Non-interactive Zaps of Knowledge

Georg Fuchsbauer[1,2](✉) and Michele Orrù[1,2](✉)

[1] Inria, Paris, France
[2] École normale supérieure, CNRS, PSL University, Paris, France
{georg.fuchsbauer,michele.orru}@ens.fr

Abstract. While non-interactive zero-knowledge (NIZK) proofs require trusted parameters, Groth, Ostrovsky and Sahai constructed non-interactive witness-indistinguishable (NIWI) proofs without any setup; they called their scheme a non-interactive zap. More recently, Bellare, Fuchsbauer and Scafuro investigated the security of NIZK in the face of parameter subversion and observe that NI zaps provide subversion-resistant soundness and WI.

Arguments of knowledge prove that not only the statement is true, but also that the prover knows a witness for it, which is essential for anonymous identification. We present the first NIWI argument of knowledge *without* parameters, i.e., a NI zap of knowledge. Consequently, our scheme is also the first subversion-resistant knowledge-sound proof system, a notion recently proposed by Fuchsbauer.

Keywords: Non-interactive proofs · Argument of knowledge
Subversion resistance

1 Introduction

The concept of zero-knowledge proof systems, first proposed by Goldwasser et al. [GMR89], is a central tool in modern cryptography. Consider an NP relation R which defines the language of all statements x for which there exists a witness w so that $R(x, w) = \mathbf{true}$. In a zero-knowledge proof for R a prover, knowing a witness, wants to convince a verifier that x is in the language. The protocol must be *complete*, that is, if the prover knows a witness for x then it can convince the verifier; it should be *sound*, in that no malicious prover can convince the verifier of a false statement, and *zero-knowledge*: the execution of the protocol reveals no information to the verifier (beyond the fact that x is in the language).

Feige and Shamir [FS90] proposed a relaxation of zero-knowledge called *witness indistinguishability*, which only requires that it is indistinguishable which witness was used to compute a proof. This notion turns out to be sufficient in many contexts. *Non-interactive* zero-knowledge proofs (NIZK) [BFM88] allow the prover to convince the verifier by only sending a single message. However, they rely on the existence of a common-reference string (CRS) to which prover and verifier have access. The CRS is assumed to have been set up by some

B. Preneel and F. Vercauteren (Eds.): ACNS 2018, LNCS 10892, pp. 44–62, 2018.
https://doi.org/10.1007/978-3-319-93387-0_3

trusted party, which represents a serious limitation for all applications of NIZK in scenarios where parties mutually distrust each other.

Dwork and Naor [DN00] constructed a two-round witness-indistinguishable proof system for NP in the plain model, that is, where no trusted CRS is assumed. In their protocol the first message (sent from the verifier to the prover) can be fixed once and for all, and the second one provides the actual proof. They called such protocols *zaps*. Barak et al. [BOV03] introduced the concept of *non-interactive* zaps, where the prover sends a single message to deliver the proof. Non-interactive zaps are thus non-interactive proof systems *without* a CRS. Since in this scenario it is impossible to achieve zero-knowledge [GO94], witness indistinguishability (WI) is the best one can hope for. Groth, Ostrovsky, and Sahai constructed the first non-interactive zaps from standard assumptions [GOS06a]. Subsequently [GOS06a], there have been many works extending this line of research [BW06, BW07, Gro06].

All aforementioned schemes guarantee that proofs can only be computed for valid statements. Arguments of knowledge are proof systems that satisfy a stronger notion of soundness. They require the prover to *know* a witness for the proved statement. This is formalized via the notion of knowledge soundness that demands that for each prover there exists an efficient extractor which can extract a witness from the prover whenever the latter outputs a valid proof. (When this holds for computationally bounded provers only, we speak of *arguments* rather than proofs.) Since, by definition, false statements have no witnesses, knowledge soundness implies the standard notion of (computational) soundness.

Succinct non-interactive arguments of knowledge (SNARKs) are non-interactive proof systems with short (that is, independent of the size of the statement or the witness) efficiently verifiable proofs that satisfy knowledge soundness. SNARKs were initially introduced for verifiable computation and are now the most widely deployed proof systems in the real world. They are used in cryptocurrencies such as Zcash [BCG+14], which guarantees anonymity via zero-knowledge SNARKs. As for all NIZK systems, a drawback of SNARKs is that they require a CRS, that is, they require a one-time trusted setup of public parameters. Since for SNARKs every CRS has a simulation trapdoor, subversion of these parameters leads to full compromise of soundness.

Subversion Resistance. Motivated by the subversion of trusted public parameters in standardized cryptographic protocols led by mass-surveillance activities, Bellare et al. [BFS16] investigate what security properties can be maintained for NIZK when its trusted parameters are subverted. CRS's for NIZK are especially easy to subvert, since they must be subvertible by design: zero knowledge requires that an honest CRS must be indistinguishable from a backdoored one, where the backdoor is the trapdoor used to simulate proofs.

Bellare et al. defined multiple security properties that protect against parameter subversion: subversion soundness (S-SND) means that no adversary can generate a malicious CRS together with a valid proof for a false statement; subversion zero knowledge (S-ZK) requires that even if the adversary sets up the CRS, there exists a simulator able to produce its full view; and subversion witness indistinguishability (S-WI) formalizes that even for proofs that were made under a subverted CRS, it is still infeasible to tell which of two witnesses was used.

Following Goldreich and Oren [GO94], Bellare et al. [BFS16] also showed that it is impossible to achieve subversion soundness and (standard) zero-knowledge simultaneously. For subversion-sound proof systems, subversion witness indistinguishability is thus the best one can hope for. The authors [BFS16] observe that since proof systems that do not rely on a CRS cannot succumb to CRS-subversion attacks, non-interactive zaps [GOS06a] achieve both S-SND and S-WI.

Bellare et al. did not consider the stronger notion of knowledge soundness, which is the notion achieved by SNARKs, and which in many applications is the required notion for the used proof systems. For example, for all kinds of anonymous authentication, users prove knowledge of signatures (often called *certificates* or *credentials*, depending on the context); in this case soundness is not sufficient, as signatures always exist, but in the security proof they must actually be extracted in order to rely on their unforgeability. Fuchsbauer [Fuc18] has recently defined a subversion-resistant notion of knowledge soundness but left it open to give a scheme that achieves it. Such a scheme would protect against possible parameter subversion in any context where proving knowledge of a witness is required.

Our Contribution. Our result can be summarized as follows:

(i) We provide the first non-interactive zap with knowledge soundness; that is, a witness-indistinguishable proof system without parameters for which there exists an extractor that recovers a witness from every valid proof.

(ii) Our zap is also the first fully subversion-resistant WI argument-of-knowledge system. In particular, it satisfies the recently defined notion of subversion knowledge soundness [Fuc18], as well as subversion witness indistinguishability [BFS16] (the strongest notion compatible with S-SND).

Bellare et al. [BFS16] introduce a new type of knowledge-of-exponent assumption, which they call DH-KE. They prove (standard) soundness and subversion zero knowledge of their main construction under DH-KE and the decision linear assumption (DLin) [BBS04]. Our construction builds on the DLin-based non-interactive zap from [GOS06a], whose soundness we upgrade to knowledge soundness, assuming DH-KE. As for this zap, the language of our proof system is circuit satisfiability and thus universal. Groth et al. [GOS06a] starting point is a “dual-mode” [GOS06b, PVW08] non-interactive proof system, for which there are two indistinguishable types of CRS: one leading to proofs that are perfectly sound and the other leading to proofs that are perfectly WI. To construct a non-interactive zap, they let the prover choose the CRS. As the prover could choose a CRS that leads to “unsound” proofs, the prover must actually choose two CRS’s that are related in a way that guarantees that at least one of them is of the “sound” type. It must then provide a proof of the statement under both of them. The authors [GOS06a] then show that this protocol still achieves computational WI.

We turn their construction into a proof of knowledge by again doubling the proof, thereby forcing the prover to prove knowledge of a trapdoor which allows to extract the witness from one of the sound proofs. We prove our non-interactive zap of knowledge secure under the same assumptions as Bellare et al.'s S-ZK+SND scheme. Our result is summarized in the following theorem.

Theorem 1. *Assuming DLin and DH-KE, there exists a non-interactive zap for circuit satisfiability that satisfies knowledge soundness. The proof size is $O(\lambda k)$, where λ is the security parameter and k is the size of the circuit.*

Let us finally note that our system also implies a proof system which achieves (standard) knowledge soundness, (standard) zero knowledge and *subversion* witness indistinguishability. This is obtained by plugging our zap of knowledge into the construction by Bellare et al. [BFS16] that achieves SND, ZK and S-WI.

Their scheme uses a length-doubling pseudorandom generator (PRG) and a CRS contains a random bit string σ of length 2λ (where λ is the security parameter). A proof for statement x is a zap for the following statement: either x is a valid statement or σ is in the range of the PRG. Using a zap of knowledge (ZaK), knowledge soundness follows from knowledge soundness of the ZaK since with overwhelming probability σ is *not* in the range of the PRG. (The extractor must thus extract a witness for x.) Zero knowledge follows from WI of the zap, as after replacing σ with an element in the range of the PRG, proofs can be simulated using a preimage of σ. Finally, S-WI follows from S-WI of the zap.

Related Work. Since the introduction of non-interactive zaps [BOV03, GOS06a], a number of papers have studied and provided different (and more efficient) implementations of zaps. Groth and Sahai [GS08] provided a more general framework for NIWI and NIZK proofs, which leads to more efficient proofs for concrete languages (instead of circuit satisfiability). Furthermore, their proof system can also be based on other assumptions apart from DLin, such as SXDH, allowing for shorter proofs.

Bitanski and Paneth [BP15] presented a different approach to constructing zaps and WI proofs based on indistinguishability obfuscation (iO), but constructions using iO are only of theoretical interest. Ràfols [Ràf15] showed how to base non-interactive zaps on Groth-Sahai proofs, thereby achieving an improvement in efficiency (by a constant factor) over the original construction [GOS06a]. Her construction can be implemented in asymmetric ("Type-1") pairing groups.

Her scheme can also serve as the starting point for a scheme achieving knowledge soundness and we explore this in the full version [FO18]. (See Table 1 for an overview.) Although this scheme is more efficient, we decided to concentrate on building a scheme from [GOS06a], as we can prove it secure under the assumptions that underlie Bellare et al.'s [BFS16] SND+S-ZK scheme; in contrast, a scheme built on asymmetric bilinear groups would require an analogue of the DH-KE assumption in such groups (we refer to it as ADH-KE in [FO18]). This is a qualitatively different assumption, as without a symmetric pairing it cannot be checked whether the triple returned by the adversary is of the right form (see Fig. 3); it would thus not be efficiently decidable if an adversary has won

Table 1. Efficiency and security of the original zaps and our constructions of zaps of knowledge, where w is the number of wires, g the number of gates and $|\mathbb{G}|$ is the size of an element of a group $\mathbb{G}$.

Protocol	Efficiency	Assumptions
Zap [GOS06a]	$(18w + 12g + 5)\,|\mathbb{G}|$	DLin
Zap of knwlg, Sect. 5	$(36w + 24g + 14)\,|\mathbb{G}|$	DLin, DH-KE
Zap [Ràf15] (of knwlg; [FO18])	$(12w + 8g + 3)\,(|\mathbb{G}_1| + |\mathbb{G}_2|)$	SXDH (ADH-KE)

the game. Finally, our main scheme achieves *tight* security, whereas our proof of knowledge soundness with asymmetric pairings (which we present in the full version [FO18]) has a security loss that is linear in the circuit size.

2 Preliminaries

Notation. Let λ be the security parameter. We let $\mathsf{M.rl}(\lambda)$ be a *length function* in λ defining the length of the randomness for a probabilistic machine M. When sampling the value a uniformly at random from the set S, we write $a \leftarrow_{\$} S$. When sampling the value a from the probabilistic algorithm M, we write $a \leftarrow \mathsf{M}$. We use $:=$ to denote assignment. Elements of $\mathbb{Z}_p$ are denoted in lower case, group elements are denoted with capital letters. We employ additive notation for groups. Let R be a relation between statements denoted by ϕ and witnesses denoted by w. By $\mathsf{R}(\phi)$ we denote the set of possible witnesses for the statement ϕ in R. We let $\mathcal{L}(\mathsf{R}) := \{\phi : \mathsf{R}(\phi) \neq \emptyset\}$ be the *language* associated to R.

We consider the language of circuit satisfiability, which is NP-complete. For a binary circuit $\mathtt{C}$, the set $\mathsf{R}(\mathtt{C})$ is the set of inputs w that satisfy $\mathtt{C}(w) = 1$. Without loss of generality, we assume that circuits consist solely of NAND gates. Unless otherwise specified, all following algorithms are assumed to be randomized and to run in time $\mathsf{poly}(\lambda)$. As Bellare et al. [BFS16], who follow [Gol93], we only consider uniform machines to model the adversary A and the extractor Ext. (See [BFS16, Fuc18] for discussions on how this choice affects the hardness assumptions and security guarantees.)

Bilinear Groups. Throughout this work, we make use of prime-order abelian groups equipped with a (symmetric) bilinear map. Concretely, we assume the existence of groups $\mathbb{G}, \mathbb{G}_T$ of odd prime order p of length λ and an efficiently computable non-degenerate bilinear map $e \colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. That is, the map e is such that for all $U, V \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p : e(aU, bV) = ab \cdot e(U, V)$, and if U is a generator of $\mathbb{G}$, then $e(U, U)$ is a generator of $\mathbb{G}_T$. We say that a bilinear group is *verifiable* if there exists an efficient verification algorithm that outputs **true** if and only if $\Gamma = (p, \mathbb{G}, \mathbb{G}_T, e)$ is the description of a bilinear group. For instance, the elliptic-curve group of [BBS04] equipped with the Weil pairing is publicly verifiable. In most practical scenarios, the group description is embedded as a part of the protocol specification and agreed upon in advance; in these cases there is no need for verification.

Throughout this paper, we assume the existence of a deterministic algorithm G that, given as input the security parameter in unary 1^λ, outputs a bilinear group description Γ. The same assumption was already employed by Bellare et al. [BFS16]. The main advantage in choosing G to be deterministic is that every entity in the scheme can (re)compute the group from the security parameter, and no party must be trusted with generating the group. Moreover, real-world pairing schemes are defined for groups that are fixed for some λ. For the sake of simplicity, we define all our schemes w.r.t. a group description Γ and assume that the security parameter ($\lambda \in \mathbb{N}$ such that $\Gamma := \mathsf{G}(1^\lambda)$) can be derived from Γ.

Extractable Commitment Schemes. A commitment scheme Com consists of the following three algorithms:

- $(\sigma, \tau) \leftarrow \mathsf{Com.K}(\Gamma)$, the key generation algorithm, outputs a CRS σ together with the trapdoor information τ.
- $(C, r) \leftarrow \mathsf{Com.C}(\sigma, v)$, the commitment algorithm, outputs a commitment C to the given value v together with the *opening information* r.
- *bool* $\leftarrow \mathsf{Com.O}(\sigma, C, v, r)$, the opening algorithm, outputs **true** if C is a commitment to v witnessed by r, and **false** otherwise.

In our case, $\mathsf{Com.C}$ returns the used randomness and $\mathsf{Com.O}$ simply recomputes the commitment and checks that $C = \mathsf{Com.C}(V; r)$. Consequently, *correctness* of the scheme is trivial. To ease notation for commitments and openings, we will always assume that the group description Γ can be deduced from σ, and omit the opening information from the returned value.

Generally, we require commitment schemes to be *hiding* and *binding*. Loosely speaking, a scheme is *hiding* if the commitment C reveals no information about v. A scheme is *binding* if a cheating committer cannot change its mind about the value it committed to. Formally, it is hard to find C, v, r, v' and r' such that $v \neq v'$ and $\mathsf{Com.O}(\sigma, C, v, r) = \textbf{true} = \mathsf{Com.O}(\sigma, C, v', r')$.

We also require a perfectly binding commitment scheme to be *extractable*, that is, Com is equipped with an efficient extraction algorithm $\mathsf{Com.E}$ that, given as input the trapdoor information τ, recovers the value v to which C is bound.

Proof Systems. A non-interactive proof system $\mathsf{\Pi}$ for a relation R consists of the following three algorithms:

- $(\sigma, \tau) \leftarrow \mathsf{\Pi.K}(\Gamma)$, the CRS generation algorithm that outputs a CRS σ (and possibly some trapdoor information τ). Since we are dealing with *publicly verifiable protocols*, the trapdoor information τ will be omitted in most cases and used solely in the proofs or when combining protocols.
- $\pi \leftarrow \mathsf{\Pi.P}(\sigma, \phi, w)$, a prover which takes as input some $(\phi, w) \in \mathsf{R}$ and a CRS σ, and outputs a proof π.
- *bool* $\leftarrow \mathsf{\Pi.V}(\sigma, \phi, \pi)$ a verifier that, given as input a statement ϕ together with a proof π outputs **true** or **false**, indicating acceptance of the proof.

```
Game $\mathrm{WI}_{\mathsf{\Pi,R,A}}(\lambda)$
$b \leftarrow_\$ \{0,1\}\,;\ \mathit{\Gamma} := \mathsf{G}(1^\lambda)$
$(\sigma, \tau) \leftarrow \mathsf{\Pi.K}(\mathit{\Gamma})$
$b' \leftarrow \mathsf{A}^{\textsc{Prove}}(\sigma)$
$\textbf{return}\ (b = b')$
```

```
Oracle $\textsc{Prove}(\phi, w_0, w_1)$
$\textbf{if}\ \mathsf{R}(\phi, w_0) = \textbf{false}\ \vee\ \mathsf{R}(\phi, w_1) = \textbf{false}$
    $\textbf{return}\ \perp$
$\pi \leftarrow \mathsf{\Pi.P}(\sigma, \phi, w_b)$
$\textbf{return}\ \pi$
```

Fig. 1. Witness indistinguishability (WI) game.

A proof is complete if every correctly generated proof verifies. If the CRS is clear from the context, we omit σ from the arguments of $\mathsf{\Pi.P}$ or $\mathsf{\Pi.V}$.

Zaps. A zap is a two-round, *witness-indistinguishable* proof system where the first-round message is fixed "once and for all" [DN00] for all future instances of the protocol. The notion of *witness-indistinguishability* [FLS90] informally states that no PPT adversary can tell which of two possible witnesses has been used to construct a proof.

Definition 2. *A proof system* $\mathsf{\Pi}$ *is witness-indistinguishable (WI) for relation* R *if* $\mathsf{Adv}^{\mathrm{wi}}_{\mathsf{\Pi,R,A}}(\lambda)$ *is negligible in* λ *for any PPT adversary* A*, where* $\mathsf{Adv}^{\mathrm{wi}}_{\mathsf{\Pi,R,A}}(\lambda) := \Pr\left[\mathrm{WI}_{\mathsf{\Pi,R,A}}(\lambda)\right] - 1/2$ *and* $\mathrm{WI}_{\mathsf{\Pi,R,A}}(\lambda)$ *is depicted in Fig. 1.*

A zap is *non-interactive* if there is no first-round message from the verifier to the prover: the prover simply sends a single message. The proof system thus reduces to a pair (P, V) or can be considered as defined above, but with a CRS generation algorithm that always outputs $\perp$. We next define the soundness notion for *non-interactive arguments of knowledge.*

Knowledge soundness [BG93] means that for any prover able to produce a valid proof there exists an efficient algorithm, which has access to the prover's random coins, capable of extracting a witness for the given statement.

Definition 3. *A proof system* $\mathsf{\Pi}$ *is* knowledge-sound *for* R *if for any PPT adversary* A *there exists a PPT extractor* Ext *such that* $\mathsf{Adv}^{\mathrm{ksnd}}_{\mathsf{A,Ext,R,\Pi}}(\lambda)$ *is negligible in* λ*, where* $\mathsf{Adv}^{\mathrm{ksnd}}_{\mathsf{\Pi,R,A,Ext}}(\lambda) := \Pr\left[\mathrm{KSND}_{\mathsf{\Pi,R,A,Ext}}(\lambda)\right]$ *and* $\mathrm{KSND}_{\mathsf{A,Ext,R,\Pi}}(\lambda)$ *is defined in Fig. 2. An* argument of knowledge *is a knowledge-sound proof system.*

Variations of this argument are often found in the literature. Most of them allow the extractor to rewind the adversary for interactive proof systems in

```
Game $\mathrm{KSND}_{\mathsf{\Pi,R,A,Ext}}(\lambda)$
$\mathit{\Gamma} := \mathsf{G}(1^\lambda); (\sigma, \tau) \leftarrow \mathsf{\Pi.K}(\mathit{\Gamma})$
$r \leftarrow_\$ \{0,1\}^{\mathsf{A.rl}(\lambda)}; (\phi, \pi) := \mathsf{A}(\sigma; r)$
$w \leftarrow \mathsf{Ext}(\sigma, r)$
$\textbf{return}\ (\mathsf{\Pi.V}(\sigma, \phi, \pi)\ \textbf{and}\ \mathsf{R}(\phi, w) = \textbf{false})$
```

Fig. 2. Game for knowledge soundness.

```
Game $\mathrm{DLin}_{\mathsf{G},\mathsf{A}}(\lambda)$
$b \leftarrow_{\$} \{0,1\}$ ; $\Gamma := (p, \mathbb{G}, \mathbb{G}_T, e, G) := \mathsf{G}(1^\lambda)$
$u, v, r, s \leftarrow_{\$} \mathbb{Z}_p$
if $b = 1$ then $H := (r + s)G$
else  $H \leftarrow_{\$} \mathbb{G}$
$b' \leftarrow \mathsf{A}(\Gamma, uG, vG, urG, vsG, H)$
return $(b = b')$
```

```
Game $\mathrm{DH\text{-}KE}_{\mathsf{G},\mathsf{A},\mathsf{Ext}}(\lambda)$
$\Gamma := (p, \mathbb{G}, \mathbb{G}_T, e, G) := \mathsf{G}(1^\lambda)$
$r \leftarrow_{\$} \{0,1\}^{\mathsf{A.rl}(\lambda)}$
$(X, Y, Z) := \mathsf{A}(\Gamma; r)$
$s \leftarrow \mathsf{Ext}(\Gamma, r)$
if $sG = X \vee sG = Y$ then return $0$
return $(e(X, Y) = e(Z, G))$
```

Fig. 3. Games for Assumptions 1 (DLin) and 2 (DH-KE).

addition to black-box access, most notably for Σ-protocols. In case of non-interactive provers the extractor is provided with the adversary's random coins.

Assumptions. Our protocol is based on the DH-KE assumption and the existence of a homomorphic extractable commitment scheme. Such schemes have been widely studied and there are constructions from standard assumptions such as the subgroup decision assumption or the decisional linear (DLin) assumption [BBS04]. For this work, we rely on the latter, which is also used in [GOS06a].

The DLin assumption [BBS04] for an abelian group $\mathbb{G} = \langle G \rangle$ of order p states that it is computationally difficult to distinguish $(uG, vG, urG, vsG, (r + s)G)$ with $u, v, r, s \leftarrow_{\$} \mathbb{Z}_p$ from a uniformly random 5-tuple in $\mathbb{G}$.

Assumption 1 (DLin). *We say that the Decisional Linear assumption holds for the group generator* G *if for all PPT adversaries* A *we have:*

$$\mathsf{Adv}^{\mathrm{dlin}}_{\mathsf{G},\mathsf{A}}(\lambda) := \Pr\left[\mathrm{DLin}_{\mathsf{G},\mathsf{A}}(\lambda)\right] - 1/2 = \mathsf{negl}(\lambda)\,,$$

where the game $\mathrm{DLin}_{\mathsf{G},\mathsf{A}}(\lambda)$ *is defined in Fig. 3.*

The intuition behind DH-KE [BFS16] is that it is difficult for some machine to produce a (Diffie-Hellman) DH triple (xG, yG, xyG) in $\mathbb{G}$ without knowing at least x or y. The assumption is in the spirit of earlier knowledge-of-exponent assumptions [Gro10, BCI+10], whose simplest form states that given $(G, xG) \in \mathbb{G}^2$ it is hard to return (yG, xyG) without knowing y.

Assumption 2 (DH-KE). *The Diffie-Hellman Knowledge of Exponent assumption holds for the bilinear group generator* G *if for any PPT adversary* A *there exists a PPT extractor* Ext *such that:*

$$\mathsf{Adv}^{\mathrm{dhke}}_{\mathsf{G},\mathsf{A},\mathsf{Ext}}(\lambda) := \Pr\left[\mathrm{DH\text{-}KE}_{\mathsf{G},\mathsf{A},\mathsf{Ext}}(\lambda)\right] = \mathsf{negl}(\lambda)\,,$$

where the game $\mathrm{DH\text{-}KE}_{\mathsf{G},\mathsf{A},\mathsf{Ext}}(\lambda)$ *is defined in Fig. 3.*

In other variants of knowledge of exponent assumptions the adversary is provided with some auxiliary information, which amounts to a stronger assumption. This is typically required as in the security proofs the reduction obtains a challenge which it needs to embed in the input to the adversary. In our specific case, all the proof material is generated by the prover itself, including the CRS. Consequently, the game DH-KE considers an adversary that simply takes as input a group description, without any auxiliary information. Compared to [BFS16], where the adversary is provided with additional information, our variant is thus weaker.

3 An Extractable Commitment Scheme from DLin

We recall the homomorphic commitment scheme based on linear encryption [BBS04] by Groth et al. [GOS06a]. It defines two types of key generation: a perfectly hiding and perfectly binding one. Given a bilinear group $\Gamma := (p, \mathbb{G}, \mathbb{G}_T, e, G)$, it defines two key-generation algorithms $\mathsf{Com.K}^{(\mathrm{b})}$ and $\mathsf{Com.K}^{(\mathrm{h})}$ producing binding and hiding keys, respectively:

```
$\mathsf{Com.K}^{(\mathrm{h})}$
$\tau := (r_u, s_v) \leftarrow\!\!\$\, (\mathbb{Z}_p^*)^2;\; (x, y) \leftarrow\!\!\$\, (\mathbb{Z}_p^*)^2$
$F := xG, \quad H := yG$
$(U, V, W) := (r_u F, s_v H, (r_u + s_v)G)$
$\sigma := (F, H, U, V, W)$
return $(\sigma, \tau)$
```

```
$\mathsf{Com.K}^{(\mathrm{b})}$
$\tau := (x, y, z) \leftarrow\!\!\$\, (\mathbb{Z}_p^*)^3;\; (r_u, s_v) \leftarrow\!\!\$\, (\mathbb{Z}_p^*)^2$
$F := xG, \quad H := yG$
$(U, V, W) := (r_u F, s_v H, (r_u + s_v + z)G)$
$\sigma := (F, H, U, V, W)$
return $(\sigma, \tau)$
```

In order to commit to a value $m \in \mathbb{Z}_p$, one samples $r, s \leftarrow\!\!\$\, \mathbb{Z}_p$ and returns:

$$C = \mathsf{Com.C}(m; r, s) = \big(mU + rF, mV + sH, mW + (r + s)G\big).$$

Since $\mathsf{Com.C}(m_0; r_0, s_0) + \mathsf{Com.C}(m_1; r_1, s_1) = \mathsf{Com.C}(m_0 + m_1; r_0 + r_1, s_0 + s_1)$, commitments are additively homomorphic. A committed value is opened by providing the randomness (r, s). Under a perfectly hiding key, a commitment to m can be opened to any value m', given trapdoor information $\tau = (r_u, s_v)$:

$$\begin{aligned} \mathsf{Com.C}(m; r, s) &= \big((mr_u + r)F, (ms_v + s)V, (mr_u + r + ms_v + s)G\big) \\ &= \mathsf{Com.C}\big(m'; r - (m' - m)r_u, s - (m' - m)s_v)\big). \end{aligned} \tag{1}$$

Under the DLin assumption, keys output by the perfectly hiding setup are computationally indistinguishable from ones output by the perfectly binding setup. For this reason, the perfectly hiding setup leads to computationally binding commitments and vice versa.

We say that a triple of group elements is *linear* w.r.t. (F, H, G) if it is of the form $(rF, sH, (r + s)G)$ for some $r, s \in \mathbb{Z}_p$. Commitments to 0 are linear triples and every commitment under a *hiding* key is also a linear. Under a *binding* key we have:

$$\mathsf{Com.C}(m; r, s) = \big((mr_u + r)F,\ (ms_v + s)H,\ mzG + (mr_u + r + ms_v + s)G\big).$$

A commitment to m is thus a *linear encryption* [BBS04] of $mzG \in \mathbb{G}_1$ under randomness $(mr_u + r, ms_v + s)$. Given a commitment C and the trapdoor information $\tau = (x, y, z)$, one can *extract* the committed message. The extraction algorithm $\mathsf{Com.E}$ is defined as:

$$\mathsf{Com.E}\big(\tau,\ (C_0, C_1, C_2)\big) := \mathsf{dLog}\big(z^{-1}(C_2 - x^{-1}C_0 - y^{-1}C_1)\big), \tag{2}$$

where dLog can be efficiently computed if the message space is of logarithmic size; for instance, assuming $m \in \{0,1\}$, we define $\mathsf{Com.E}$ to return 0 if $(C_2 - x^{-1}C_0 - y^{-1}C_1)$ is the identity element, and 1 otherwise.

Theorem 4 ([GOS06a]). *Assuming DLin,* Com*, as defined above, is an extractable homomorphic commitment scheme that is:*

- *perfectly binding, computationally hiding when instantiated with* $\mathsf{Com.K}^{(\mathrm{b})}$*;*
- *computationally binding, perfectly hiding when instantiated with* $\mathsf{Com.K}^{(\mathrm{h})}$*.*

The "parameter switching" technique, which defines different types of keys that are computationally indistinguishable, has proved very useful and also applies to encryption schemes. The idea has been defined (and named) several times. "Parameter switching" [GOS06a] is also called "meaningful/meaningless encryption" [KN08], "dual-mode encryption" [PVW08] and "lossy encryption" [BHY09].

Proofs of Binarity. As a building block for their zaps Groth et al. [GOS06a] first construct a witness-indistinguishable non-interactive proof system Bin. Given a commitment key $\sigma = (F, H, U, V, W)$ and a commitment $C \in \mathbb{G}^3$, it allows to prove that C commits to a value in $\{0,1\}$ under σ. The proof is perfectly sound and perfectly witness-indistinguishable. (We recall their scheme in the full version [FO18].)

4 Non-interactive Zaps

To construct a non-interactive zap (i.e., a WI proof system without a CRS), Groth et al. [GOS06a] first construct a proof system for circuit satisfiability *with* a CRS, based on the commitment scheme from Sect. 3 and their proof of binarity. Then, in order to make their scheme CRS-less, they define the prover to pick two CRS's that are correlated in a way that makes it impossible for the adversary to cheat under both of them.

As the commitment scheme described in Sect. 3 is homomorphic, it is possible to perform linear operations on commitments, and in particular prove logical relations between them.

First, proving that either C or $C' := C - (U, V, W)$ is linear proves that C is a commitment to a bit. In order to prove that committed values satisfy wire assignments of a NAND gate, Groth et al. [GOS06b] observe that if $a, b \in \{0,1\}$ then $c := \neg(a \wedge b)$ iff $t := a + b + 2c - 2 \in \{0,1\}$. Reasoning with homomorphic commitments, we have that three commitments $A := (A_0, A_1, A_2)$, $B := (B_0, B_1, B_2)$, and $C := (C_0, C_1, C_2)$ are bound respectively to the values a, b, c, such that $c = \neg(a\ \wedge\ b)$, if and only if

$$T := A + B + 2 \cdot C - 2 \cdot (U, V, W) \tag{3}$$

```
$\mathsf{ZAP.P}(1^\lambda, \phi, w)$
    $\Gamma := \mathsf{G}(1^\lambda)$ ; $(\sigma_0, \tau) \leftarrow \mathsf{Circ.K}(\Gamma)$
    $\sigma_1 := \sigma_0 + (0, 0, 0, 0, G)$
    $\pi_0 \leftarrow \mathsf{Circ.P}(\sigma_0, \phi, w)$; $\pi_1 \leftarrow \mathsf{Circ.P}(\sigma_1, \phi, w)$
    return $(\sigma_0, \pi_0, \pi_1)$
```

```
$\mathsf{ZAP.V}(\phi, (\sigma_0, \pi_0, \pi_1))$
    $\sigma_1 := \sigma_0 + (0, 0, 0, 0, G)$
    return $\left(\bigwedge_{i \in \{0,1\}} \mathsf{Circ.V}(\sigma_i, \phi, \pi_i)\right)$
```

Fig. 4. The (non-interactive) ZAP protocol of [GOS06a].

is a commitment to either 0 or 1. Thus, to prove that A, B, C are commitments to values in $\{0, 1\}$ and that C is a commitment to the NAND of the values in A and B, it is sufficient to prove that A, B, C and T are all bit commitments. With these observations, GOS construct a perfectly witness-indistinguishable proof system Circ for circuit satisfiability as follows:

The key generation algorithm $\mathsf{Circ.K}$ simply emulates $\mathsf{Com.K}^{(\mathrm{h})}$, that is, it generates a hiding commitment key. The prover $\mathsf{Circ.P}(\sigma, \mathsf{C}, w)$ takes as input a circuit C and a witness w satisfying $\mathsf{C}(w) = 1$, and does the following: represent the circuit evaluation $\mathsf{C}(w)$ in such a way that w_k is the value running in the k-th wire. For each w_k, produce a commitment $C_k \leftarrow \mathsf{Com.C}(\sigma, w_k)$ to w_k and prove it is to a bit under σ using proof system Bin. For each gate, construct T from the commitments corresponding to the ingoing and outgoing wires as above and prove that it too is a commitment to 0 or 1. For the output commitment, create a commitment C_{out} to 1 that can be easily reproduced and checked by the verifier: $C_{\mathrm{out}} := \mathsf{Com.C}(\sigma, 1; (0, 0))$. Let Π be the collection of all other commitments together with the respective proofs of binarity generated. Return Π.

The verifier $\mathsf{Circ.V}(\sigma, \mathsf{C}, \Pi)$, computes $C_{\mathrm{out}} := \mathsf{Com.C}(\sigma, 1; (0, 0))$ and for every gate the value T as in Eq. (3); using $\mathsf{Bin.V}$, it checks that all the wire commitments are to values in $\{0, 1\}$ and respect the gates (by checking the values T); if all verifications succeed, return **true**. Otherwise, return **false**.

Theorem 5 **([GOS06a]).** *Assuming DLin,* Circ *is a non-interactive, perfectly sound computationally witness-indistinguishable proof system.*

The reason why we cannot let the prover choose the CRS in Circ is that it could chose it as a perfectly hiding CRS and then simulate proofs. However, if the prover must construct two proofs under two different CRS's which are related in such a way that at least one of them is not linear (and thus binding), then the prover cannot cheat. In particular, note that given a 5-tuple $\sigma_0 \in \mathbb{G}^5$, and defining $\sigma_1 := \sigma_0 + (0, 0, 0, 0, G)$ then at *most* one of σ_0, σ_1 is linear. At the same time, both of them are valid CRS's. With this last trick, it is straightforward to construct the zap scheme ZAP, as illustrated in Fig. 4.

Theorem 6 **([GOS06a]).** *Assuming DLin,* ZAP *is a non-interactive zap with perfect soundness and computational witness indistinguishability.*

Remark 7. We note that soundness of ZAP relies only on the fact that Γ is a bilinear group. In [GOS06a] the prover is allowed to generate Γ and it is required

```
$\mathsf{ZAK.P}(1^\lambda, \phi, w)$
$\varGamma := \mathsf{G}(1^\lambda)$
for $i = 0, 1$ do
    $(\sigma_{i,0}, \tau_i) \leftarrow \mathsf{Circ.K}(\varGamma)$
    $\sigma_{i,1} := \sigma_{i,0} + (0, 0, 0, 0, G)$
    $\pi_{i,0} \leftarrow \mathsf{Circ.P}(\sigma_{i,0}, \phi, w)$
    $\pi_{i,1} \leftarrow \mathsf{Circ.P}(\sigma_{i,1}, \phi, w)$
Compute $\varDelta$ from $\tau_0, \tau_1$ as in Eq. (4).
$\varSigma := [\sigma_{i,0}]_{i \in \{0,1\}}$, $\varPi = [\pi_{i,j}]_{i,j \in \{0,1\}}$
return $(\varSigma, \varDelta, \varPi)$
```

```
$\mathsf{ZAK.V}(\phi, (\varSigma, \varDelta, \varPi))$
// Check if $\varDelta$ is consistent with $\varSigma$
if not $\mathsf{DH}(\varDelta, \varSigma)$ return false
for $i$ in $\{0, 1\}$ do
    $\sigma_{i,1} := \sigma_0 + (0, 0, 0, 0, G)$
return ( $\bigwedge_{i,j \in \{0,1\}} \mathsf{Circ.V}(\sigma_{i,j}, \phi, \pi_{i,j})$ )
```

Fig. 5. The ZAK protocol.

that $\varGamma$ is verifiable. We presented a zap for deterministically generated groups, as considered by Bellare et al. [BFS16], which is also required for our construction of non-interactive zaps of knowledge in the next section.

5 ZAK: A Non-interactive Zap of Knowledge

We now present our NIWI argument of knowledge for circuit satisfiability. The high-level idea of our protocol is to double the ZAP proof of [GOS06a] and link the two CRS's so the prover must know the extraction trapdoor for one of them. Whereas the protocol ZAP used two Circ proofs to construct a zap from a proof that requires a CRS, we will use two zap proofs to not only prove circuit satisfiability, but to prove *knowledge* of a satisfying assignment. More specifically, knowledge soundness is obtained by generating two independent zap proofs, and then linking the respective trapdoor information with multiple DH in a matrix of group elements $\varDelta$. This additional matrix $\varDelta$, that we call *linking element*, is constructed in such a way that (under DH-KE) it is possible to recover the trapdoor from one of the two zap proofs, and use it to extract the witness from the commitments contained in a valid zap proof. Witness indistinguishability of the single proofs follows immediately from [GOS06a], but our proofs also contain the linking element $\varDelta$, which depend on the randomness of the CRS's. We thus have to argue that these additional elements do not harm witness indistinguishability.

Bellare et al. [BFS16] also used an extractor to recover the trapdoor hidden in an adversarially generated CRS to construct a scheme satisfying subversion-zero knowledge. Our protocol is detailed in Fig. 5, where by DH we denote the algorithm that checks that $\delta_{i,j}$ is the CDH of $(\sigma_{0,0})_i$ and $(\sigma_{1,0})_j$ (see below).

The trapdoor information $\tau_0 = (x_0, y_0)$ and $\tau_1 = (x_1, y_1)$ is correlated in $\varDelta$ to form the following products:

$$\varDelta := [\delta_{i,j}]_{i,j \in \{0,1\}} = \begin{bmatrix} x_0 x_1 G & x_0 y_1 G \\ y_0 x_1 G & y_0 y_1 G \end{bmatrix} \tag{4}$$

Correctness of Δ can be checked by the verification algorithm using the bilinear map. For $i = 0, 1$, let the CRS be $\sigma_i = (F_i, H_i, U_i, V_i, W_i)$, and let x_i, y_i be such that:

$$F_i \coloneqq x_i G, \qquad H_i \coloneqq y_i G,$$

in which case Δ is constructed as in Eq. (4). The verifier checks that the following holds:

$$\begin{aligned} e(\delta_{0,0}, G) = e(F_0, F_1), \quad e(\delta_{0,1}, G) = e(F_0, H_1), \\ e(\delta_{1,0}, G) = e(H_0, F_1), \quad e(\delta_{1,1}, G) = e(H_0, H_1). \end{aligned} \tag{5}$$

Let us denote by DH the algorithm that, given as input Σ and Δ returns **true** if all equalities of Eq. (5) are satisfied, and **false** otherwise. This procedure is used by the verification equation, as detailed in Fig. 5.

We now proceed with the proof of our main result, Theorem 1, which we rephrase here for completeness:

Theorem 1. *Assume that DLin and DH-KE hold for* G. *Then* ZAK *as defined in Fig. 5 is a non-interactive zap that satisfies knowledge soundness and witness indistinguishability. In particular, we have*

$$\mathsf{Adv}^{\text{ksnd}}_{\mathsf{ZAK}}(\lambda) \leq 4 \cdot \mathsf{Adv}^{\text{dh-ke}}(\lambda) \quad \textit{and} \quad \mathsf{Adv}^{\text{wi}}_{\mathsf{ZAK}}(\lambda) \leq 8 \cdot \mathsf{Adv}^{\text{dlin}}(\lambda).$$

Completeness of the protocol is trivial: the prover (respectively, the verifier) simply performs 4 iterations of Circ proofs (respectively, verifications), and therefore correctness is implied by Theorem 5 and the fact that Δ as in Eq. 4 satisfies Eq. 5. We now prove knowledge soundness and witness indistinguishability.

Proof (of computational knowledge soundness). We show that for any adversary able to produce a valid proof we can construct a PPT extractor that can extract a witness from such a proof with overwhelming probability.

Let A be an adversarial prover in game $\text{KSND}(\lambda)$ (Fig. 2, with $\Pi.\mathsf{K}$ void). On input 1^λ, A returns a proof consisting of $\sigma_{i,0} = (F_i, H_i, U_i, V_i, W_i)$ for $i \in \{0, 1\}$, of $\Delta = [\delta_{i,j}]_{i,j \in \{0,1\}}$ and $\Pi = [\pi_{i,j}]_{i,j \in \{0,1\}}$. From A we construct four adversaries $\mathsf{A}_{i,j}$ (for $i, j \in \{0, 1\}$) that execute A and output some components of the proof produced by A, namely

$$\begin{aligned} (F_0,\, F_1,\, \delta_{0,0}) &= (x_0 G,\, x_1 G,\, x_0 x_1 G), && (\text{for } \mathsf{A}_{0,0}) \\ (F_0,\, H_1,\, \delta_{0,1}) &= (x_0 G,\, y_1 G,\, x_0 y_1 G), && (\text{for } \mathsf{A}_{0,1}) \\ (H_0,\, F_1,\, \delta_{1,0}) &= (y_0 G,\, x_1 G,\, y_0 x_1 G), && (\text{for } \mathsf{A}_{1,0}) \\ (H_0,\, H_1,\, \delta_{0,1}) &= (y_0 G,\, y_1 G,\, y_0 y_1 G), && (\text{for } \mathsf{A}_{1,1}) \end{aligned}$$

where x_i, y_i are such that $F_i = x_i G$, $H_i = y_i G$, and these four equations hold if $\mathsf{ZAK.V}(\mathsf{C}, (\Sigma, \Delta, \Pi))$ returns **true**. By the DH-KE assumption there exist extractors $\mathsf{Ext}_{i,j}$ for each of the adversaries $\mathsf{A}_{i,j}$ that given its coins outputs:

$$\begin{aligned} &x_0 \text{ or } x_1, \qquad && x_0 \text{ or } y_1, \qquad && (\text{for } \mathsf{Ext}_{0,0},\, \mathsf{Ext}_{0,1}) \\ &y_0 \text{ or } x_1, \qquad && y_0 \text{ or } y_1 \qquad && (\text{for } \mathsf{Ext}_{1,0},\, \mathsf{Ext}_{1,1}) \end{aligned}$$

if the above equations hold. The statement $(x_0 \vee x_1) \wedge (y_0 \vee x_1) \wedge (x_0 \vee y_1) \wedge (y_0 \vee y_1)$ is logically equivalent to $(x_0 \wedge y_0) \vee (x_1 \wedge y_1)$. This means that together, these four extractors allow to recover either (x_0, y_0) or (x_1, y_1), that is, the extraction trapdoor for one of the CRS's. Let i^* be such that (x_{i^*}, y_{i^*}) is the extracted pair.

For $j \in \{0,1\}$, let $F_{i^*}, H_{i^*}, U_{i^*}, V_{i^*}, W_{i^*} \in \mathbb{G}$ be such that $\sigma_{i^*,j} = (F_{i^*}, H_{i^*}, U_{i^*}, V_{i^*}, W_{i^*} + jG)$. Let $j^* \in \{0,1\}$ be the smallest integer satisfying:

$$x_{i^*}^{-1} U_{i^*} + y_{i^*}^{-1} V_{i^*} - (W_{i^*} + j^* G) \neq 0G.$$

The above implies that σ_{i^*,j^*} is not a linear tuple, which means that it is a binding CRS. Let $C_{(i^*,j^*),k}$ denote the commitment to the k-th wire contained in π_{i^*,j^*}. Using the extraction algorithm described in Eq. (2) we can recover this witness:

$$w_k = \mathsf{Com.E}\big((x_{i^*}, y_{i^*}),\ C_{(i^*,j^*),k}\big).$$

It remains to prove that the extracted witness is indeed correct. Upon receiving a valid proof from adversary A, we know from the verification equation (the subroutine DH) that each $\mathsf{A}_{i,j}$ will output a DH triple. Therefore, extractors $\mathsf{Ext}_{i,j}$ together recover $\tau_{i^*} = (x_{i^*}, y_{j^*})$ with probability at least $1 - \sum_{i,j \in \{0,1\}} \mathsf{Adv}^{\mathrm{dhke}}_{\mathsf{G},\mathsf{A}_{i,j},\mathsf{Ext}_{i,j}}(\lambda)$, that is, by DH-KE, with overwhelming probability. Since the commitment scheme Com is perfectly binding if the CRS is not a linear tuple (Theorem 4), a message w_k is always successfully extracted. Correctness of w_k follows from the underlying proof system: by perfect soundness of Bin we are guaranteed that $w_k \in \{0,1\}$; by perfect soundness of Circ (Theorem 5) that each gate evaluation is correct. The bound in the construction of the extractor is tight: we have $\mathsf{Adv}^{\mathrm{ksnd}}(\lambda) \leq 4 \cdot \mathsf{Adv}^{\mathrm{dhke}}(\lambda)$. □

Proof (of computational witness indistinguishability). Consider an adversary in the WI game (Fig. 1, where $\Pi.\mathsf{K}$ is void) that makes $q = q(\lambda)$ queries to the Prove oracle, each of the form $(\mathsf{C}^{(k)}, w_0^{(k)}, w_1^{(k)})$, for $0 \leq k < q$. Consider the following sequence of hybrid games where H_0 corresponds to $\mathrm{WI}_{\mathsf{ZAK},\textsc{circ-sat},\mathsf{A}}(\lambda)$ with $b = 0$ and H_{12} corresponds to $\mathrm{WI}_{\mathsf{ZAK},\textsc{circ-sat},\mathsf{A}}(\lambda)$ with $b = 1$. The games differ in how the Prove oracle is implemented, which is specified in Fig. 6 for the first half of the hybrids (the second half is analogous). We give an overview of all hybrids in Table 2 below.

H_0 The challenger simulates an honest Prove oracle, using (for every $k < q$) the first witness $w_0^{(k)}$ supplied by the adversary. It outputs $(\Sigma^{(k)}, \Delta^{(k)}, \Pi^{(k)})$, where in particular we recall:

$$\Sigma^{(k)} = \begin{bmatrix} \sigma_{0,0}^{(k)} = (F_0^{(k)}, H_0^{(k)}, U_0^{(k)}, V_0^{(k)}, W_0^{(k)}) \\ \sigma_{1,0}^{(k)} = (F_1^{(k)}, H_1^{(k)}, U_1^{(k)}, V_1^{(k)}, W_1^{(k)}) \end{bmatrix} \quad \text{and} \quad \Pi^{(k)} = \begin{bmatrix} \pi_{0,0}^{(k)} & \pi_{0,1}^{(k)} \\ \pi_{1,0}^{(k)} & \pi_{1,1}^{(k)} \end{bmatrix}.$$

Recall that the two rows of $[\Sigma^{(k)} | \Pi^{(k)}]$ are independent zaps and that $\sigma_{0,0}^{(k)}$ and $\sigma_{1,0}^{(k)}$ are chosen to be *hiding*. The Prove oracle computes $\sigma_{i,j}^{(k)}$ which

```
Oracle PROVE in $\mathsf{H}_1$, $\boxed{\mathsf{H}_2}$, and $\boxed{\mathsf{H}_3}$
$\Gamma := \mathsf{G}(1^\lambda)$
$(\sigma_{0,0}, \tau_i) \leftarrow \mathsf{Circ.K}(\Gamma)$
$\boxed{(\sigma_{0,0}, \tau_i) \leftarrow \mathsf{Com.K}^{(\mathrm{b})}(\Gamma)}$
$\sigma_{0,1} := \sigma_{0,0} + (0, 0, 0, 0, G)$
$\boxed{\begin{array}{l} (\sigma_{0,1}, \tau_i) \leftarrow \mathsf{Circ.K}(\Gamma) \\ \sigma_{0,0} := \sigma_{0,1} - (0, 0, 0, 0, G) \end{array}}$
$\pi_{0,0} \leftarrow \mathsf{Circ.P}(\sigma_{0,0}, \mathtt{C}, w_1)$
$\pi_{0,1} \leftarrow \mathsf{Circ.P}(\sigma_{0,1}, \mathtt{C}, w_0)$
// The second zap is as in ZAK.P using $w_0$.
$(\sigma_{1,0}, \pi_{1,0}, \pi_{1,1}) \leftarrow \mathsf{ZAP.P}(1^\lambda, \mathtt{C}, w_0)$
Compute $\Delta$ as in Eq. (4).
return $(\Sigma, \Delta, \Pi)$
```

```
Oracle PROVE in $\mathsf{H}_4$ and $\boxed{\mathsf{H}_5}$
$\Gamma := \mathsf{G}(1^\lambda)$
$(\sigma_{0,1}, \tau_i) \leftarrow \mathsf{Circ.K}(\Gamma)$
$\sigma_{0,0} := \sigma_{0,1} - (0, 0, 0, 0, G)$
$\boxed{(\sigma_{0,1}, \tau_i) \leftarrow \mathsf{Com.K}^{(\mathrm{b})}(\Gamma)}$
$\pi_{0,0} \leftarrow \mathsf{Circ.P}(\sigma_{0,0}, \mathtt{C}, w_1)$
$\pi_{0,1} \leftarrow \mathsf{Circ.P}(\sigma_{0,1}, \mathtt{C}, w_1)$
// The second zap is as in ZAK.P using $w_0$.
$(\sigma_{1,0}, \pi_{1,0}, \pi_{1,1}) \leftarrow \mathsf{ZAP.P}(1^\lambda, \mathtt{C}, w_0)$
Compute $\Delta$ as in Eq. (4).
return $(\Sigma, \Delta, \Pi)$
```

Fig. 6. Overview of the simulations of the prove oracle in the first hybrid games for the proof of WI. Hybrids H_1 and H_4 are defined by ignoring all boxes (the light gray highlights the differences with respect to the previous hybrids), whereas $\boxed{\mathsf{H}_2}$ and $\boxed{\mathsf{H}_5}$ include the light boxes but not the gray one and $\boxed{\mathsf{H}_3}$ includes all boxes.

is of the form $\sigma_{i,j}^{(k)} = \left(F_i^{(k)}, H_i^{(k)}, U_i^{(k)}, V_i^{(k)}, W_i^{(k)} + jG\right)$, for $i, j \in \{0, 1\}$. Furthermore, $\pi_{i,j}^{(k)}$ is a Circ proof using $w_0^{(k)}$ under the CRS $\sigma_{i,j}^{(k)}$.

H_1 For every PROVE query, the simulator uses witness $w_1^{(k)}$ (instead of $w_0^{(k)}$) to produce $\pi_{0,0}^{(k)}$. As the respective CRS $\sigma_{0,0}^{(k)}$ was generated using the perfectly hiding commitment setup $\mathsf{Circ.K}$, the two hybrids are distributed equivalently (any commitment under a hiding key is a random linear triple; cf. Eq. (1)).

H_2 For every PROVE query, the simulator now generates CRS $\sigma_{0,0}^{(k)}$ as a *binding* key via $\mathsf{Com.K}^{(b)}$; $\sigma_{0,1}^{(k)}$ is generated as before (adding $(0, 0, 0, 0, G)$), and so are all proofs. Note that the linking elements $\Delta^{(k)}$ can be constructed knowing only the trapdoor $(x_1^{(k)}, y_1^{(k)})$ of the CRS $\sigma_{1,0}^{(k)}$, which remained unchanged:

$$\Delta^{(k)} = \begin{bmatrix} y_1^{(k)} H_0^{(k)} & y_1^{(k)} F_0^{(k)} \\ x_1^{(k)} H_0^{(k)} & x_1^{(k)} F_0^{(k)} \end{bmatrix}. \tag{6}$$

H_1 and H_2 are computationally indistinguishable under the DLin assumption: given a DLin challenge (F, H, U, V, W), the reduction can exploit the random self-reducibility property of DLin to construct q instances of the DLin challenge: $\forall k < q$ select $\bar{x}^{(k)}, \bar{y}^{(k)}, \bar{r}^{(k)}, \bar{s}^{(k)}, \bar{z}^{(k)} \leftarrow_{\$} \mathbb{Z}_p$ and compute $\sigma_{0,0}^{(k)}$ as $\big(\bar{x}^{(k)} F,\ \bar{y}^{(k)} H,\ \bar{r}^{(k)} \bar{x}^{(k)} F + \bar{z}^{(k)} \bar{x}^{(k)} U,\ \bar{s}^{(k)} \bar{y}^{(k)} H + \bar{z}^{(k)} \bar{y}^{(k)} V,\ (\bar{r}^{(k)} + \bar{s}^{(k)}) G + \bar{z}^{(k)} W\big)$.

Each $\sigma_{0,0}^{(k)}$ is a random linear tuple if and only if the DLin challenge is, and it is a uniformly random tuple if the DLin challenge is, as shown in [BFS16].

Table 2. Overview of changes throughout the hybrids: (h) denotes hiding setup; (b) denotes binding setup; w_b identifies the witness used to produce the proof.

Hybrid	$\sigma_{0,0}^{(k)}$	$\pi_{0,0}^{(k)}$	$\sigma_{0,1}^{(k)}$	$\pi_{0,1}^{(k)}$	$\sigma_{1,0}^{(k)}$	$\pi_{1,0}^{(k)}$	$\sigma_{1,1}^{(k)}$	$\pi_{1,1}^{(k)}$
H_0	(h)	w_0	(b)	w_0	(h)	w_0	(b)	w_0
H_1		w_1						
H_2	(b)							
H_3			(h)					
H_4				w_1				
H_5			(b)					
H_6	(h)							
H_7						w_1		
H_8					(b)			
H_9							(h)	
H_{10}								w_1
H_{11}							(b)	
H_{12}	(h)	w_1	(b)	w_1	(h)	w_1	(b)	w_1

Computing $\sigma_{1,0}^{(k)}$ as in H_1 (hiding) and defining $\varDelta$ as in Eq. 6, the simulator generates the rest of the game as defined. It returns the adversary's guess and thus breaks DLin whenever the adversary distinguishes H_1 and H_2.

H_3 The simulator replaces each CRS $\sigma_{0,1}^{(k)}$ for all $k < q$ with a *hiding* commitment and defines $\sigma_{0,0}^{(k)} := \sigma_{0,1}^{(k)} - (0, 0, 0, 0, G)$, which is therefore (once again) binding. More specifically, the simulator creates a linear tuple invoking $\mathsf{Circ.K}$:

$$\sigma_{0,1}^{(k)} = \big(x_0^{(k)}G,\ y_0^{(k)}G,\ x_0^{(k)}r^{(k)}G,\ y_0^{(k)}s^{(k)}G,\ (r^{(k)} + s^{(k)})G\big)$$

where $x_0^{(k)}, y_0^{(k)}, r^{(k)}, s^{(k)} \leftarrow_{\$} \mathbb{Z}_p$.

The two distributions are proven computationally indistinguishable under DLin by an argument analogous to the one for $\mathsf{H}_1 \to \mathsf{H}_2$. This time the challenger constructs all the instances of the DLin challenge for $\sigma_{0,1}^{(k)}$, while $\sigma_{0,0}^{(k)}$ is derived. From there, the proof proceeds identically.

H_4 The simulator replaces each proof $\pi_{0,1}^{(k)}$ by using $w_1^{(k)}$ instead of $w_0^{(k)}$ ($\forall k < q$). This hybrid is equivalently distributed as the previous one; this is proved via the same argument as for $\mathsf{H}_0 \to \mathsf{H}_1$.

H_5 The simulator switches $\sigma_{0,1}^{(k)}$ from a hiding to a binding key. This game hop is analogous to the hop $\mathsf{H}_1 \to \mathsf{H}_2$ (which switched $\sigma_{0,0}^{(k)}$ from hiding to binding).

H_6 The simulator switches $\sigma_{0,0}^{(k)}$ from binding to hiding. Indistinguishability from the previous hybrid is shown analogously to the hop $\mathsf{H}_2 \to \mathsf{H}_3$. Note that in this hybrid the first zap $(\sigma_{0,0}^{(k)}, \pi_{0,0}^{(k)}, \pi_{0,1}^{(k)})$ is distributed according to the protocol specification, but using witness $w_1^{(k)}$.

Hybrids H_7 to H_{12} are now defined analogously to hybrids H_1 to H_6, except for applying all changes to $\sigma_1^{(k)}$ and $\pi_{1,0}^{(k)}$ and $\pi_{1,1}^{(k)}$. In hybrid H_{12} the adversary is then given arguments of knowledge for witness w_1.

As the difference between hybrids H_1 and H_{12} is bounded by 8 times the advantage of a DLin distinguisher, the adversary has total advantage

$$\mathsf{Adv}^{\mathrm{wi}}_{\mathsf{ZAK,C,A}}(\lambda) \leq 8 \cdot \mathsf{Adv}^{\mathrm{dlin}}_{\mathsf{ZAK,C,A}}(\lambda) = \mathsf{negl}(\lambda)\,.$$

The bound is thus tight. □

Acknowledgements. The authors would like to thank the anonymous reviewers of PKC 2018 and ACNS 2018 for their helpful comments. The first author is supported by the French ANR EfTrEC project (ANR-16-CE39-0002). The second author is supported by ERC grant 639554 (project aSCEND).

References

[BBS04] Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3

[BCG+14] Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, pp. 459–474. IEEE Computer Society Press, May 2014

[BCI+10] Brier, E., Coron, J.-S., Icart, T., Madore, D., Randriam, H., Tibouchi, M.: Efficient indifferentiable hashing into ordinary elliptic curves. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 237–254. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_13

[BFM88] Blum, M., Feldman, P., Micali, S.: Non-interactive zero-knowledge and its applications (extended abstract). In: 20th ACM STOC, pp. 103–112. ACM Press, May 1988

[BFS16] Bellare, M., Fuchsbauer, G., Scafuro, A.: NIZKs with an untrusted CRS: security in the face of parameter subversion. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 777–804. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_26

[BG93] Bellare, M., Goldreich, O.: On defining proofs of knowledge. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 390–420. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-48071-4_28

[BHY09] Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_1

[BOV03] Barak, B., Ong, S.J., Vadhan, S.: Derandomization in cryptography. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 299–315. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_18

[BP15] Bitansky, N., Paneth, O.: ZAPs and non-interactive witness indistinguishability from indistinguishability obfuscation. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9015, pp. 401–427. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46497-7_16

[BW06] Boyen, X., Waters, B.: Compact group signatures without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 427–444. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_26

[BW07] Boyen, X., Waters, B.: Full-domain subgroup hiding and constant-size group signatures. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 1–15. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_1

[DN00] Dwork, C., Naor, M.: Zaps and their applications. In: 41st FOCS, pp. 283–293. IEEE Computer Society Press, November 2000

[FLS90] Feige, U., Lapidot, D., Shamir, A.: Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In: 31st FOCS, pp. 308–317. IEEE Computer Society Press, October 1990

[FO18] Fuchsbauer, G., Orrú, M.: Non-interactive zaps of knowledge. Cryptology ePrint Archive, Report 2018/228 (2018)

[FS90] Feige, U., Shamir, A.: Witness indistinguishable and witness hiding protocols. In: 22nd ACM STOC, pp. 416–426. ACM Press, May 1990

[Fuc18] Fuchsbauer, G.: Subversion-zero-knowledge SNARKs. In: Abdalla, M., Dahab, R. (eds.) PKC 2018. LNCS, vol. 10769, pp. 315–347. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76578-5_11

[GMR89] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989)

[GO94] Goldreich, O., Oren, Y.: Definitions and properties of zero-knowledge proof systems. J. Cryptol. **7**(1), 1–32 (1994)

[GOS06a] Groth, J., Ostrovsky, R., Sahai, A.: Non-interactive zaps and new techniques for NIZK. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 97–111. Springer, Heidelberg (2006). https://doi.org/10.1007/11818175_6

[GOS06b] Groth, J., Ostrovsky, R., Sahai, A.: Perfect non-interactive zero knowledge for NP. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 339–358. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_21

[GS08] Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_24

[Gol93] Goldreich, O.: A uniform-complexity treatment of encryption and zero-knowledge. J. Cryptol. **6**(1), 21–53 (1993)

[Gro06] Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_29

[Gro10] Groth, J.: Short pairing-based non-interactive zero-knowledge arguments. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 321–340. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_19

[KN08] Kol, G., Naor, M.: Cryptography and game theory: designing protocols for exchanging information. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 320–339. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78524-8_18

[PVW08] Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_31

[Ràf15] Ràfols, C.: Stretching groth-sahai: NIZK proofs of partial satisfiability. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9015, pp. 247–276. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46497-7_10