $\mu$.*

▸ **Question 10.** *Come up with an Honest-Verifier ZKPoK protocol for the graph isomorphism problem, meaning that as long as the Verifier strictly follows the protocol, the zero-knowledge property is indeed achieved.*

▸ **Question 11.** *Prove that this protocol is indeed HVZKPoK. What are the odds that an adversary fool a verifier? Can this quantity be made negligible in the context of polytime verifiers?*

We now focus on designing a zero-knowledge proof of knowledge for the 3-coloring problem and establish a well-known result about a subclass of languages that belongs to ZKPoK.

▸ **Question 12.** *Propose a ZKPoK protocol for the 3-coloring problem on graphs.*

▸ **Question 13.** *Prove that this is indeed a ZKPoK protocol.*

▸ **Question 14.** *Conclude that **NP** $\subseteq$ **ZK**.*

[‡] In this context, a necessary observation is that the isomorphic relation is an equivalence relation.