






# A Generic Transform from Multi-Round Interactive Proof to NIZK

Pierre-Alain Fouque<sup>1</sup> , Adela Georgescu<sup>2</sup> , Chen Qian<sup>3,4</sup> , Adeline Roux-Langlois<sup>5</sup> , and Weiqiang Wen<sup>6</sup> 

<sup>1</sup> Rennes University, CNRS, INRIA, Rennes, France

<sup>2</sup> Department of Computer Science, University of Bucharest, Romania

<sup>3</sup> Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao, Shandong, China

<sup>4</sup> School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China

<sup>5</sup> Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

<sup>6</sup> LTCI, Telecom Paris, Institut Polytechnique de Paris, France

**Abstract.** We present a new generic transform that takes a multi-round interactive proof for the membership of a language  $\mathcal{L}$  and outputs a non-interactive zero-knowledge proof (not of knowledge) in the common reference string model. Similar to the Fiat-Shamir transform, it requires a hash function  $H$ . However, in our transform the zero-knowledge property is in the standard model, and the adaptive soundness is in the non-programmable random oracle model (NPROM). Behind this new generic transform, we build a new generic OR-composition of two multi-round interactive proofs. Note that the two common techniques for building OR-proofs (parallel OR-proof and sequential OR-proof) cannot be naturally extended to the multi-round setting. We also give a proof of security for our OR-proof in the quantum oracle model (QROM), surprisingly the security loss in QROM is independent from the number of rounds.

## 1 Introduction

Non-interactive zero-knowledge (NIZK) proofs [18,25] can prove a statement without leaking any additional information about the witness. Since its first introduction, NIZK plays an important role in constructing almost every primitive from the basic ones like chosen-ciphertext encryption [33], signature [22] to complex cryptographic protocols like e-voting [17], and e-cash system [12].

**Fiat-Shamir and Random Oracle Model.** The most common and efficient way to construct a non-interactive zero-knowledge proof in the random oracle model (ROM) is via the Fiat-Shamir transform [22]. One first constructs a  $\Sigma$ -protocol (1-round interactive proof), then turns it into non-interactive by simulating the random challenge using a hash function modeled as a random oracle.

Since its first introduction [2], the random oracle model (ROM) has been controversial. The advantage of ROM is that, it is generally easier to build cryptographic

primitives with it, and the resulting primitives are usually more efficient than their standard model version (without random oracle). However, a decade after its introduction Canetti, Goldreich and Halevi [10] discovered that the instantiation of RO is theoretically impossible. More precisely, there exist cryptosystems that are secure in the random oracle model, but for which replacing the random oracle by any implementation leads to an insecure cryptosystem. Therefore, standard model constructions are usually considered as more secure than the constructions in ROM.

Beside of theoretical impossibility, ROM also suffers from some security concerns in real world applications. For example, a common way to instantiate the random oracle is with hash functions (like MD5, SHA-1, SHA-2, SHA-3 etc.). Therefore, any progress in cryptanalysis of hash functions could potentially make the ROM-based schemes insecure. As a concrete example, the work of [38,35] have shown that standard hash functions like MD5 or SHA-1 are far from behaving like random oracles. Based on these attacks, Stevens *et al.* [36] showed an attack on constructing two colliding X.509 certificates for different identities and public keys, while the system is still secure in the ROM.

**NIZK without random oracle.** Efficient NIZK in the standard model is considered as a challenging problem. In the classical setting, a quite efficient NIZK in the standard model has been proposed by [26]. However, the situation of the efficient standard model NIZK in the post-quantum setting is less clear. Several works have constructed efficient post-quantum NIZK schemes by relaxing the soundness definition (only average-case soundness [14] against classical worst-case soundness) or the syntax of NIZK itself (Designated-Verifier NIZK [31], NIZK in the preprocessing model [28]). The full-fledged post-quantum NIZK in the standard model is only due to a new framework in the recent breakthrough results [9,8], which gives the first lattice-based NIZK without RO [34]. As another instantiation of this framework, a new NIZK based on Learning Parity with Noise assumption and Trapdoor Hash Functions has also been proposed [6]. However, the efficiency of all these constructions in the standard model is still far from that of post-quantum NIZK in ROM [32,7,21].

**Non-programmable random oracle.** In recent years, there is another research direction of NIZK consists of replacing the ROM by its weaker variant non-programmable random oracle model NPROM, while preserving the efficiency [29,15]. These constructions are both generic transforms from  $\Sigma$ -protocols to NIZK. Interestingly, they both have zero-knowledge property in the standard model, and soundness property in the non-programmable random oracle model (NPROM).

Another interesting point about these two constructions is that, their zero-knowledge property is independent of the random oracle model. Therefore, in many applications, such as e-voting or authenticated encryptions, it guarantees that even the hash function is broken in the future, the privacy is still preserved.

**Limits of NIZK in NPROM.** One big problem of both transforms [29,15] is that, they only work for  $\Sigma$  protocols but not the more generic multi-round public-coin interactive proofs (PCIP). As several recent results of interactive proofs are exploiting

the multi-round property of PCIP to gain efficiency, such as bullet proofs [7], exact proofs [21] or amortized exact proofs [4], an interesting question would be to extend the [29,15] transforms to multi-round interactive protocols. Moreover, between these two transforms, [15] not only requires less properties of the starting  $\Sigma$ -protocol than [29] (optimal soundness against special soundness) but it is also more efficient. Therefore, we have chosen to focus on extending [15] in this paper. Unfortunately, it cannot be easily extended, as its principal building block is an OR-composition of two  $\Sigma$ -protocol, and the existing OR-composition techniques do not apply to multi-round PCIP. We will give below a quick overview of the existing OR-proofs.

**OR-proof.** The OR-composition of  $\Sigma$ -protocols has been initially used to construct ring-signature schemes by [16] based on the programmable random oracle. Another OR-composition technique has been proposed by [1] to weaken the model, they only require the NPROM, and [1] has a shorter proof than [16] (one hash value less in the proof.) However, neither of them can be extended to the OR-composition of multi-round public-coin interactive proofs. Note that, for multi-round interactive proofs, we can firstly use Fiat-Shamir transform to reduce the number of rounds, then apply [16] or [1] to construct NIZK. But, the Fiat-Shamir transform requires programmability of the random oracle for the zero-knowledge property. As our goal is to keep the zero-knowledge property in the standard model, this approach does not work. This raises a natural question:

*Can we build a generic OR-composition of multi-round PCIP, with zero-knowledge in the standard model and soundness in NPROM?*

We will answer this question positively by giving a new technique for OR-composition.

**Security in the Quantum Random Oracle model (QROM).** Security of random oracle model in the quantum setting is not a trivial problem. Intuitively, a quantum adversary can build the hash function and run the primitive himself by querying quantum states. Therefore, the adversary can get a superposition of exponentially many samples of the random oracle, which gives him more advantage than a classical adversary. Many recent works address this issue [19,20,30], and they give detailed analysis for the Fiat-Shamir transform in this setting. As we claim that we have a post-quantum zero-knowledge proof, we also give an analysis of our transform in the QROM.

## 1.1 Our contributions

In this paper, we bring several contributions. Firstly, we propose a new generic transform from multi-round PCIP to NIZK, with zero-knowledge property in the standard model and soundness in NPROM. The principal new technique behind this transform is a new OR-proof of two different PCIPs. Surprisingly, the soundness in QROM of both multi-round PCIP to NIZK and OR-proof of PCIPs has a security loss of  $O(Q_H^4)$  which is independent from the number of rounds.

More precisely:

- We propose in this paper a new generic transform from multi-round public-coin interactive proofs (PCIP) to a non-interactive zero-knowledge proof system (NIZK). Compared to Fiat-Shamir transform, the zero-knowledge property of our transform is in the *standard model*, and soundness property is in the *non-programmable random oracle model* (NPROM) (RO without programmability). While comparing with similar type of transforms [29,15], ours additionally supports multi-round PCIP.
- Behind our generic transform, we have developed a new technique to generate an OR-proof from two optimal sound PCIP:  $PCIP_0, PCIP_1$ . The direct approach consists of using Fiat-Shamir transform to turn both  $PCIP_0$  and  $PCIP_1$  into  $\Sigma$ -protocols, then apply either [16] or [1] transform to get an OR-proof. Compared to the direct approach, the zero-knowledge property of our transform is in the *standard model*, and our adaptive soundness property is in the NPROM. We believe that this new OR-composition has other applications and independent interests.
- Finally, we analyze the soundness property of our OR-proof in the QROM. Note that the zero-knowledge property of our OR-proof is in the standard model, therefore it is naturally secure in the QROM. Moreover, our transform from PCIP to NIZK has the same security loss as our OR-proof. Surprisingly, the security loss of the soundness is  $O(Q_H^4)$  which is independent of the number of rounds.

## 1.2 Technical overview

Our main technique consists in constructing the OR-proof for multi-round PCIPs. We dedicate this section to explain the intuition behind our OR-proof. Firstly, we will give a quick overview of the existing parallel OR-proof [16] and sequential OR-proof [1,24] as we will borrow ideas from both transforms. Then, we explain why they can not be extended to  $n$ -round PCIPs, and our new techniques of OR-proof.

**Why [16] does not work for  $n$ -round PCIPs?** Given  $\Sigma_0$  and  $\Sigma_1$  two  $\Sigma$ -protocols with transcripts  $\{R_0, h_0, s_0\}$  and  $\{R_1, h_1, s_1\}$ , the intuition behind the parallel [16] transform is that, after generating the first round commitments  $(R_0, R_1)$ , the corresponding challenges are chosen such that  $h_0 \oplus h_1 = H(R_0, R_1)$ . Therefore any adversary can freely choose one (and only one) between  $h_0$  and  $h_1$  even before seeing  $(R_0, R_1)$ . By using the HVZK property of the  $\Sigma$ -protocol, once  $h_0$  (or  $h_1$ ) chosen, the adversary can simulate the proof  $(R_0, s_0)$  or  $(R_1, s_1)$  without knowing any witness.

Let us now see why this approach can not be extended to  $n$ -round interactive protocols when  $n > 1$ . The natural extension of [16] would be to define the  $i$ -th round challenges ( $i \in [n]$ ) such that  $h_{i,0} \oplus h_{i,1} = H(\{R_{j,0}, R_{j,1}\}_{j=1}^i)$ . This transform is not secure. To show this, we construct below an example of two 2-round protocols that are secure individually, but once combined, the resulting OR-proof is not secure anymore.

**Counter-example of [16] applying on 2-round PCIPs.** Given two  $\Sigma$ -protocols  $\Sigma_0$  and  $\Sigma_1$ , we will construct two 2-round protocols  $PCIP_0, PCIP_1$  by adding one unused round into each of  $\Sigma_0, \Sigma_1$  but in different order. Namely, valid transcripts of  $PCIP_0$  and  $PCIP_1$  are of the form  $(\bar{R}_0, \bar{h}_0, R_0, h_0, s_0)$  and  $(R_1, h_1, \bar{R}_1, \bar{h}_1, s_1)$ , where

$(\bar{R}_0, \bar{h}_0, \bar{R}_1, \bar{h}_1)$  are just random strings and ignored in the verification process. If we apply the naive extension of [16] transform to  $\text{PCIP}_0$  and  $\text{PCIP}_1$ , an adversary  $\mathcal{A}$  can randomly choose  $h_0, h_1$ , then use HVZK to simulate  $(R_0, h_0, s_0)$  and  $(R_1, h_1, s_1)$ . As  $(\bar{R}_0, \bar{h}_0, \bar{R}_1, \bar{h}_1)$  are ignored by the individual verification of  $\text{PCIP}_0$  and  $\text{PCIP}_1$ ,  $\mathcal{A}$  can define  $\bar{R}_0, \bar{R}_1$  to be random strings and

$$\bar{h}_0 := h_1 \oplus H(\bar{R}_0, R_1), \quad \bar{h}_1 := h_0 \oplus H(R_0, \bar{R}_1).$$

By the correctness of  $\text{PCIP}_0$  and  $\text{PCIP}_1$ ,  $(\bar{R}_0, \bar{h}_0, R_0, h_0, s_0, R_1, h_1, \bar{R}_1, \bar{h}_1, s_1)$  is a valid proof for which  $\mathcal{A}$  does not need to know any witness in order to produce it, so he can easily break soundness of the OR-proof composition.

The above attack works because we have given too much "freedom" to  $\mathcal{A}$ . He can freely chose one challenge per round. Therefore, we need to limit  $\mathcal{A}$  to only be able to freely choose the challenges from the same interactive protocol.

**Overview of sequential OR-proof [1,24].** Given two  $\Sigma$ -protocols  $\Sigma_0$  and  $\Sigma_1$ , together with two statements  $x_0, x_1$  and a witness  $w_0$ . (*w.l.o.g.* we can assume that we know  $w_0$ .) The intuition of the sequential OR-proof is that  $H(R_0)$  is used as the challenge  $h_1$  for  $\Sigma_1$  and  $H(R_1)$  is used as the challenge  $h_0$  for  $\Sigma_0$ . The honest generation of the proof is given as in Figure 1.

<pre> Prove(<math>x_0, x_1, w_0</math>): 01 <math>(R_0, st_0) \xleftarrow{\\$} \Sigma_0.\text{Prove}_1(x_0, w_0)</math> 02 <math>h_1 := H(R_0)</math> 03 <math>(R_1, s_1) \xleftarrow{\\$} \Sigma_1.\text{Sim}(x_1, h_1)</math> 04 <math>h_0 := H(R_1)</math> 05 <math>s_0 \xleftarrow{\\$} \Sigma_0.\text{Prove}_2(x_0, w_0, h_0, st_0)</math> 06 <b>return</b> <math>(R_0, R_1, h_0, h_1, s_0, s_1)</math> </pre>
---

**Fig. 1.** Prove algorithm of sequential OR-proof

The intuition behind the sequential OR-proof is that, one can freely choose to generate  $R_0$  or  $R_1$  first. However, once chosen to generate  $R_b$  and  $h_{1-b}$  first, then  $h_b$  will be chosen independently from the value  $R_b$ . By the soundness of  $\Sigma_b$  without  $w_b$ , no PPT adversary can generate a valid transcript  $\text{Trans}_b = (R_b, h_b, s_b)$ .

For  $n$ -round PCIPs, we can notice that before the honest side ( $b$ ) has been executed until the  $(n - 1)$ th round, the simulation side  $(1 - b)$  doesn't have all the challenges, therefore even an honest prover with  $w_b$  cannot generate a valid proof when  $n > 1$ .

**Intuition behind our approach.** Let us consider two  $n$ -round public-coin interactive proofs  $\text{PCIP}_0$  and  $\text{PCIP}_1$  for proving the membership of two languages  $\mathcal{L}_0$  and  $\mathcal{L}_1$ . For simplicity, we assume  $\text{PCIP}_0$  and  $\text{PCIP}_1$  have same number of rounds in this section. We will prove that  $x_0 \in \mathcal{L}_0$  or  $x_1 \in \mathcal{L}_1$  without revealing exactly which witness is used.

Let  $\text{Trans}_0 = (\{R_{i,0}, h_{i,0}\}_{i=1}^n, s_0)$  and  $\text{Trans}_1 = (\{R_{i,1}, h_{i,1}\}_{i=1}^n, s_1)$  be two transcripts of PCIP<sub>0</sub> and PCIP<sub>1</sub> respectively.

Our starting point is the parallel OR-proof. To prevent the above attack against multi-round parallel OR-proof, our idea is to combine all the challenges of the same side together by an offset. Therefore, once the offset and the first  $i$  rounds commitments are fixed, the challenges are fixed. More precisely, for  $b \in \{0, 1\}$ , we denote by  $A_b = \{a_{1,b}, \dots, a_{n,b}\}$  two offsets, we could compute the challenges of the  $i$ -th round as follows,

$$h_{i,0} = H(\{R_{j,0}\}_{j=1}^i) + a_{i,0}, \quad h_{i,1} = H(\{R_{j,1}\}_{j=1}^i) + a_{i,1}. \quad (1)$$

Now, the challenges are all related. We emphasize the fact that the adversary can freely choose  $A_b$ , where  $b \in \{0, 1\}$ , is equivalent to be able to choose every challenge of  $b$  side.

The second step is to only allow the adversary to freely choose one and only one offset between  $A_0$  and  $A_1$ . To do this, we borrow the idea from the sequential or-proof by putting  $A_0$  and  $A_1$  into the hash of the opposite side. More precisely, we have

$$h_{i,0} = H(\{R_{j,0}\}_{j=1}^i, A_1) + a_{i,0}, \quad h_{i,1} = H(\{R_{j,1}\}_{j=1}^i, A_0) + a_{i,1}. \quad (2)$$

As in sequential OR-proof, the order of query  $A_0$  and  $A_1$  is crucial in our case. Namely, at least one of the two cases must happen:

- Before the RO query on  $(\{R_{j,0}\}_{j=1}^i, A_1)$ , there exists a query of the form  $(\cdot, A_0)$ .
- Before the RO query on  $(\{R_{j,1}\}_{j=1}^i, A_0)$ , there exists a query of the form  $(\cdot, A_1)$ .

This forces the adversary to choose  $A_0$  before having seen  $H(\{R_{j,0}\}_{j=1}^i, A_1)$  or  $A_1$  before having seen  $H(\{R_{j,1}\}_{j=1}^i, A_0)$ . We can use this property to reduce the adaptive soundness of our OR-proof to the optimal soundness of the underlying PCIPs.

**Security in the QROM.** In our QROM security proof, we apply the Measure-then-Reprogram 2.0 technique [19]. There is a price to pay for proving our transform in the QROM, that is we need the programmability of the random oracle. Moreover, if we want to prove our transform for round-by-round, we need to program the random oracle in every round, this will introduce an exponential security loss in the number of rounds. Therefore, we restrict our transform to only optimal-sound PCIPs, then we can prove our transform with only  $O(Q_H^4)$  security loss.

Note that, despite the fact that our OR-proof is a composition of two multi-round PCIPs, we only need to apply the Measure-then-Reprogram 2.0 technique on 2 entries. This is due to the fact that our OR-proof is not a proof of knowledge, but only a proof of membership, which is already useful in many applications such as voting schemes etc.

Therefore, we do not need all the entries to be able to extract the witness. This observation makes our security loss of the adaptive soundness as low as  $O(Q_H^4)$  in QROM, which is independent from the number of rounds  $n$ . Different from our result, [19] has considered the soundness with proof of knowledge (stronger than our adaptive soundness) of Fiat-Shamir transform and their security loss is  $O(Q_H^{2n})$ .

Very recently, there is a new semi-generic transformation [27] from PCIPs to non-interactive proofs in the QROM while achieving proof of knowledge. However it requires the prover's response to be in linear form. As a comparison, our transformation is generic and does not impose any restriction on the prover's response.

In comparison, Unruh's transform [37] works for any  $\Sigma$ -protocol, but introduces a noticeable overhead depending on the size of the challenge set. In [13], Chen et al extend Unruh's framework for a 3-round protocol where the second challenge is binary.

## 2 Preliminaries

### 2.1 Notations.

For  $n \in \mathbb{N}$ , let  $[n] = \{1, \dots, n\}$ . For a finite set  $\mathcal{S}$ , we denote the sampling of a uniform random element  $x$  by  $x \xleftarrow{\$} \mathcal{S}$ . For simplicity of the notations, we omit that every algorithm takes as input the public parameter  $\text{par}$ . For an algorithm  $A$  which takes  $x$  as input, we denote its computation by  $y \xleftarrow{\$} A(x)$ . We assume all the algorithms (including adversaries) in this paper to be probabilistic unless stated otherwise. We denote an algorithm  $A$  with access to an oracle  $\mathcal{O}$  by  $A^{\mathcal{O}}$ .

For an NP language  $\mathcal{L}$ , we denote by  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$  the fact that the statement  $\mathbf{x}$  is in the language  $\mathcal{L}$  with the witness  $\mathbf{w}$ .

We use code-based games [3] to present our definitions and proofs. We implicitly assume all Boolean flags to be initialized to 0 (**false**), numerical variables to 0, sets to  $\emptyset$  and strings to  $\perp$ . We make the convention that a procedure terminates once it has returned an output.  $\text{Exp}_{\Sigma, A}^G(1^\lambda) = b$  denotes the final (Boolean) output  $b$  of the adversary  $A$  running the security experiment  $G$  on the scheme  $\Sigma$  with security parameter  $\lambda$ , and if  $b = 1$  we say  $A$  wins  $G$ . The randomness in  $\Pr[\text{Exp}_{\Sigma, A}^G(1^\lambda) = 1]$  is over all the random coins in experiment  $G$ . Within a procedure, "abort" means that we terminate the run of an adversary  $A$ .

### 2.2 $n$ -Round Public Coin Interactive Proof (PCIP)

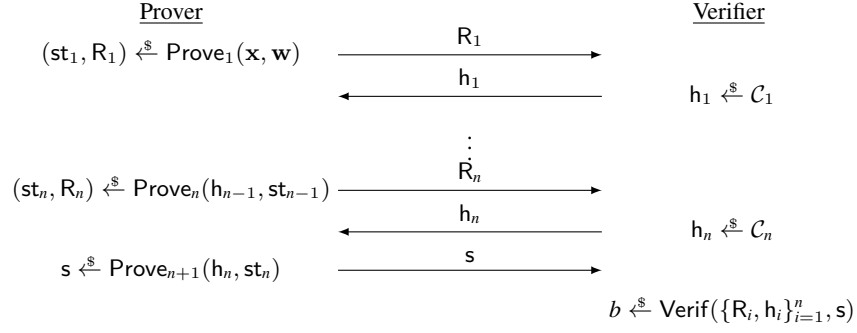
The general structure of an  $n$ -round Public-Coin Interactive Proof of the form depicted in Figure 2 is defined as follows.<sup>7</sup> Notice that for  $n = 1$ , PCIP is a  $\Sigma$ -protocol, and PCIP is also named as identification scheme in some literatures.

**Definition 1 ( $n$ -round Public-Coin Interactive Proof).** *Let  $\mathcal{L}$  be an NP language. To prove a statement  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$ , an  $n$ -round public-coin interactive proof consists of  $n + 2$  PPT stateful algorithms  $\text{PCIP} = (\{\text{Prove}_i\}_{i=1}^{n+1}, \text{Verif})$  with the following syntax:*

- $\text{Prove}_i(h_{i-1}, \text{st}_{i-1})$  takes a challenge  $h_{i-1}$  and a state  $\text{st}_{i-1}$  as input, and returns a commitment  $R_i$  and a new state  $\text{st}_i$ , where  $\text{st}_0 = (\mathbf{x}, \mathbf{w})$ , and  $R_{n+1} = \mathbf{s}$ .
- $\text{Verif}(\mathbf{x}, (\{R_i, h_i\}_{i=1}^n, \mathbf{s}))$ : The verification  $\text{Verif}$  takes as input a statement  $\mathbf{x}$  and a transcript  $(\{R_i, h_i\}_{i=1}^n, \mathbf{s})$  and returns a decision 0 or 1.

*We introduce the following definitions for a PCIP scheme:*

<sup>7</sup> In this paper, we use the convention that  $n$ -round PCIP has  $2n + 1$  moves.



**Fig. 2.** An  $n$ -round Interactive Protocol

- **Transcript:** We define a **transcript** as all messages between the prover and the verifier of the form  $\text{Trans} = (\{R_i, h_i\}_{i=1}^n, s)$ . Moreover, we define a partial transcript  $\text{Trans}'$  as prefix of another transcript of the form  $(\{R_i, h_i\}_{i=1}^j)$  with  $j \leq n$ .

We require the following properties for an  $n$ -round PCIP:

- **Correctness:** For all  $(\mathbf{x}, \mathbf{w})$  such that  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$  and for all honestly generated transcripts  $\text{Trans} = (\{R_i, h_i\}_{i=1}^n, s)$  using  $(\mathbf{x}, \mathbf{w})$ , we say that PCIP is  $\rho$ -correct if we have:

$$\Pr[\text{Verif}(\mathbf{x}, (\{R_i, h_i\}_{i=1}^n, s)) = 0] \leq \rho.$$

- **Honest-Verifier Zero-Knowledge:** For all  $(\mathbf{x}, \mathbf{w})$  such that  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$ , we say that PCIP is  $\Delta$ -HVZK, if there exists a PPT simulator  $\text{Sim}$  that takes  $\mathbf{x}$  as input, and returns a transcript  $\text{Trans}$ , such that the distribution of  $\text{Trans}$  is at statistical distance at most  $\Delta$  from the distribution of an honestly generated transcript. In particular, if  $\Delta = 0$ , we say that PCIP has perfect HVZK.
- **Round-by-Round Soundness:** Let PCIP be an interactive-proof with  $i$ -th round challenge space  $\mathbb{Z}_{\ell_i}$ . We say that PCIP is round-by-round sound if, there exists a "doomed set"  $\mathcal{D} \in \{0, 1\}^*$  such that,
  - If  $\mathbf{x} \notin \mathcal{L}$ , then  $(\mathbf{x}, \emptyset) \in \mathcal{D}$ , where  $\emptyset$  denotes the empty transcript.
  - For all partial transcript  $\text{Trans}$ , such that  $(\mathbf{x}, \text{Trans}) \in \mathcal{D}$ , for all next message  $R_i$  given by the prover, there exists a negligible function  $\text{negl}(\cdot)$  such that

$$\Pr[(\mathbf{x}, \text{Trans} \| R_i \| h_i) \notin \mathcal{L} \mid h_i \xleftarrow{\$} \mathbb{Z}_{\ell_i}] \leq \text{negl}(\lambda).$$

- For any complete transcript  $\text{Trans}$ , if  $(\mathbf{x}, \text{Trans}) \in \mathcal{D}$  then  $\text{Verif}(\mathbf{x}, \text{Trans}) = \text{false}$ .

Notice that the round-by-round soundness originally proposed by [8] is a very weak security notion. Since we only consider the constant rounds interactive proofs, by [8,



Proposition 5.3 and 5.4] round-by-round soundness and negligible soundness are equivalent. On the other hand, optimal soundness (c.f. Definition 9 which is a multi-round version of special soundness) is a commonly used term for many protocols. If a protocol is  $\varepsilon$ -optimal sound then it can be seen as no transcript can escape the doomed set except in one specific round with probability  $\varepsilon$ . Therefore, optimal soundness tightly implies round-by-round soundness. This provides us an alternative way to use our transform.

### 2.3 Non-Interactive Proof NIP

For the sake of completeness, we define two different types of non-interactive proofs NIP: Non-Interactive Zero-Knowledge proofs (NIZK) and Non-Interactive Witness Indistinguishable proofs (NIWI). Notice that we don't consider the proof of knowledge in this paper, and we use the adaptive soundness for NIPs.

**Definition 2 (Non-Interactive Proof NIP).** Let  $\mathcal{L}$  be an NP language. To prove a statement  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$ , a non-interactive proof consists of four PPT algorithms  $\Pi = (\text{Setup}, \text{Prove}, \text{Verif}, \text{Sim} = (\text{Sim}_0, \text{Sim}_1))$  defined as follows:

- $\text{Setup}(1^\lambda) \rightarrow \text{CRS}$  : The setup algorithm Setup returns a common reference string CRS.
- $\text{Prove}(\text{CRS}, \mathbf{x}, \mathbf{w}) \rightarrow \pi$  : The prove algorithm Prove returns a proof  $\pi$  that  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$  using  $\mathbf{w}$  as witness.
- $\text{Verif}(\text{CRS}, \mathbf{x}, \pi) \rightarrow \{0, 1\}$  : The verification algorithm Verif returns a decision, 1 (acceptance) or 0 (rejection).
- $\text{Sim}_0(1^\lambda) \rightarrow (\text{CRS}, \tau)$  : The first part of the simulation algorithm  $\text{Sim}_0$  outputs a common reference string CRS and a simulation trapdoor  $\tau$ .
- $\text{Sim}_1(\tau, \mathbf{x}) \rightarrow \pi$  : The second part of the simulation algorithm  $\text{Sim}_1$  outputs a simulated proof  $\pi$ .

We will also define the completeness, adaptive soundness, zero-knowledge, witness-indistinguishability of NIP as follows.

**Definition 3 ( $\rho$ -Completeness).** A NIP is  $\rho$ -complete if, for all  $\mathbf{x} \in_{\mathbf{w}} \mathcal{L}$  we have:

$$\Pr \left[ \text{Verif}(\text{CRS}, \mathbf{x}, \pi) = 0 \mid \begin{array}{l} \text{CRS} \xleftarrow{\$} \text{Setup}(1^\lambda) \\ \pi \xleftarrow{\$} \text{Prove}(\text{CRS}, \mathbf{x}, \mathbf{w}) \end{array} \right] \leq \rho.$$

**Definition 4 ( $(\varepsilon, Q_H)$ -Adaptive Soundness).** A NIP is  $(\varepsilon, Q_H)$ -adaptively sound in the non-programmable random oracle model NPRM, if for all PPT adversaries  $\mathcal{A}$  requiring at most  $Q_H$  hash queries we have:

$$\Pr \left[ \mathbf{x}^* \in \{0, 1\}^n \setminus \mathcal{L} \wedge \text{Verif}(\text{CRS}, \mathbf{x}^*, \pi^*) = 1 \mid \begin{array}{l} \text{CRS} \xleftarrow{\$} \text{Setup}(1^\lambda) \\ (\mathbf{x}^*, \pi^*) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{Hash}}}(\text{CRS}) \end{array} \right] \leq \varepsilon.$$

We consider the hash function as an NPRO in the soundness proof.

**Definition 5 (Zero-Knowledge).** A NIP is  $\Delta$ -Zero-Knowledge, if there exists a simulator  $\text{Sim} = (\text{Sim}_0, \text{Sim}_1)$  such that, the statistical distance between the output distributions of **Game** Sim and **Game** Real as defined in Figure 3 is at most  $\Delta$ .

Moreover, if  $\Delta = 0$ , NIP is perfectly zero-knowledge.

<b>Game Sim:</b> 01 $(\text{CRS}, \tau) \xleftarrow{\$} \text{Sim}_0(1^\lambda)$ 02 $(\mathbf{x}, \mathbf{w}) \xleftarrow{\$} \mathcal{A}(\text{CRS}) \quad \ \mathbf{x} \in_{\mathbf{w}} \mathcal{L}$ 03 $\pi \xleftarrow{\$} \text{Sim}_1(\mathbf{x}, \tau)$ 04 <b>return</b> $(\text{CRS}, \pi)$	<b>Game Real:</b> 05 $\text{CRS} \xleftarrow{\$} \text{Setup}(1^\lambda)$ 06 $(\mathbf{x}, \mathbf{w}) \xleftarrow{\$} \mathcal{A}(\text{CRS}) \quad \ \mathbf{x} \in_{\mathbf{w}} \mathcal{L}$ 07 $\pi \xleftarrow{\$} \text{Prove}(\text{CRS}, \mathbf{x}, \mathbf{w})$ 08 <b>return</b> $(\text{CRS}, \pi)$
---	--

**Fig. 3.** Real and Sim experiments for the zero-knowledge property

**Definition 6 (Witness Indistinguishable for OR-Composition).** Let  $\mathcal{L}_\vee = \mathcal{L}_0 \vee \mathcal{L}_1$  be an OR-relation. A NIP is  $\Delta$ -Witness Indistinguishable for  $\mathcal{L}_\vee$ , if for the statement  $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1)$  and the witness  $(\mathbf{w}_0, \mathbf{w}_1)$  such that  $\mathbf{x}_0 \in_{\mathbf{w}_0} \mathcal{L}_0 \vee \mathbf{x}_1 \in_{\mathbf{w}_1} \mathcal{L}_1$ , the statistical distance between the output distributions of the **Game 0** and the **Game 1** as defined in Figure 4 is at most  $\Delta$ .

<b>Game 0:</b> 01 $\text{CRS} \xleftarrow{\$} \text{Setup}(1^\lambda)$ 02 $\pi \xleftarrow{\$} \text{Prove}(\text{CRS}, \mathbf{x}, \mathbf{w}_0)$ 03 <b>return</b> $\pi$	<b>Game 1:</b> 04 $\text{CRS} \xleftarrow{\$} \text{Setup}(1^\lambda)$ 05 $\pi \xleftarrow{\$} \text{Prove}(\text{CRS}, \mathbf{x}, \mathbf{w}_1)$ 06 <b>return</b> $\pi$
--	--

**Fig. 4.** Real and Sim experiments for the witness-indistinguishability

Moreover, if  $\Delta = 0$ , NIP is perfectly witness indistinguishable.

We define NIZK as NIP that satisfy completeness, adaptive soundness and zero-knowledge property while for NIWI, the zero-knowledge property is replaced with witness-indistinguishability.

### 3 From Interactive to Non-Interactive

One of the most common way to construct a non-interactive zero-knowledge proof is via the Fiat-Shamir [23] transform. However, we additionally require the zero-knowledge property to be ROM-free, which is not the case using this transform. The two existing variants available for  $\Sigma$ -protocols (1-round protocols) are [29] and its more efficient and more generic improvement [15].

**Lindell's transform [29]** In Lindell's transform, the challenge of  $\Sigma$ -protocol is of the form  $H(\mathbf{x}, \text{Com}(\mathbf{R}))$ , where  $\mathbf{R}$  is the first round message of the  $\Sigma$ -protocol and  $\text{Com}$  is a dual-mode commitment [29] (aka. hybrid trapdoor commitment [11]). However, if we want to generalize this transform to multi-round PCIP, this approach is not very efficient. That is because, we need to include the commitments and the decommitments of every round of PCIP into the final proof. Moreover, following the generic construction of dual-mode commitment from PCIP schemes in [29], the size of one commitment

and one decommitment is equal to the size of one PCIP proof. Therefore, if we directly apply the Lindell’s transform, we will have a proof size blow-up of factor  $O(n)$ , where  $n$  is the number of rounds. Consequently, it may lose the efficiency gain of multi-round PCIP schemes over  $\Sigma$ -protocols.

**Ciampi *et al.* transform [15]** The transform in [15] requires only computational optimal soundness (weaker than special soundness) and computational HVZK of the underlying interactive protocols, and it is more efficient than [29]. However, the [15] transform relies heavily on the existence of an OR-composition of interactive protocols. Unfortunately, the most efficient interactive lattice-based proof systems are all 2-round protocols [5,21,4], and the previous OR-compositions of interactive proof systems [16,1,24] cannot be applied to multi-round PCIPs.

In this section, we further improve the [15] transform by extending it to support OR-composition of an  $n_0$ -round computational HVZK and round-by-round sound PCIP<sub>0</sub> and an  $n_1$ -round computational HVZK and round-by-round sound PCIP<sub>1</sub>. Notice that if we apply our transform to two 1-round PCIPs ( $\Sigma$ -protocols), the resulting NIZK scheme is almost as efficient as in [15]. More precisely, in the case of  $\Sigma$ -protocol, we only have two more elements  $(a_0, a_1) \in \mathbb{Z}_{\ell_{1,0}} \times \mathbb{Z}_{\ell_{1,1}}$  than [15], where  $\ell_{1,0}, \ell_{1,1}$  are the size of the challenge spaces of PCIP<sub>0</sub> and PCIP<sub>1</sub>. In Section 2.3 we recall the definitions of two different types of non-interactive proofs NIP: NIZK proofs and Non-Interactive Witness Indistinguishable (NIWI) proofs.

### 3.1 Construction of our OR-Proof

We recall that the intuition behind our OR-proof is explained in Section 1.2. We then directly give the construction of our OR-proof in this section.

Let PCIP<sub>0</sub> (*resp.* PCIP<sub>1</sub>) be an  $n_0$ -round (*resp.*  $n_1$ -round) public coin interactive proof for proving the membership of two languages  $\mathcal{L}_0$  and  $\mathcal{L}_1$ , and we denote the size of challenge spaces by  $(\ell_{1,0}, \dots, \ell_{n_0,0}, \ell_{1,1}, \dots, \ell_{n_1,1})$ . The goal is to prove that  $\mathbf{x}_0 \in \mathcal{L}_0$  or  $\mathbf{x}_1 \in \mathcal{L}_1$  without revealing exactly which witness is used. The idea behind this proof, using  $w_b$ , is to first sample a random offset  $A_b = (a_{1,b}, \dots, a_{n_b,b})$ . Then, we simulate the proof PCIP<sub>1-b</sub> for which we don’t have a witness to build the second offset  $(a_{1,1-b}, \dots, a_{n_{1-b},1-b})$ , which depends on  $A_b$  and on the commitments  $\{R_{i,1-b}\}_{j=1}^{n_{1-b}}$ . Finally, we can use  $A_{1-b}$  to build the proof PCIP<sub>b</sub> for which we know the witness. To verify the proof, we first verify that all the  $\{h_{i,b}\}$  have been correctly generated, then that both proofs pass their verification algorithm.

We give our transform in pseudo-code in Figure 5. We define  $\mathcal{C}_{i,b}$  as the challenge space of  $i$ -th round of PCIP<sub>b</sub>, we assume that  $\mathcal{C}_{i,b}$  is isomorphic to the additive group  $(\mathbb{Z}_{\ell_{i,b}}, +)$ .

**Properties of our NIP.** We will prove in the remaining part of this section that the non-interactive proof NIP constructed as in Figure 5 is correct (Theorem 1), witness-indistinguishable (Theorem 2), and adaptively sound (Theorem 3), if the underlying protocols PCIP<sub>0</sub>, PCIP<sub>1</sub> are both correct, HVZK and round-by-round sound. Moreover,

```

Prove( $\mathbf{x}_0, \mathbf{x}_1, \mathbf{w}_b$ ):
01  $\mathbf{A}_b := (a_{1,b}, \dots, a_{n_b,b}) \xleftarrow{\$} \mathbb{Z}_{\ell_{1,b}} \times \dots \times \mathbb{Z}_{\ell_{n_b,b}}$ 
02  $\text{Trans}_{1-b} \xleftarrow{\$} \text{PCIP}_{1-b}.\text{Sim}(1^\lambda, \mathbf{x}_{1-b})$ 
03  $(\{\mathbf{R}_{i,1-b}, \mathbf{h}_{i,1-b}\}_{i=1}^{n_{1-b}}, \mathbf{s}_{1-b}) =: \text{Trans}_{1-b}$ 
04 for  $i = 1..n_{1-b}$  do
05    $a_{i,1-b} \leftarrow \mathbf{h}_{i,1-b} - \mathbf{H}(\{\mathbf{R}_{j,1-b}\}_{j=1}^i, \mathbf{A}_b)$ 
06  $\mathbf{A}_{1-b} \leftarrow (a_{1,1-b}, \dots, a_{n_{1-b},1-b})$ 
07  $\text{st}_{0,b} = \emptyset; \mathbf{h}_{0,b} = \perp$ 
08 for  $i = 1..n_b$  do
09    $(\mathbf{R}_{i,b}, \text{st}_{i,b}) \xleftarrow{\$} \text{PCIP}_b.\text{Prove}_i(\text{st}_{i-1,b}, \mathbf{h}_{i-1,b}, \mathbf{x}_b, \mathbf{w}_b)$ 
10    $\mathbf{h}_{i,b} := \mathbf{H}(\{\mathbf{R}_{j,b}\}_{j=1}^i, \mathbf{A}_{1-b}) + a_{i,b}$ 
11  $\mathbf{s}_b \xleftarrow{\$} \text{PCIP}_b.\text{Prove}_{n_b}(\text{st}_{n_b-1,b}, \mathbf{h}_{n_b-1,b}, \mathbf{x}_b, \mathbf{w}_b)$ 
12 return  $\pi := (\{\mathbf{R}_{i,0}\}_{i=1}^{n_0}, \{\mathbf{R}_{i,1}\}_{i=1}^{n_1}, \mathbf{A}_0, \mathbf{A}_1, \mathbf{s}_0, \mathbf{s}_1)$ 
Verif( $\mathbf{x}_0, \mathbf{x}_1, \pi$ ):
13 for  $i = 1..n_0$  do
14    $\mathbf{h}_{i,0} := \mathbf{H}(\{\mathbf{R}_{j,0}\}_{j=1}^i, \mathbf{A}_1) + a_{i,0}$ 
15 for  $i = 1..n_1$  do
16    $\mathbf{h}_{i,1} := \mathbf{H}(\{\mathbf{R}_{j,1}\}_{j=1}^i, \mathbf{A}_0) + a_{i,1}$ 
17  $\text{Trans}_0 := (\{\mathbf{R}_{i,0}, \mathbf{h}_{i,0}\}_{i=1}^{n_0}, \mathbf{s}_0)$ 
18  $\text{Trans}_1 := (\{\mathbf{R}_{i,1}, \mathbf{h}_{i,1}\}_{i=1}^{n_1}, \mathbf{s}_1)$ 
19 if  $\text{PCIP}_0.\text{Verify}(\mathbf{x}_0, \text{Trans}_0) = 1 \wedge \text{PCIP}_1.\text{Verify}(\mathbf{x}_1, \text{Trans}_1) = 1$  then
20   return 1
21 else return 0

```

**Fig. 5.** In this figure, we construct an NIP system  $\Pi = (\text{Setup}, \text{Prove}, \text{Verif})$ , which is an OR-composition to prove that  $\mathbf{x}_0 \in \mathcal{L}_0 \vee \mathbf{x}_1 \in \mathcal{L}_1$ . We recall that all challenge spaces are considered as an additive group. Namely, for all operations in the  $i$ -th round of  $\text{PCIP}_b$  are modulo  $\mathbb{Z}_{\ell_{i,b}}$ .

if  $\text{PCIP}_0$  and  $\text{PCIP}_1$  are both perfectly HVZK, then the resulting NIP is a NIWI proof with perfect witness-indistinguishability.

**Theorem 1 (Correctness).** *If  $\text{PCIP}_0$  and  $\text{PCIP}_1$  are both  $\rho$ -correct and  $\Delta$ -HVZK, then  $\Pi$  is  $2\rho + \Delta$ -correct.*

*Proof.* We can observe that in the resulting proof  $\pi$ , we have randomly chosen a bit  $b$ , and the proof  $\pi$  can be divided into two parts  $(\pi_0, \pi_1)$ , where  $\pi_b = (\{\mathbf{R}_{i,b}\}_{i=1}^{n_b}, \mathbf{A}_b, \mathbf{s}_b)$  is an honestly generated proof of  $\text{PCIP}_b$  with correctness error at most  $\rho$ , and  $\pi_{1-b}$  is a simulated transcript of  $\text{PCIP}_{1-b}$  with correctness error at most  $\rho + \Delta$ . Therefore, by the union bound over the correctness of  $\pi_0$  and  $\pi_1$ , we have  $\pi$  has correctness error at most  $2\rho + \Delta$ .  $\square$

**Theorem 2 (Witness-Indistinguishability).** *If  $\text{PCIP}_0$  and  $\text{PCIP}_1$  are two  $\Delta$ -HVZK  $(n_0, n_1)$ -rounds public-coin interactive proofs for the language  $\mathcal{L}_0$  and  $\mathcal{L}_1$  respectively, then  $\Pi$  is  $2\Delta$ -Witness-Indistinguishable. Namely, given a statement  $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1)$  such that  $\mathbf{x}_0 \in_{\mathbf{w}_0} \mathcal{L}_0 \wedge \mathbf{x}_1 \in_{\mathbf{w}_1} \mathcal{L}_1$ , the statistical distance between the proof generated using  $\mathbf{w}_0$  and the one generated using  $\mathbf{w}_1$  is at most  $2\Delta$ .*

**Theorem 3 (Adaptive Soundness).** For  $b \in \{0, 1\}$ , let  $\text{PCIP}_b$  be an  $n_b$ -round round-by-round  $\varepsilon'$ -sound interactive protocol, then  $\Pi$  is  $(t, \varepsilon, Q_H)$ -adaptively sound, where

$$t = \text{poly}(\lambda), \quad \varepsilon \leq (Q_H + 2n)^2 \cdot n \cdot \varepsilon',$$

with  $n = \max(n_0, n_1)$ .

*Proof.* Assuming  $\mathcal{A}$  a PPT adversary, running in polynomial time  $t$ , wins the adaptive soundness game within probability  $\varepsilon$  by generating a valid OR-proof  $\pi$  for  $(\mathbf{x}_0, \mathbf{x}_1)$  where  $\mathbf{x}_0 \notin \mathcal{L}_0$  and  $\mathbf{x}_1 \notin \mathcal{L}_1$ ,

$$\pi = (\{\mathbf{R}_{i,0}\}_{i=1}^{n_0}, \{\mathbf{R}_{i,1}\}_{i=1}^{n_1}, \mathbf{A}_0, \mathbf{A}_1, \mathbf{s}_0, \mathbf{s}_1).$$

Moreover, we can compute  $\mathbf{A}_0 = (a_{1,0}, \dots, a_{n_0,0})$ ,  $\mathbf{A}_1 = (a_{1,1}, \dots, a_{n_1,1})$ , and  $h_{i,b} = \text{H}(\{\mathbf{R}_{j,b}\}_{j=1}^i, \mathbf{A}_{1-b}) + a_{i,b}$ . We give the security proof via a sequence of games:

- **Game<sub>0</sub>** : The **Game<sub>0</sub>** is the original adaptive soundness game.
- **Game<sub>1</sub>** : In this game, we assume that for  $i_0 \in [n_0], i_1 \in [n_1]$ , all the queries of the form  $(\{\mathbf{R}_{i,0}\}_{j=1}^{i_0}, \mathbf{A}_1)$  and  $(\{\mathbf{R}_{i,1}\}_{j=1}^{i_1}, \mathbf{A}_0)$  have been queried to the random oracle. Remind that if the adversary  $\mathcal{A}$  does not fulfil this condition, we can construct a new adversary  $\mathcal{B}$  that additionally makes the above two queries with the same running time and winning probability against the adaptive soundness game. Therefore, we have  $\text{Adv}_0 = \text{Adv}_1$ , but the number of queries has slightly increased  $Q'_H = Q_H + n_0 + n_1$ .

*Analysis of the winning probability  $\text{Adv}_1$  of  $\mathcal{A}$  in **Game<sub>1</sub>**.* We define the bit  $b \in \{0, 1\}$  such that there is a random oracle query of the form  $(\cdot, \mathbf{A}_b)$  happens before any query of the form  $(\cdot, \mathbf{A}_{1-b})$ .

Since  $\pi$  is a valid proof, we have for  $i \in [n_b]$  that  $h_{i,b} = \text{H}(\{\mathbf{R}_{j,b}\}_{j=1}^i, \mathbf{A}_{1-b}) + a_{i,b}$ . Note that in the proof given by the adversary is of the form  $\pi = (\pi_0, \pi_1)$  where any query of the form  $(\cdot, \mathbf{A}_{1-b})$  happens after a query of the form  $(\cdot, \mathbf{A}_b)$ . Therefore, the adversary  $\mathcal{A}$  can only choose at most  $Q_H + 2n$  different offsets as  $\mathbf{A}_b$ . Moreover, for all  $i \in [n_b]$ , given  $\{\mathbf{R}_{j,b}\}_{j=1}^i$  and  $\mathbf{A}_b = (\{a_{j,b}\}_{j=1}^{n_b})$ , there are at most  $Q_H + 2n$  different challenge values  $h_{i,b} := \text{H}(\{\mathbf{R}_{j,b}\}_{j=1}^i, \mathbf{A}_{1-b}) + a_{i,b}$  depending on the choice of  $\mathbf{A}_{1-b}$ . Thus, the adversary has in total at most  $(Q_H + 2n)^2$  choices of  $h_{i,b}$ .

We emphasize that the output distribution of the random oracle is uniformly random. Therefore, the distribution of  $h_{i,b}$  conditioned on the choice of  $\mathbf{A}_b, \mathbf{A}_{1-b}$  is still uniformly random by using the One-Time Pad argument.

We recall that, for the round-by-round  $\varepsilon$ -soundness, for all  $j \in [n_b]$ , given the prover's messages  $(\{\mathbf{R}_{i,0}\}_{i=1}^j)$ , if the challenge is selected uniformly, the partial transcript has probability  $1 - \varepsilon$  to be "doomed". The adversary has  $(Q_H + 2n)^2$  choices over  $(\mathbf{A}_b, \mathbf{A}_{1-b})$ . On the other hand, the total transcript is in the "doomed set" with probability  $1 - (1 - \varepsilon')^n \leq n \cdot \varepsilon'$ . Therefore, we have that the success probability for the adversary in finding a pair of  $(\mathbf{A}_b, \mathbf{A}_{1-b})$  such that the transcript of the side  $b$  is not doomed is at most  $(Q_H + 2n)^2 \cdot n \cdot \varepsilon'$ .

Summarizing all the hybrid games, we have

$$t = \text{poly}(\lambda), \quad \varepsilon \leq (Q_H + 2n)^2 \cdot n \cdot \varepsilon'.$$

□

### 3.2 Adaptively sound Non-Interactive Zero-Knowledge Proof

We follow the same framework of [15] for defining a transform from  $n$ -round interactive proof systems to NIZK: we use our OR-composition in Section 3.1 to let the prover combine the interactive proof system with a proof of hard membership problem.

Since the transform of [15] (and ours) makes use of a membership-hard language  $\mathcal{L}$ , let us first define it in Definition 7.

**Definition 7 (NP membership problem[29]).** *A language  $\mathcal{L}$  is a  $(t, \varepsilon_{\mathcal{L}})$ -hard NP membership language if there exists a PPT sampler  $\mathcal{S} = (\mathcal{S}_0, \mathcal{S}_1)$  such that for every PPT distinguisher  $\mathcal{D}$ , running in polynomial time  $t$ , we have*

$$|\Pr[\mathcal{D}(\mathcal{S}_0(1^\lambda), 1^\lambda) = 1] - \Pr[\mathcal{D}(\mathcal{S}_1(1^\lambda), 1^\lambda) = 1]| \leq \varepsilon_{\mathcal{L}},$$

where  $\mathcal{S}$  behaves as follows

- $\mathcal{S}_0(1^\lambda)$  samples  $(\mathbf{x}_0, \mathbf{w}_0) \xleftarrow{\$} \mathcal{L}$ , and returns  $\mathbf{x}_0$ .
- $\mathcal{S}_1(1^\lambda)$  samples  $\mathbf{x}_1 \xleftarrow{\$} \{0, 1\}^\lambda \setminus \mathcal{L}$ , and returns  $\mathbf{x}_1$ .

**Transform from interactive to non-interactive.** Given a language  $\mathcal{L}_0$  and an instance  $\mathbf{x}_0 \in_{\mathbf{w}_0} \mathcal{L}_0$ , our goal is to prove that  $\mathbf{x}_0 \in \mathcal{L}_0$  without leaking any additional information about  $\mathbf{w}_0$ . We follow the same overall framework as [15] by adding a membership-hard language  $\mathcal{L}_1$  together with an instance  $\mathbf{x}_1 \in \mathcal{L}_1$ , then the NIZK proof consists of a proof that  $\mathbf{x}_0 \in \mathcal{L}_0 \vee \mathbf{x}_1 \in \mathcal{L}_1$ , and  $(\mathbf{x}_1, \mathcal{L}_1)$  is the CRS of the NIZK proof system. We give below some intuitions behind the soundness and the zero-knowledge property of this general construction.

- **Soundness:** As  $\mathcal{L}_1$  is a membership-hard problem, we can switch  $\mathbf{x}_1 \in_{\mathbf{w}_1} \mathcal{L}_1$  into  $\mathbf{x}'_1 \in \{0, 1\}^\lambda \setminus \mathcal{L}_1$  without the adversary noticing it. Since  $\mathbf{x}'_1 \in \{0, 1\}^\lambda \setminus \mathcal{L}_1$ , a valid proof  $\pi$  for the fact that  $\mathbf{x}_0 \in \mathcal{L}_0 \vee \mathbf{x}'_1 \in \mathcal{L}_1$  directly implies that  $\mathbf{x}_0 \in \mathcal{L}_0$ .
- **Zero-Knowledge:** We can simulate every proof using  $\mathbf{w}_1$  instead of  $\mathbf{w}_0$ . By the witness-indistinguishability of the OR-proof, this change is oblivious for the adversary. This proves the zero-knowledge property of the NIZK proof system.

Formally, let  $\text{PCIP}_0$  be a  $(k, \ell)$ -sound  $n_0$ -round interactive proof system for the NP language  $\mathcal{L}_0$ . We will consider a  $(t, \varepsilon_{\mathcal{L}})$ -hard NP membership  $\mathcal{L}_1$  and its associated interactive proof system  $\text{PCIP}_1$ . Let  $\Pi$  denote the NIWI scheme obtained by applying the OR-composition from Section 3.1 to  $\text{PCIP}_0$  and  $\text{PCIP}_1$ . We give the explicit transform from an IP protocol  $\text{PCIP}_0$  to a NIZK scheme  $\Sigma$  in Figure 6.

The correctness of  $\Sigma$  is straightforward from Theorem 1:

**Theorem 4 (Correctness).** *If  $\text{PCIP}_0$  and  $\text{PCIP}_1$  are both at least  $\rho$ -correct and  $\Delta$ -HVZK, then  $\Sigma$  is  $2\rho + \Delta$ -correct.*

**Theorem 5 (Zero-Knowledge).** *If  $\text{PCIP}_0$  and  $\text{PCIP}_1$  are both  $\Delta$ -HVZK multi-round  $(n_0, n_1)$  rounds respectively) interactive protocols, then  $\Sigma$  is  $2\Delta$ -Zero-Knowledge.*

*Proof.* Since we have  $\mathbf{x}_1 \in_{\mathbf{w}_1} \mathcal{L}_1$ , we can use  $\mathbf{w}_1$  to compute the NIWI proof, which simulates an honestly generated proof with statistical distance at most  $2\Delta$  by Theorem 2.  $\square$

$\text{Setup}(1^\lambda):$ 01 $(\mathbf{x}_1, \mathbf{w}_1) \xleftarrow{\$} \mathcal{L}_1$ 02 $\text{CRS} := \mathbf{x}_1$ 03 <b>return</b> CRS	$\text{Prove}(\text{CRS}, \mathbf{x}_0, \mathbf{w}_0):$ 04 $\pi \xleftarrow{\$} \Pi.\text{Prove}((\mathbf{x}_0, \text{CRS}), \mathbf{w}_0)$ 05 <b>return</b> $\pi$  $\text{Verif}(\text{CRS}, \mathbf{x}, \pi):$ 06 <b>return</b> $\Pi.\text{Verif}((\mathbf{x}, \text{CRS}), \pi)$
--	--

**Fig. 6.** Transform from an optimal-sound interactive protocol  $\text{PCIP}_0$  into adaptively sound NIZK scheme  $\Sigma$ .

**Theorem 6 (Adaptive Soundness).** For  $b \in \{0, 1\}$ , let  $\text{PCIP}_b$  be a  $\varepsilon_b$ -Round-By-Round sound  $n_b$ -round interactive protocol such that  $\text{PCIP}_1$  is the interactive proof associated to a  $(t', \varepsilon'_\mathcal{L})$ -hard NP membership language  $\mathcal{L}_1$ , then  $\Sigma$  is  $(t, \varepsilon, \mathbf{Q}_H)$ -adaptively sound, where

$$t \approx t', \quad \varepsilon \leq (\mathbf{Q}_H + 2n)^2 \cdot n \cdot \varepsilon' + \varepsilon'_\mathcal{L},$$

with  $\varepsilon' = \max(\varepsilon_0, \varepsilon_1)$  and  $n = \max(n_0, n_1)$ .

*Proof.* We will give a simple game-based proof of this theorem. There are only 2 hybrids described as in Figure 7.

$\text{Exp}_{\text{AdSnd}}(1^\lambda):$ 01 $(\mathbf{x}_1, \mathbf{w}_1) \xleftarrow{\$} \mathcal{L}_1$ 02 $\mathbf{x}_1 \xleftarrow{\$} \{0, 1\}^\lambda \setminus \mathcal{L}_1$ 03 $\text{CRS} := \mathbf{x}_1$ 04 $(\mathbf{x}^*, \pi^*) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{Hash}}(\text{CRS})}$ 05 <b>if</b> $\mathbf{x}^* \in \{0, 1\}^\lambda \setminus \mathcal{L}_0 \wedge \text{Verif}(\text{CRS}, \mathbf{x}^*, \pi^*) = 1$ <b>then</b> 06 <b>return</b> 1 07 <b>else return</b> 0	 // <b>Game</b> <sub>0</sub> // <b>Game</b> <sub>1</sub>	$\mathcal{O}_{\text{Hash}}(\mathbf{R}):$ 08 $\mathbf{h} \xleftarrow{\$} \mathcal{C}$ 09 <b>return</b> $\mathbf{h}$
---	--	--

**Fig. 7.** The security games for proving the adaptive soundness of  $\Sigma$ . The line commented with **Game** <sub>$i$</sub>  is the pseudo-code that only exists in  $i$ -th hybrid.

The **Game**<sub>0</sub> is the original security game for the adaptive soundness of  $\Sigma$ . In game **Game**<sub>1</sub>, the only difference is that  $\mathbf{x}_1$  in CRS is chosen from the set  $\{0, 1\}^\lambda \setminus \mathcal{L}_1$ . Therefore, we have

$$\text{Adv}_0 = \varepsilon, \quad |\text{Adv}_1 - \text{Adv}_0| \leq \varepsilon'_\mathcal{L}.$$

where  $\text{Adv}_0$  (respectively  $\text{Adv}_1$ ) is the advantage of  $\mathcal{A}$  in game **Game**<sub>0</sub> (respectively **Game**<sub>1</sub>). Moreover, in **Game**<sub>1</sub>, since  $\mathbf{x}_1$  is not in  $\mathcal{L}_1$  and  $\mathbf{x}_0$  is neither in  $\mathcal{L}_0$ ,  $\pi$  is a valid attack for the underlying NIWI scheme. Therefore, we have  $\text{Adv}_1 \leq (\mathbf{Q}_H + 2n)^2 \cdot n \cdot \varepsilon'$  from Theorem 3. Combining hybrids together we have  $t \approx t'$  and

$$\varepsilon \leq (\mathbf{Q}_H + 2n)^2 \cdot n \cdot \varepsilon' + \varepsilon'_\mathcal{L}.$$

□

## 4 Security of our Transform in the Quantum Random Oracle Model

In this section, we give a security proof of our OR-composition from two public-coin interactive proofs ( $n_0$ -round and  $n_1$ -round respectively) into one NIZK in the quantum random oracle model. Note that we can straightforwardly extend our proof in the QROM to our transform from PCIP to NIZK as described in Section 3.2.

While it is an important achievement to prove security in the QROM for post-quantum primitives, there is a price that one has to pay. One drawback is that there is a significant loss in the security argument. The second one is related to the programmability of the random oracle: proofs that were in the NPRM in the classical setting now need the quantum random oracle to be programmable in the security reduction. The last one is that we cannot prove our transform for round-by-round sound PCIP with acceptable security loss (polynomial in the number of rounds), due to the fact that we need to reprogram every round to fulfill a reduction, which introduces an exponential security loss in the number of rounds. Therefore, we limit our transform to optimal-sound PCIP protocols. Firstly, we introduce the notion of answerable challenge and provide the formal definition of optimal-soundness.

**Definition 8 (Answerable Challenges).** *Let  $\text{Ans}(\text{Trans}_i, h_i)$  be a function that takes a partial transcript until  $i$ -th round  $\text{Trans}_i = (\{R_j, h_j\}_{j=1}^{i-1}, R_i)$  and a challenge  $h_i$  as input, and returns 1 if there exists  $\text{Trans}' = (\{R_j, h_j\}_{j=i+1}^n, s)$  such that  $(\text{Trans}_i, h_i, \text{Trans}')$  is a valid transcript and 0 otherwise. We say that a challenge  $h_i$  is an **answerable challenge** for round  $i$  if  $\text{Ans}(\text{Trans}_i, h_i) = 1$ .*

*We emphasize that the function  $\text{Ans}$  can be a non-efficiently computable function here.*

**Definition 9 (Optimal Soundness).** *Let  $\mathcal{L}$  be an NP language, we say that PCIP is  $(k, \ell, i)$ -optimal sound if, for all statement not in the language  $x \notin \mathcal{L}$ , and for all partial transcripts  $\text{Trans}_i = (\{R_j, h_j\}_{j=1}^{i-1}, R_i)$  there exist at most  $k$  answerable challenges  $\{h_i^{(j)}\}_{j \in [k]}$  such that  $\text{Ans}(\text{Trans}_i, h_i^{(j)}) = 1$  for all  $j \in [k]$  and the size of the  $i$ -th challenge space is at least  $2^\ell$ .*

We note that, the optimal soundness is implied by the special soundness which is the case for most PCIP protocols. Moreover optimal soundness straightforwardly implies the negligible soundness, while the latter one is equivalent to the round-by-round soundness in our case. Thus, limiting our transform to the PCIPs with optimal soundness is indeed a restriction.

We will use the measure-and-reprogram 2.0 technique proposed in [19] and we apply it to our NIZK transform in the same way that [19] apply it for proving sequential-OR proof. Firstly, we give a quick overview of the measure-and-reprogram 2.0 technique proposed in [19].



**Measure-and-Reprogram 2.0, multiple input [19].** Let  $\mathcal{A}$  be a quantum adversary that has  $Q_H$  quantum queries to a random oracle  $H : \mathcal{X} \rightarrow \mathcal{Y}$ , where  $\mathcal{X}, \mathcal{Y}$  are both finite non-empty sets. Assuming that for a predicate (possibly quantum and not efficiently computable)  $\Gamma$ , the adversary  $\mathcal{A}$  can output in polynomial time  $t$  a transcript  $\text{Trans} = (X_0, \dots, X_{n-1}, z)$  such that  $\Gamma(\text{Trans}, H(X_0), \dots, H(X_{n-1})) = \text{True}$ .

The goal is to build a multi-stage simulator  $\mathcal{R}^{\mathcal{A}}$  such that stage by stage it outputs  $X_i$ 's and takes the corresponding  $\Theta_i$ 's as input and finally outputs a (possibly quantum)  $z$  such that for the same predicate we have  $\Gamma(X_0, \dots, X_{n-1}, z, \Theta_0, \dots, \Theta_{n-1}) = \text{True}$ .

Don et al. [19] showed the existence of a quantum adversary  $\mathcal{R}^{\mathcal{A}}$  that proceeds as follows: Firstly, it outputs a permutation  $\sigma$  together with a hash input  $x_{\sigma(0)}$  and it takes as input  $\Theta_{\sigma(0)}$  from a third party  $\mathcal{V}$ . Then for every stage  $0 < i \leq n-1$ ,  $\mathcal{R}^{\mathcal{A}}$  outputs a hash input  $x_{\sigma(i)}$  and it takes as input  $\Theta_{\sigma(i)}$  from  $\mathcal{V}$ . Finally, it outputs a possibly quantum  $z$ . We denote this procedure as  $(\sigma, \sigma(X), z) \stackrel{s}{\leftarrow} \langle \mathcal{R}^{\mathcal{A}}, \sigma(\Theta) \rangle$ , where  $X = (X_0, \dots, X_{n-1})$  and  $\Theta = (\Theta_0, \dots, \Theta_{n-1})$ . In the special case of PCIP protocols,  $\mathcal{V}$  refers to the verifier.

More precisely, we have the following theorem:

**Theorem 7 ([19, Theorem 6]).** *Let  $\mathcal{X}$  and  $\mathcal{Y}$  be the input and output sets of the hash function  $H : \mathcal{X} \rightarrow \mathcal{Y}$ . Let  $\mathcal{A}$  be a polynomial time oracle quantum algorithm that makes  $Q_H$  random oracle queries to  $H$  and outputs an  $n$ -dimensional vector  $X = (X_0, \dots, X_{n-1})$  and a possibly quantum  $z$ . There exists a  $(n+1)$ -stage quantum algorithm  $\mathcal{R}^{\mathcal{A}}$  that behaves as described above, satisfying the following property: For any  $X^* \in \mathcal{X}^n$  without duplicate entries and for any predicate (possibly quantum and not efficiently computable)  $\Gamma$ , and a third party  $\mathcal{V}$ , we have:*

$$\Pr \left[ \begin{array}{l} X = X^* \wedge \\ \Gamma(X, \Theta, z) \end{array} \middle| (\sigma, \sigma(X), z) \stackrel{s}{\leftarrow} \langle \mathcal{R}^{\mathcal{A}}, \sigma(\Theta) \rangle \right] \geq \frac{1}{(2Q_H + 1)^{2n}} \cdot \Pr \left[ \begin{array}{l} X = X^* \wedge \\ \Gamma(X, H(X), z) \end{array} \middle| (X, z) \stackrel{s}{\leftarrow} \mathcal{A}(1^\lambda) \right]. \quad (3)$$

**Application to our zero-knowledge proof.** Formally, given a  $n_0$ -round PCIP<sub>0</sub> and a  $n_1$ -round PCIP<sub>1</sub>, for languages  $\mathcal{L}_0$  and  $\mathcal{L}_1$  respectively. We proposed a non-interactive proof of the form  $\pi_{\mathcal{V}} = (A_0, A_1, \{R_{i,0}\}_{i=0}^{n_0}, \{R_{i,1}\}_{i=1}^{n_1}, s_0, s_1)$  for the language  $\mathcal{L}_{\mathcal{V}} = \{(x_0, x_1) : x_0 \in \mathcal{L}_0 \vee x_1 \in \mathcal{L}_1\}$ .

We assume that for  $b \in \{0, 1\}$ , the interactive protocol PCIP<sub>b</sub> is  $(k_b, \ell_b, i_b)$ -optimal sound, and we have  $i_b^*$  such that given the first  $i_b^*$  elements  $R_{1,b}, \dots, R_{i_b^*,b}$ , there are only  $k_b$  answerable challenges. This property is captured by the answerable predicates given in the optimal soundness  $\text{Ans}_b(R_{1,b}, \dots, R_{i_b^*,b}, h_{i_b^*,b}^*)$ .

**Theorem 8.** *For  $b \in \{0, 1\}$ , let PCIP<sub>b</sub> be a  $(k, \ell, i_b)$ -optimal sound  $n_b$ -round interactive protocol. Let  $\Pi_{\mathcal{V}}$  be the non-interactive zero-knowledge proof given by applying our transform in Section 3.1. Any quantum adversary  $\mathcal{A}$  running in time  $t$ , making  $Q_H$  quantum random oracle, breaks the adaptive soundness of  $\Pi_{\mathcal{V}}$  with probability at most  $\frac{k}{2^{\ell}} \cdot (2Q_H + 1)^4$ .*

*Proof.* Assuming  $\mathcal{A}$  is a quantum adversary making  $Q_H$  quantum random oracle queries against the adaptive soundness of  $\Pi_{\mathcal{V}}$ . By the definition of adaptive soundness, given

two false statements  $\mathbf{x}_0 \notin \mathcal{L}_0$  and  $\mathbf{x}_1 \notin \mathcal{L}_1$ ,  $\mathcal{A}$  can generate a valid proof  $\pi_\vee = (A_0, A_1, \{\mathbf{R}_{i,0}\}_{i=1}^{n_0}, \{\mathbf{R}_{i,1}\}_{i=1}^{n_1}, s_0, s_1)$  with non-negligible advantage. For simplicity, we denote the challenge by,

$$h_{i,b} := H(\{\mathbf{R}_{j,b}\}_{j=1}^i, A_{1-b}) + a_{i,b}. \quad (4)$$

Note that, in our non-interactive proof construction  $h_{i,b}$  is used as the challenges in the underlying interactive protocols. Since  $\pi_\vee$  is a valid proof, for  $b \in \{0, 1\}$ , and  $i \in [n_b]$ , we have  $\text{Ans}_b(\{\mathbf{R}_{j,b}\}_{j=1}^i, h_{j,b}) = \text{True}$ .

For our convenience, we will consider an adversary  $\mathcal{A}'$  that proceeds exactly like  $\mathcal{A}$ , except that it only outputs a partial proof  $\pi' = (\{\mathbf{R}_{i,0}\}_{i=1}^{i_0^*}, A_1, \{\mathbf{R}_{i,1}\}_{i=1}^{i_1^*}, A_0)$ . For more compact notation, we denote  $\mathbf{X}_b = (\{\mathbf{R}_{i,b}\}_{i=1}^{i_b^*}, A_{1-b})$  for  $b \in \{0, 1\}$ . We also define a predicate  $\Gamma$  as follows:

$$\Gamma((\mathbf{X}_0, \mathbf{X}_1), (H(\mathbf{X}_0), H(\mathbf{X}_1))) = \text{Ans}_0(\{\mathbf{R}_{i,0}\}_{i=1}^{i_0^*}, h_{i_0^*,0}^*) \wedge \text{Ans}_1(\{\mathbf{R}_{i,1}\}_{i=1}^{i_1^*}, h_{i_1^*,1}^*).$$

Here, we recall that  $h_{i_b^*,b}^*$  can be computed by using  $\pi'$ ,  $H(\mathbf{X}_0)$ ,  $H(\mathbf{X}_1)$  as in Equation (4). By the definition of the answerable challenge predicate, assuming a valid proof  $\pi_\vee$ , the corresponding partial proof  $\pi' = (\mathbf{X}_0, \mathbf{X}_1)$  verifies that  $\Gamma((\mathbf{X}_0, \mathbf{X}_1), (H(\mathbf{X}_0), H(\mathbf{X}_1))) = \text{True}$ .

Now, it is easy to see that  $(\mathcal{A}', \Gamma)$  fits into the requirement of Theorem 7. By simply applying Theorem 7, for all  $(\mathbf{X}_0^*, \mathbf{X}_1^*)$ , two uniformly chosen  $\Theta_0, \Theta_1$  and two instances  $(\mathbf{x}_0, \mathbf{x}_1)$ , we have an adversary  $\mathcal{B}$  such that:

$$\begin{aligned} & \Pr \left[ \begin{array}{l} \mathbf{X}_0 = \mathbf{X}_0^* \wedge \\ \mathbf{X}_1 = \mathbf{X}_1^* \wedge \\ \Gamma((\mathbf{X}_0, \mathbf{X}_1), (\Theta_0, \Theta_1)) \end{array} \middle| (\sigma, \sigma(\mathbf{X}_0, \mathbf{X}_1), \perp) \stackrel{\$}{\leftarrow} \langle \mathcal{B}(\mathbf{x}_0, \mathbf{x}_1), \sigma(\Theta_0, \Theta_1) \rangle \right] \\ & \geq \frac{1}{(2Q_H + 1)^4} \cdot \Pr \left[ \begin{array}{l} \mathbf{X}_0 = \mathbf{X}_0^* \wedge \\ \mathbf{X}_1 = \mathbf{X}_1^* \wedge \\ \Gamma((\mathbf{X}_0, \mathbf{X}_1), (H(\mathbf{X}_0), H(\mathbf{X}_1))) \end{array} \middle| \begin{array}{l} (\mathbf{X}_0, \mathbf{X}_1, \perp) \\ \stackrel{\$}{\leftarrow} \mathcal{A}^H(\mathbf{x}_0, \mathbf{x}_1) \end{array} \right]. \quad (5) \end{aligned}$$

In the final step, we will construct an adversary  $\mathcal{C}$  that helps us to choose  $(\Theta_0, \Theta_1)$ . More precisely, we describe the behavior of  $\mathcal{C}$  as in Figure 8.

Note that the left side of Equation (5) can be bounded by  $\frac{k}{2^\ell}$ . More precisely, since we have  $\Gamma((\mathbf{X}_0, \mathbf{X}_1), (\Theta_0, \Theta_1)) = \text{True}$ , we have also  $\text{Ans}_b(\mathbf{X}_b, h_b) = \text{True}$ . But, the challenge  $h_b$  is chosen uniformly random by an honest verifier  $\text{Verifier}_b$  in line 09 Figure 8. Therefore  $\Pr[\text{Ans}_b(\mathbf{X}_b, h_b)] \leq \frac{k}{2^\ell}$  by the optimal soundness. Combining this upper bound with Equation (5), we have the probability of  $\mathcal{A}$  breaking the adaptive soundness of  $\Pi_\vee$  is at most  $\frac{k}{2^\ell} \cdot (2Q_H + 1)^4$ .  $\square$

## Acknowledgement

We thank the anonymous reviewers of Asiacrypt 2022 and PKC 2023 for their many insightful suggestions to improve our paper.

This work is supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704702), the Major Basic Research Project of Natural Science Foundation of Shandong Province, China (Grant No. ZR202010220025).

$\mathcal{C}(x \notin \mathcal{L})$ : 01 $(\sigma, X_{\sigma(0)}, \text{st}) \stackrel{\$}{\leftarrow} \mathcal{B}_1(x_0, x_1)$ 02 $b \leftarrow \sigma(1)$ 03 $\mathbf{x}_b := \mathbf{x}; \mathcal{L}_b := \mathcal{L}; \text{Verifier}_b := \text{Verifier}$ 04 $\mathbf{x}_{1-b} \stackrel{\$}{\leftarrow} \{0, 1\}^*; \mathcal{L}_{1-b} \stackrel{\$}{\leftarrow} \{0, 1\}^*$ 05 $\Theta_{\sigma(0)} \stackrel{\$}{\leftarrow} \mathcal{Y}$ 06 $(X_{\sigma(1)}, \text{st}) \stackrel{\$}{\leftarrow} \mathcal{B}_2(\Theta_{\sigma(0)}, \text{st})$ 07 <b>parse</b> $(R_{1,\sigma(1)}, \dots, R_{i_{\sigma(1)},\sigma(1)}, A_{\sigma(1)}) =: X_{\sigma(1)}$ 08 <b>parse</b> $(a_{1,\sigma(1)}, \dots, a_{n_{\sigma(1)},\sigma(1)}) =: A_{\sigma(1)}$ 09 $h_{\sigma(1)} \stackrel{\$}{\leftarrow} \text{Verifier}_{\sigma(1)}(X_{\sigma(1)})$ 10 $\Theta_{\sigma(1)} := h_{\sigma(1)} - a_{i_{\sigma(1)},\sigma(1)}$ 11 $\perp \stackrel{\$}{\leftarrow} \mathcal{B}_3(\Theta_{\sigma(1)}, \text{st})$ 12 <b>return</b> $(X_{\sigma(1)}, h_{\sigma(1)}, \Theta_0, \Theta_1)$
---

**Fig. 8.** Assuming PCIP<sub>0</sub> and PCIP<sub>1</sub> are  $(k, \ell, i)$ -optimal sound, we give the description of the adversary  $\mathcal{C}$  which interacts with the verifier Verifier of the underlying PCIP. Note that  $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$  is a 3-stage algorithm with an internal state st.

This work is also supported by the PEPR quantique France 2030 programme (ANR-22-PETQ-0008), and by the ANR ASTRID project AMIRAL (ANR-21-ASTR-0016). This work was carried out in the context of Beyond5G, a project funded by the French government as part of the economic recovery plan, namely "France Relance", and the investments for the future program. Adela Georgescu was partly funded by the Direction Générale de l'Armement (Pôle de Recherche CYBER), with the support of Région Bretagne.

## References

1. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 415–432. Springer, Heidelberg, December 2002.
2. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.
3. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006.
4. Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. More efficient amortization of exact zero-knowledge proofs for LWE. In Elisa Bertino, Haya Shulman, and Michael Waidner, editors, *ESORICS 2021, Part II*, volume 12973 of *LNCS*, pages 608–627. Springer, Heidelberg, October 2021.
5. Jonathan Bootle, Vadim Lyubashevsky, and Gregor Seiler. Algebraic techniques for short(er) exact lattice-based zero-knowledge proofs. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 176–202. Springer, Heidelberg, August 2019.

6. Zvika Brakerski, Venkata Koppula, and Tamer Mour. NIZK from LPN and trapdoor hash via correlation intractability for approximable relations. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 738–767. Springer, Heidelberg, August 2020.
7. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy*, pages 315–334. IEEE Computer Society Press, May 2018.
8. Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. Fiat-Shamir: from practice to theory. In Moses Charikar and Edith Cohen, editors, *51st ACM STOC*, pages 1082–1090. ACM Press, June 2019.
9. Ran Canetti, Yilei Chen, Leonid Reyzin, and Ron D. Rothblum. Fiat-Shamir and correlation intractability from strong KDM-secure encryption. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 91–122. Springer, Heidelberg, April / May 2018.
10. Ran Canetti, Oded Goldreich, and Shai Halevi. On the random-oracle methodology as applied to length-restricted signature schemes. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 40–57. Springer, Heidelberg, February 2004.
11. Dario Catalano and Ivan Visconti. Hybrid commitments and their applications to zero-knowledge proof systems. *Theor. Comput. Sci.*, 374(1-3):229–260, 2007.
12. David Chaum. Blind signature system. In David Chaum, editor, *CRYPTO’83*, page 153. Plenum Press, New York, USA, 1983.
13. Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. SOFIA:  $\mathcal{MQ}$ -based signatures in the QROM. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part II*, volume 10770 of *LNCS*, pages 3–33. Springer, Heidelberg, March 2018.
14. Yilei Chen, Alex Lombardi, Fermi Ma, and Willy Quach. Does fiat-shamir require a cryptographic hash function? In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part IV*, volume 12828 of *LNCS*, pages 334–363, Virtual Event, August 2021. Springer, Heidelberg.
15. Michele Ciampi, Giuseppe Persiano, Luisa Siniscalchi, and Ivan Visconti. A transform for NIZK almost as efficient and general as the Fiat-Shamir transform without programmable random oracles. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 83–111. Springer, Heidelberg, January 2016.
16. Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In Yvo Desmedt, editor, *CRYPTO’94*, volume 839 of *LNCS*, pages 174–187. Springer, Heidelberg, August 1994.
17. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *EUROCRYPT’97*, volume 1233 of *LNCS*, pages 103–118. Springer, Heidelberg, May 1997.
18. Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Non-interactive zero-knowledge proof systems. In Carl Pomerance, editor, *CRYPTO’87*, volume 293 of *LNCS*, pages 52–72. Springer, Heidelberg, August 1988.
19. Jelle Don, Serge Fehr, and Christian Majenz. The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 602–631. Springer, Heidelberg, August 2020.
20. Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

21. Muhammed F. Esgin, Ngoc Khanh Nguyen, and Gregor Seiler. Practical exact proofs from lattices: New techniques to exploit fully-splitting rings. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 259–288. Springer, Heidelberg, December 2020.
22. Uriel Feige, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In Alfred Aho, editor, *19th ACM STOC*, pages 210–217. ACM Press, May 1987.
23. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.
24. Marc Fischlin, Patrick Harasser, and Christian Janson. Signatures from sequential-OR proofs. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 212–244. Springer, Heidelberg, May 2020.
25. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987.
26. Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.
27. Shuichi Katsumata. A new simple technique to bootstrap various lattice zero-knowledge proofs to QROM secure NIZKs. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part II*, volume 12826 of *LNCS*, pages 580–610, Virtual Event, August 2021. Springer, Heidelberg.
28. Sam Kim and David J. Wu. Multi-theorem preprocessing NIZKs from lattices. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 733–765. Springer, Heidelberg, August 2018.
29. Yehuda Lindell. An efficient transform from sigma protocols to NIZK with a CRS and non-programmable random oracle. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 93–109. Springer, Heidelberg, March 2015.
30. Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, August 2019.
31. Alex Lombardi, Willy Quach, Ron D. Rothblum, Daniel Wichs, and David J. Wu. New constructions of reusable designated-verifier NIZKs. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 670–700. Springer, Heidelberg, August 2019.
32. Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, December 2009.
33. Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.
34. Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 89–114. Springer, Heidelberg, August 2019.
35. Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. The first collision for full SHA-1. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 570–596. Springer, Heidelberg, August 2017.
36. Marc Stevens, Arjen K. Lenstra, and Benne de Weger. Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In Moni Naor, editor, *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 1–22. Springer, Heidelberg, May 2007.

37. Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 755–784. Springer, Heidelberg, April 2015.
38. Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 19–35. Springer, Heidelberg, May 2005.