Structure vs. Hardness Through the Obfuscation Lens

Nir Bitansky, Akshay Degwekar(✉), and Vinod Vaikuntanathan

MIT, Cambridge, USA
{nirbitan,akshayd,vinodv}@csail.mit.edu

Abstract. Much of modern cryptography, starting from public-key encryption and going beyond, is based on the hardness of structured (mostly algebraic) problems like factoring, discrete log or finding short lattice vectors. While structure is perhaps what enables advanced applications, it also puts the hardness of these problems in question. In particular, this structure often puts them in low complexity classes such as $\mathsf{NP} \cap \mathsf{coNP}$ or statistical zero-knowledge (SZK).

Is this structure really necessary? For some cryptographic primitives, such as one-way permutations and homomorphic encryption, we know that the answer is *yes*—they imply hard problems in $\mathsf{NP} \cap \mathsf{coNP}$ and SZK, respectively. In contrast, one-way functions do *not* imply such hard problems, at least not by *fully black-box reductions*. Yet, for many basic primitives such as public-key encryption, oblivious transfer, and functional encryption, we do not have any answer.

We show that the above primitives, and many others, do *not* imply hard problems in $\mathsf{NP} \cap \mathsf{coNP}$ or SZK via fully black-box reductions. In fact, we first show that even the very powerful notion of Indistinguishability Obfuscation (IO) does *not* imply such hard problems, and then deduce the same for a large class of primitives that can be constructed from IO.

Keywords: Indistinguishability obfuscation · Statistical zero-knowledge · $\mathsf{NP} \cap \mathsf{coNP}$ · Structured hardness · Collision-resistant hashing

1 Introduction

The last four decades of research in cryptography has produced a host of fantastic objects, starting from one-way functions and permutations to public-key encryption [DH76,RSA78,GM82] and zero-knowledge proofs [GMR85] in the

MIT CSAIL. Research supported in part by NSF Grants CNS-1350619 and CNS-1414119, Alfred P. Sloan Research Fellowship, Microsoft Faculty Fellowship, the NEC Corporation, a Steven and Renee Finn Career Development Chair from MIT. This work was also sponsored in part by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Research Office under contracts W911NF-15-C-0226.

J. Katz and H. Shacham (Eds.): CRYPTO 2017, Part I, LNCS 10401, pp. 696–723, 2017.
DOI: 10.1007/978-3-319-63688-7_23

1980s, all the way to fully homomorphic encryption [RAD78, Gen09, BV11] and indistinguishability obfuscation [BGI+01, GGH+13a] in the modern day.

The existence of all these objects requires at the very minimum that $\mathsf{NP} \not\subseteq \mathsf{BPP}$, but that is hardly ever enough. While one-way functions (OWFs), the most basic cryptographic object, does not seem to require much structure, as we advance up the ranks, we seem to require that certain *structured problems are hard*. For example, conjectured hard problems commonly used in cryptography (especially the public-key kind), such as factoring, discrete logarithms, and shortest (or closest) vectors on lattices all have considerable algebraic structure. On the one hand, it is this structure that enables strong applications such as public-key and homomorphic encryption. On the other hand, this structure is also what puts their hardness in question, and is exactly what algorithms may try to exploit in order to solve these problems. There is of course the fear that this structure will (eventually, if not today) deem these problems *easy*. Or, as Barak says more eloquently [Bar13]:

> [...] *based on the currently well studied schemes, structure is strongly associated with (and perhaps even implied by) public key cryptography. This is troubling news, since it makes public key crypto somewhat of an "endangered species" that could be wiped out by a surprising algorithmic advance. Therefore the question of whether structure is inherently necessary for public key crypto is not only of mathematical interest but also of practical importance as well.*

Thus, a fundamental question in cryptography is *what type of structure is necessary for different primitives?* Indeed, the answer to this question may be crucial to our understanding of what are the minimal assumptions required to construct these primitives. While there may be different ways of approaching this question, one main approach, which is also taken in this work, has been through the eyes of complexity theory. That is, we wish to understand which cryptographic primitives require hardness in low (and so called structured) complexity classes such as $\mathsf{NP} \cap \mathsf{coNP}$, TFNP (the class of total NP search problems), or SZK (the class of problems with statistical zero-knowledge proofs).

Aiming to answer this question, one line of research demonstrates that, for some cryptographic primitives, hardness in structured complexity classes is indeed necessary. The existence of one-way permutations (OWPs) requires a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$ [Bra79]; the same holds for restricted cases of public-key encryption schemes satisfying specific structural properties (e.g. ciphertext certification) [Bra79, GG98]; homomorphic encryption schemes and non-interactive computational private information retrieval schemes imply hard problems in SZK [BL13, LV16]; and indistinguishability obfuscation schemes imply a hard problem in $\mathsf{PPAD} \subseteq \mathsf{TFNP}$ (assuming $\mathsf{NP} \not\subseteq \mathsf{ioBPP}$) [BPR15].

Yet, for many primitives such hardness is not known to be inherent. While this is perhaps expected for OWFs, it is also the case for seemingly structured primitives such as collision-resistant hash functions, oblivious transfer, and general public-key encryption schemes. *Do these primitives require hardness in structured complexity classes? Can we prove that they do or that they don't?*

Black-Box Separations. Formalizing this question in a meaningful way requires care. Indeed, it may be easy to formalize a statement of the form "the existence of crypto primitive $\mathcal{P}$ *implies* hardness in a complexity class $\mathcal{C}$": one just needs to show a reduction from breaking $\mathcal{P}$ to solving problems in $\mathcal{C}$. However, it is not clear how to prove statements of the form "the existence of crypto primitive $\mathcal{P}$ does *not* imply hardness in a complexity class $\mathcal{C}$". For example, it is commonly believed that $\mathsf{NP} \cap \mathsf{coNP}$ *does* contain hard problems. So in a trivial logical sense the existence of such problems is implied by any primitive $\mathcal{P}$. Instead, we follow the methodology of black-box separations, whose study in cryptography was pioneered by Impagliazzo and Rudich [IR89]. Faced with a similar problem of how to show that a primitive $\mathcal{P}$ (OWFs) cannot be used to construct another primitive $\mathcal{P}'$ (public-key encryption), they prove this cannot be shown through *black-box reductions*—cryptography's de facto technique for showing such implications.

A bit more elaborately, a *fully black-box reduction* [RTV04] of a primitive (or, in our case, a problem) $\mathcal{P}'$ to a primitive $\mathcal{P}$ consists of a black-box *construction* and a black-box *security reduction*. The construction of $\mathcal{P}'$ from $\mathcal{P}$ does not exploit the actual implementation of primitive $\mathcal{P}$, but rather just its input-output interface. The security reduction can use any adversary that breaks (or, in our case, solves) $\mathcal{P}'$ to break $\mathcal{P}$, and is oblivious to the implementation of the adversary (as well as of that of $\mathcal{P}$).

Following [IR89], there has been a rich study of black-box separations in cryptography (see, e.g., [Rud91, Sim98, KST99, GKM+00, GT00, GMR01, BT03, RTV04, HR04, GGKT05, Pas06, GMM07, BM09, HH09, BKSY11, DLMM11, KSS11, GKLM12, DHT12, BBF13, Fis12, Pas13, BB15, HHRS15] and many others). Most of this study has been devoted to establishing separations between different cryptographic primitives. (In particular, the most relevant to us are the recent works of Asharov and Segev [AS15, AS16] that study black-box separations for indistinguishability obfuscation, which we elaborate on below.) Some of this study puts limitations on basing cryptographic primitives on NP-hardness [GG98, AGGM06, MX10, HMX10, BL13, BB15, LV16].

Going back to our main question of which primitives require structured hardness, we know the following.

- As described above, OWPs imply a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$ [Bra79], homomorphic encryption and PIR imply hard problems in SZK [BL13, LV16] and IO (with OWFs) implies a hard problem in PPAD [BPR15] via *black-box reductions*.
- On the flip side, we know that there are no black-box reductions from hard problems in $\mathsf{NP} \cap \mathsf{coNP}$ to OWFs [BI87, Rud88], and from hard-on-average problems in SZK to OWPs (corollary from [Ost91, OV08, HHRS15]).

For more advanced primitives, most notably (general) public-key encryption, we do not have results in either direction. In fact, many existing constructions are based on problems in $\mathsf{NP} \cap \mathsf{coNP}$ or SZK. We are thus left with (quite basic) primitives at an unclear state; as far as we know, they may very well imply hard problems in structured complexity classes, even by black-box reductions.

1.1 Our Results

We revisit the relationship between two structured complexity classes, statistical zero-knowledge (SZK) and $\mathsf{NP} \cap \mathsf{coNP}$, and cryptographic primitives. In broad strokes, we show that there are no fully black-box reductions of hard problems in these classes to any one of a variety of cryptographic primitives, including (general) public-key encryption, oblivious transfer, deniable encryption, and functional encryption. More generally, we separate SZK and $\mathsf{NP} \cap \mathsf{coNP}$ from indistinguishability obfuscation (IO). Then, leveraging on the fact that IO can be used to construct a wide variety of cryptographic primitives in a black-box way, we derive corresponding separations for these primitives.[1] One complexity-theoretic corollary of this result is a separation between SZK and $\mathsf{NP} \cap \mathsf{coNP}$ from the class PPAD [MP91] that captures the complexity of computing Nash Equilibria.

On the positive side, we construct collision-resistant hash functions from a strong form of SZK-hardness and IO. It was previously known [AS15] that IO by itself does not imply collision-resistant hashing in a black-box way; we show that it does if one adds SZK-hardness as a "catalyst".
We now go into more detail on each of the results.

Statistical Zero-Knowledge and Cryptography. The notion of statistical zero-knowledge proofs was introduced in the seminal work of Goldwasser et al. [GMR85]. The class of *promise problems* with statistical zero-knowledge proofs (SZK) can be characterized by several complete problems, such as *statistical difference* [SV03] and *entropy difference* [GV99]. SZK hardness is known to follow from various number-theoretic problems that are commonly used in cryptography, such as Discrete Logarithms [GK93], Quadratic Residuosity [GMR85], Lattice Problems [GG98, MV03] as well as problems like Graph Isomorphism [GMW91]. As mentioned, we also know that a handful of cryptographic primitives such as homomorphic encryption [BL13], private information retrieval [LV16] and rerandomizable encryption imply hardness in SZK. (On the other hand, $\mathsf{SZK} \subseteq \mathsf{AM} \cap \mathsf{coAM}$ [For89, AH91], and thus, SZK cannot contain NP-hard problems, unless the polynomial hierarchy collapses [BHZ87].)

We ask more generally which cryptographic primitives can be shown to imply such hardness, with the intuition that such primitives are *structured* in a certain way. In particular, whereas one may not expect a seemingly unstructured object like OWFs to imply such hardness, what can we say for instance about OWPs, public-key encryption, or even IO (which has proven to be powerful enough to yield almost any known cryptographic goal)?

We prove that none of these primitives imply such hardness through black-box reductions.

[1] More accurately, these primitives follow from IO and OWFs (OWFs), and accordingly our separation addresses IO and OWFs in conjunction. The concept of a black-box reduction from IO and OWF requires clarification and discussion. Here we will follow the framework of Asharov and Segev [AS15]. We elaborate below.

Theorem 1.1 (Informal). *There is no fully black-box reduction of any (even worst-case) hard problem in* SZK *to IO and OWPs.*

Corollary 1.2 (from *[SW14, Wat15],* **Informal).** *There is no such reduction to (general) public-key encryption, oblivious transfer, deniable encryption, functional encryption, or any other object that has a black-box reduction to IO and OWPs.*

We would like to elaborate a bit more on what a black-box construction of a hard problem in SZK means. We shall focus on the characterization of SZK by the *statistical difference* promise problem [SV03]. In this problem, an instance is a pair of circuit samplers $C_0, C_1 : \{0,1\}^n \to \{0,1\}^m$ which induce distributions $\boldsymbol{C}_0$ and $\boldsymbol{C}_1$ where the distribution $\boldsymbol{C}_b$ obtained by evaluating the circuit C_b on a uniformly random input. The promise is that the statistical distance $s = \Delta(\boldsymbol{C}_0, \boldsymbol{C}_1)$ of the corresponding distributions is either large (say, $s \geq 2/3$) or small (say, $s \leq 1/3$). The problem, named $\mathbf{SD}^{1/3,2/3}$ (or just **SD**), is to decide which is the case.

Let us look at a specific example of the construction of such a problem from *rerandomizable encryption*. In a (say, symmetric-key) rerandomizable encryption scheme, on top of the usual encryption and decryption algorithms $(\mathsf{Enc}, \mathsf{Dec})$ there is a ciphertext rerandomization algorithm ReRand that can statistically refresh ciphertexts. Namely, for any ciphertext CT encrypting a bit b, $\mathsf{ReRand}(\mathsf{CT})$ produces a ciphertext that is statistically close to a fresh encryption $\mathsf{Enc}_{\mathsf{sk}}(b)$. This immediately gives rise to a hard statistical difference problem [BL13]: given a pair of ciphertexts $(\mathsf{CT}_0, \mathsf{CT}_1)$, decide whether the corresponding rerandomized distributions given by the circuits $(C_0(\cdot), C_1(\cdot)) := (\mathsf{ReRand}(\mathsf{CT}_0; \cdot), \mathsf{ReRand}(\mathsf{CT}_1; \cdot))$ are statistically far or close. Indeed, this corresponds to whether they encrypt the same bit or not, which is hard to decide by the security of the encryption scheme.

A feature of this reduction of hard statistical difference instances to rerandomizable encryption is that, similarly to most reductions in cryptography, it is *fully black-box* [RTV04] in the sense that the circuits C_0, C_1 only make black-box use of the encryption scheme's algorithms, and can in fact be represented as oracle-aided circuits $(C_0^{\mathsf{ReRand}(\cdot)}, C_1^{\mathsf{ReRand}(\cdot)})$. Furthermore, "hardness" can be shown by a black-box security proof that can use any decider for the problem in a black-box way to break the underlying encryption scheme. More generally, one can consider the statistical difference problem relative to different oracles implementing different cryptographic primitives and ask when can hardness be shown based on a black-box reduction. Theorem 1.1 rules out such reductions relative to IO and OWPs (and everything that follows from these in a fully black-box way). For more details, see Sect. 1.2 and the full version.

NP ∩ coNP and Cryptography. Hard (on average) problems in NP ∩ coNP are known to follow based on several number-theoretic problems in cryptography, such as Discrete Log, Factoring and Lattice Problems [Has88, LLJS90, AR04]. As in the previous section for SZK, we are interested in understanding which cryptographic primitives would imply such hardness, again with the intuition

that this implies structure. For instance, it is known [Bra79] that any OWP $f : \{0,1\}^n \to \{0,1\}^n$ implies a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$, e.g. given an index $i \in [n]$ and an image $f(x)$ find the ith preimage bit x_i. In contrast, Blum and Impagliazzo [BI87] and Rudich [Rud88] proved that seemingly unstructured objects like OWFs do not imply hardness in $\mathsf{NP} \cap \mathsf{coNP}$ by fully black-box reductions. In this context, a fully black-box reduction essentially means that the non-deterministic verifiers only make black-box use of the OWF (or OWP in the previous example) and the reduction establishing the hardness is also black-box (in both the decider and the OWF).[2]

But what about more structured primitives such as public-key encryption, oblivious transfer, or even IO? We rule out fully black-box reductions from OWFs (or even *injective OWFs*) and IO to hard problems in $\mathsf{NP} \cap \mathsf{coNP}$. Hence, also for the other primitives, which can be constructed from IO (with OWFs) in a fully black-box way.

Theorem 1.3 (Informal). *There is no fully black-box reduction of any (even worst-case) hard problem in* $\mathsf{NP} \cap \mathsf{coNP}$ *to IO and OWFs.*

Corollary 1.4 (from [SW14,Wat15] Informal). *There is no such reduction to (general) public-key encryption, oblivious transfer, deniable encryption, functional encryption, or any other object that has a black-box reduction to IO and OWFs.*

Our approach also gives a new (rather different) proof to the original separation between OWFs and $\mathsf{NP} \cap \mathsf{coNP}$ [BI87,Rud88]. For more details, see Sect. 1.2 and the full version.

We remark that unlike our result for SZK (which ruled out hard *promise problems*), the above result only rules out hard *languages* in $\mathsf{NP} \cap \mathsf{coNP}$. Indeed, Even et al. [ESY84] demonstrated promise problems in $\mathsf{NP} \cap \mathsf{coNP}$ that are NP-hard. Hence even the assumption $\mathsf{P} \neq \mathsf{NP}$ (let alone OWFs) gives us hard promise problems in $\mathsf{NP} \cap \mathsf{coNP}$. (See [Gol06] for further reading.)

Relation to the Work of Asharov and Segev. The flood of IO applications following, starting from [GGH+13b,SW14], has lead many to conjecture that IO may be "complete for cryptography" (assuming also OWFs, or just $\mathsf{NP} \not\subseteq \mathsf{ioBBP}$ [KMN+14]). Nevertheless, some cryptographic goals could not be constructed based on IO.

Asharov and Segev [AS15,AS16] were the first to initiate a formal study to understand *the limits of IO*. Our separations for IO are based on their framework [AS15]. We aim to draw the complexity-theoretic boundaries of IO. Indeed, black-box separations from IO require some care, given that the typical use of

[2] Roughly speaking, [BI87] rule out *perfectly correct constructions*, where the $\mathsf{NP} \cap \mathsf{coNP}$ structure is guaranteed for any implementation of the OWF oracle. In [Rud88], this is generalized also to *almost perfectly correct constructions* that only work for an overwhelming fraction of OWF oracles. We also rule out constructions that are perfectly correct.

IO makes non-black-box use of the circuits it obfuscates and thus any associated cryptographic primitive such as OWFs. The Asharov-Segev framework considers obfuscators that take as input circuits with OWF (or OWP) gates. They observe, most known IO-based constructions fall into this category. Thus, a separation in this model allows deriving the corresponding separations between SZK or NP ∩ coNP and a wide variety of cryptographic primitives. See Sect. 1.2 for more details.

In terms of results, they show that collision-resistant hashing and (domain invariant) OWPs do not have black-box reductions to IO (and OWFs). Our separation of IO and NP ∩ coNP is more general and implies their previous result for OWPs (and gives a rather different proof for this fact). Their result for collision-resistant hashing is not captured by our results (indeed collision-resistance is not known to imply hardness in either SZK or NP ∩ coNP). We also stress that our separation of SZK from IO and OWPs does not follow from their results; indeed, SZK-hardness is not known to imply collision-resistance.[3]

Indistinguishability Obfuscation: Perspective. Since the breakthrough of [GGH+13b], the notion of IO has been extensively studied. While we already understand that IO has far reaching implications, our understanding of how it can be constructed and under what assumptions is still at an early stage. Indeed, basing IO on solid foundations is one of cryptography's greatest challenges today. In this context, we stress that the results presented in this work hold regardless of the state of existing candidates. In fact, even if it turned out that there is no secure realization of IO, the separation of SZK and NP ∩ coNP from primitives such as public-key encryption, which follow from IO, still holds. The expressiveness of IO (established in [GGH+13b,SW14] and onwards) allows us to prove many separations in one shot. (Indeed, three years ago we would have probably addressed each primitive separately.)

As for the search for candidates itself, while at this point candidates are based on lattice-related problems that do break in SZK, our work suggests the theoretical possibility that IO candidates may not require such structure. A similar conclusion is true of course for the much more basic and long-studied question of public-key encryption. Almost all known public-key encryption candidates rely on very algebraic assumptions (that do break in SZK or NP ∩ coNP). Constructing public key encryption from less structured assumptions remains a fascinating open question. While there has been initial steps trying to diverge from such structure [Ale03,ABW10], there is yet a long way to go.

On TFNP vs. NP ∩ coNP. One of the corollaries of our result is a separation between SZK and NP ∩ coNP from the complexity class PPAD. PPAD, a subclass

[3] We note that previous work [Ost91,OV08] does imply that constant-round statistically-hiding commitments have a black-box reduction to any *hard-on-average* SZK problem. However, [AS15] do not rule these out (but only collision-resistant hashing). We also note that in any case, our result also rules out constructions of worst-case hard SZK problems (rather than average-case hard problems).

of total NP search problems called TFNP [MP91], was defined by Papadimitriou [Pap94] and has been shown to capture the complexity of computing Nash equilibria [DGP06, CDT09]. It was recently shown [BPR15] that IO and injective OWFs can be used (in a black-box way) to construct hard problems in PPAD. Put together with our separation, we get that there is no black-box construction of an SZK (resp. $\mathsf{NP} \cap \mathsf{coNP}$) hard problem from PPAD-hardness.[4]

Given that TFNP, which contains PPAD, is commonly thought of as a search version of $\mathsf{NP} \cap \mathsf{coNP}$, it is interesting to note that the result shows that hardness in $\mathsf{NP} \cap \mathsf{coNP}$ (of decisional problems) does not follow from hardness in TFNP (aka, hardness of search problems) in a black-box way. Namely, there is no black-box "search-to-decision reduction" between these classes.

The Positive Result: Collision-Resistant Hashing from Strong SZK*-Hardness.* We end our paper with a positive result. While most of our focus has been on showing that hardness in SZK and $\mathsf{NP} \cap \mathsf{coNP}$ does *not* follow from cryptography, here we ask the "inverse question", namely whether certain cryptographic primitives can be built from other cryptographic primitives together with hardness in certain structured complexity classes. Little is known in this direction with the exception of the beautiful work of Ostrovsky [Ost91] which constructs a OWF from average-case SZK-hardness, and the recent work of Applebaum and Raykov [AR16] who showed that average-case hardness in the subclass $\mathsf{PRE} \subseteq \mathsf{SRE} \subseteq \mathsf{SZK}$ of languages with a perfect randomized encoding gives us collision-resistant hashing.

We construct collision-resistant hashing from a strong form of SZK-hardness and IO. It was previously known [AS15] that IO by itself does not imply collision-resistant hashing in a black-box way; we show that it does if one adds SZK-hardness as a "catalyst". Slightly more precisely, in the SZK-complete problem $\mathbf{SD}^{1/3,2/3}$ is required to distinguish between distributions that are 1/3-close from ones that are 2/3-far. We show that IO together with average-case hardness of $\mathbf{SD}^{0,1}$ (a stronger assumption) implies collision-resistant hashing.

Theorem 1.5 (Informal). *Assuming average-case hardness of* $\mathbf{SD}^{0,1}$ *and the existence of IO, there is a collision-resistant hashing scheme.*

Organization. Due to the paucity of space, most of the proofs are deferred to the full version. We give an overview of the methodology and techniques used in the following Sect. 1.2. The black-box separation between SZK and IO (plus OWPs) is stated in Sect. 2. The separation between $\mathsf{NP} \cap \mathsf{coNP}$ and IO (plus injective OWFs) is described in Sect. 3.

1.2 Overview of Techniques

We now give an overview of our approach and main ideas. We start by discussing how to capture fully black-box constructions in the context of indistinguishabil-

[4] We note that in concurrent and independent work, Rosen et al. [RSS16] show that one-way functions do not have black-box reductions to PPAD-hardness, which combined with [Ost91], also yields a separation between SZK and PPAD.

ity obfuscation following [AS15]. We then recall the common methodology for ruling out black-box constructions [IR89,RTV04,BBF13], and explain the main ideas behind our impossibility results for SZK and NP ∩ coNP. In the last part of this section, we outline the construction of collision-resistant hashing from indistinguishability obfuscation and SZK-hardness and the main ideas behind it.

Indistinguishability Obfuscation and Black-Box Constructions. Traditionally, when thinking about a *black-box construction* of one cryptographic primitive $\mathcal{P}'$ (e.g., a pseudo-random generator) from a primitive $\mathcal{P}$ (e.g., a one-way function), we mean that all algorithms in the construction of $\mathcal{P}'$ invoke $\mathcal{P}$ as a black-box, oblivious of its actual implementation. This is hardly the case in constructions based on indistinguishability obfuscation where circuits that explicitly invoke the primitive $\mathcal{P}$ may be obfuscated.

Nonetheless, as observed by Asharov and Segev [AS15], in almost all existing constructions, the code implementing $\mathcal{P}$ is used in a very restricted manner. Typically, obfuscated circuits can be implemented as oracle aided circuits $C^{\mathcal{P}}$ that are completely black-box in $\mathcal{P}$, where $\mathcal{P}$ is some low-level primitive, such as a one-way function. Indeed, in most cases the circuits obfuscated are symmetric-key primitives, such as puncturable pseudo-random functions [SW14], which can be constructed in a black-box way from one-way functions (in some constructions more structured low-level primitives may be used, like injective one-way functions, or one-way permutations). Furthermore, in these constructions, the obfuscator $i\mathcal{O}$ itself is also treated as a black-box.

Accordingly, almost all existing constructions based on indistinguishability obfuscation can be cast into a model in which indistinguishability obfuscation exists for oracle-aided circuits $C^{\mathcal{P}}$, where $\mathcal{P}$ is say a one-way function, and both $\mathcal{P}$ and the obfuscator $i\mathcal{O}$ can only be accessed as black-boxes. On top of that, they can be proven secure in this model by a *black-box reduction* that makes black-box use of $(\mathcal{P}, i\mathcal{O})$ and any attacker against the constructed primitive $\mathcal{P}'$. Such constructions where both the construction itself and the reduction are black-box are called *fully black-box constructions* [RTV04]. Following Asharov and Segev [AS15,AS16], we shall prove our results in this model, ruling out black-box constructions of hard problems in SZK and NP ∩ coNP based on indistinguishability obfuscation for oracle-aided circuits. Further details follow.

Ruling out Black-Box Reductions. We prove our results in the model described above following the methodology of oracle separations (see e.g. [IR89,Sim98, RTV04,HR04]). Concretely, to prove that there is no fully black-box construction of a primitive $\mathcal{P}'$ from primitive $\mathcal{P}$, we demonstrate oracles $(\Psi, \mathcal{A})$ such that:

- relative to Ψ, there exists a construction $C_{\mathcal{P}}^{\Psi}$ realizing $\mathcal{P}$ that is secure in the presence of $\mathcal{A}$,
- but *any* construction $C_{\mathcal{P}'}^{\Psi}$ realizing $\mathcal{P}'$ can be broken in the presence of $\mathcal{A}$.

Indeed, if such oracles $(\Psi, \mathcal{A})$ exist, then no efficient reduction will be able to use (as a black-box) the attacker $\mathcal{A}$ against $\mathcal{P}'$ to break $\mathcal{P}$ (as the construction of $\mathcal{P}$ is secure in the presence of $\mathcal{A}$). In our case, we would like to apply this

paradigm rule out black-box constructions of hard instances in either SZK or $\mathsf{NP} \cap \mathsf{coNP}$ from a low-level primitive (e.g. a one-way function) indistinguishability obfuscation for oracle-aided circuits. We next outline the main ideas behind the construction and analysis of the oracles $(\Psi, \mathcal{A})$ in each of the two cases.

Ruling out Black-Box Constructions of Hard SZK *Problems.* As explained in the previous section, we focus on the characterization of SZK by its complete problem: the statistical difference problem $\mathbf{SD}$ [SV03]. We demonstrate oracles $(\Psi, \mathcal{A})$ such that relative to Ψ there exist constructions of one-way permutations (OWPs) and IO for circuits with OWP gates, and these constructions are secure in the presence of $\mathcal{A}$. At the same time, $\mathcal{A}$ will decide (in the worst-case) $\mathbf{SD}^{\Psi}$. Since $\mathbf{SD}$ is complete for SZK in a relativizing manner, deciding $\mathbf{SD}^{\Psi}$ suffices to break SZK^{Ψ}. That is, $\mathcal{A}$ will decide *all* instances (C_0^{Ψ}, C_1^{Ψ}) of circuit samplers that only use the IO and OWPs realized by Ψ in a black-box manner. We next explain how each of the two are constructed.

The construction of Ψ follows a general recipe suggested in [AS15, AS16]. The oracle consists of three parts $(f, \mathcal{O}, \mathsf{Eval}^{f,\mathcal{O}})$ where:

1. f is a random permutation, realizing the one-way permutation primitive.
2. $\mathcal{O}$ is a random injective function, realizing the obfuscation algorithm. It takes as input an oracle-aided circuit $C^{(\cdot)}$ along with randomness r and outputs an obfuscation $\widehat{C} = \mathcal{O}(C, r)$.
3. $\mathsf{Eval}^{\mathcal{O},f}$ realizes evaluation of obfuscated circuits. On input $(\widehat{C}, x)$, it inverts $\mathcal{O}$ to find (C, r), and outputs $C^f(x)$. If $\widehat{C}$ is not in the image of $\mathcal{O}$, it returns $\perp$.

The above construction readily satisfies the syntactic (or "functionality") requirements of one-way permutations and indistinguishability obfuscation. Furthermore, using standard techniques, it is not hard to show that relative to Ψ, the function f is one-way and $\mathcal{O}$ satisfies IO indistinguishability requirement. The challenge is to now come up with an oracle $\mathcal{A}$ that, on one hand, will decide $\mathbf{SD}^{\Psi}$, but on the other, will not compromise the security of the latter primitives.

Recall that deciding $\mathbf{SD}^{\Psi}$ means that given two oracle-aided circuit samplers (C_0, C_1) such that the statistical distance of the corresponding distributions $(\boldsymbol{C}_0^{\Psi}, \boldsymbol{C}_1^{\Psi})$ is $s = \Delta(\boldsymbol{C}_0^{\Psi}, \boldsymbol{C}_1^{\Psi}) \in [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$, the oracle $\mathcal{A}$ must decide in which of the two intervals s lies, whereas if the promise is not satisfied and $s \in (\frac{1}{3}, \frac{2}{3})$, there is no requirement whatsoever. With this in mind, a first naive attempt would be the following. $\mathcal{A}$ will have unbounded access to Ψ, give a query (C_0, C_1), it would compute $s = \Delta(\boldsymbol{C}_0, \boldsymbol{C}_1)$, and simply say whether $s < \frac{1}{2}$ or $s \geq \frac{1}{2}$. While such an oracle would definitely decide $\mathbf{SD}^{\Psi}$, it is not too hard to show that it is simply too powerful, and would not only break IO and OWPs, but would, in fact, allow solving any problem in NP^{Ψ} (or even in PP^{Ψ}). Other naive attempts such as refusing to answer outside the promise intervals, encounter a similar problem.

At high-level, the problem with such oracles is that solutions to hard problems can be easily correlated with "tiny" differences in the statistical distance of the two input circuits, whereas the above oracle may reflect tiny changes when the statistical distance is close to some threshold (1/2 in the above example) on which the oracle changes its behaviour. This motivates our actual definition of $\mathcal{A}$ as

a *noisy oracle* that produces its answer, not according to some fixed threshold, but according to a random threshold, chosen afresh for each and every query. Concretely, the oracle, which we call StaDif^{Ψ}, for any query (C_0, C_1), chooses a uniformly random threshold $t \leftarrow (\frac{1}{3}, \frac{1}{3})$, and answers accordingly:

$$\mathsf{StaDif}^{\Psi}(C_0, C_1) = \begin{cases} Y & \text{if } s \geq t \text{ (far distributions)} \\ N & \text{if } s < t \text{ (similar distributions)} \end{cases}.$$

The main challenge in proving that the security of the IO and OWPs realized by $\mathcal{A}$ is not compromised by this oracle is that StaDif^{Ψ} has the power to query Ψ on exponentially many points in order to compute s. For instance, it may query Ψ on the preimage of a OWP challenge $f(x)$ or of a given obfuscation $\mathcal{O}(C, r)$. The key observation behind the proof is that the oracle's final answer still does not reflect how Ψ behaves locally on random points.

Intuitively, choosing the threshold t at random, for each query (C_0, C_1), guarantees that with high probability t is "far" from the corresponding statistical distance $s = \Delta(C_0^{\Psi}, C_1^{\Psi})$. Thus, changing the oracle Ψ on, say, a single input x, such as the preimage of an OWP challenge $f(x)$, should not significantly change s and will not affect the oracle's answer; that is, unless the circuits query Ψ on x with high probability to begin with. We give a reduction showing that we can always assume that (C_0, C_1) are "smooth", in the sense that they do not make any specific query to Ψ with too high probability.

Following this intuition, we are able to show that through such local changes that go undetected by StaDif^{Ψ}, we can move to an ideal world where inverting the OWP or breaking IO can be easily shown to be impossible. We refer the reader to the full version for further details.

Ruling out Black-Box Constructions of Hard $\mathsf{NP} \cap \mathsf{coNP}$ *Problems.* As mentioned earlier, a fully black-box construction of hard problems in $\mathsf{NP} \cap \mathsf{coNP}$ is actually known assuming one-way permutations (OWPs), and cannot be ruled out as in the case of SZK. Instead, we rule out constructions from (non-surjective) injective one-way functions (IOWFs) and IO for circuits with IOWF gates. This generalizes several previous results by Blum and Impagliazzo [BI87] and Rudich [Rud88], showing that OWFs do not give hardness in $\mathsf{NP} \cap \mathsf{coNP}$, by Matsuda and Matsuura [MM11], showing that IOWFs do not give OWPs (which are a special case of hardness $\mathsf{NP} \cap \mathsf{coNP}$), and by Asharov and Segev [AS16], showing that OWFs and IO for circuits with OWF gates do not give OWPs. In fact, our approach yields a new (and rather different) proof for each one of these results.

We follow a similar methodology to one we used for the case of SZK. That is, we would like to come up with oracles $(\Psi, \mathcal{A})$ such that Ψ realizes IOWFs and IO for circuits with IOWFs gates, which are both secure in the presence of $\mathcal{A}$, whereas black-box constructions of problems in $\mathsf{NP} \cap \mathsf{coNP}$ from these primitives can be easily solved by $\mathcal{A}$. By black-box constructions here we mean a pair of efficient oracle-aided non-deterministic verifiers $V_0^{(\cdot)}, V_1^{(\cdot)}$ that for every oracle Ψ implementing IOWFs and IO, yield co-languages $\overline{L}^{\Psi}, L^{\Psi}$ in $\mathsf{NP} \cap \mathsf{coNP}[\Psi]$.

The requirement that V_0, V_1 give a language in $\mathsf{NP} \cap \mathsf{coNP}$ for *every* oracle implementing IOWFs and IO follows previous modeling [BI87],[5] and aligns with how we usually think about *correctness* of black-box constructions of cryptographic primitives. For instance, the construction of public-key encryption from trapdoor permutations is promised to be correct, for all oracles implementing the trapdoor permutation. Similarly, the construction of hard $\mathsf{NP} \cap \mathsf{coNP}$ languages from one-way permutations, give an $\mathsf{NP} \cap \mathsf{coNP}$ language for any oracle implementing a permutation.[6]

We stress that a construction where correctness is only guaranteed for particular (even if natural) oracles may definitely exist. This is for example the case if we only consider implementations of IO similar to those presented above in the context of SZK. Indeed, in that construction the implementation of IO has an additional property—it allows identifying *invalid obfuscations* (the Eval oracle would simply return $\perp$ on such obfuscations). This "verifiability" property coupled with the injectivity of obfuscators actually imply a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$ in a black-box way.[7] Our separation thus leverages the fact that IO need not necessarily be verifiable, and rules out constructions that are required to be correct for any implementation of IO, even a non-verifiable one.

Accordingly, the oracles $\Psi = (f, \mathcal{O}, \mathsf{Eval}^{f,\mathcal{O}})$ that we consider are a tweaked version of the oracles considered in the SZK case. Now f is a random injective function that is expanding, rather than a permutation, the oracle $\mathcal{O}$ is defined as before, and the oracle $\mathsf{Eval}^{f,\mathcal{O}}$ is defined as before for valid obfuscations $\widehat{C} \in \mathrm{Image}(\mathcal{O})$ *but is allowed to act arbitrarily for invalid obfuscations.* As for $\mathcal{A}$, this time it is trivially implemented by an oracle Decide^{Ψ} that, given input x, simply returns the unique bit b such that $V_b(x) = 1$, namely it just decides the corresponding language L^{Ψ}.

In the results mentioned above [Rud88, MM11, AS16], it is actually shown that any query to such an oracle can be completely simulated with a small number of queries to Ψ.[8] We do not show such a simulation process. Instead, we take a different approach inspired by our proof for the SZK setting described above. Roughly speaking, we show that somewhat similarly to our statistical difference oracle StaDif^{Ψ}, the oracle Decide^{Ψ} is also rather robust to random local changes. The main observation here is that for any fixed yes-instance $x \in L^{\Psi}$, tweaking Ψ at a random input into a new oracle Ψ', it is likely that x will still

[5] Rudich [Rud88] also considered a slight relaxation of constructions that are correct for an overwhelming fraction of oracles rather than all.

[6] We note that this issue does not come up for black-box constructions of SZK *promise* problems, because the construction is allowed to yield instances that do not obey the promise; there correctness is always guaranteed, and the only question is whether the instances that do satisfy the promise are hard to decide.

[7] E.g. the language of all valid obfuscations and indices i, such that the ith bit of the obfuscated circuit is 1.

[8] More accurately, this is the case for Rudich's result for $\mathsf{NP} \cap \mathsf{coNP}$, whereas for the other results that rule out constructions of one-way permutations, one can simulate an analog of Decide that inverts the permutation.

be a yes-instance in $L^{\Psi'}$, as long as Ψ' is in our allowed family of oracles and $L^{\Psi'}$ is indeed in $\mathsf{NP} \cap \mathsf{coNP}[\Psi']$ (and the same is true for no-instances).

In slightly more detail, fixing a witness w such that $V_1^{\Psi}(x, w) = 1$, we can show that since V_1 makes a small number of oracle calls, with high probability tweaking the oracle Ψ at a random place will not affect these oracle calls and thus $V_1^{\Psi'}(x, w) = V_1^{\Psi}(x, w) = 1$. Then, assuming $L^{\Psi'}$ is guaranteed to be in $\mathsf{NP} \cap \mathsf{coNP}$, we can deduce that x must still a yes-instance (other witnesses for this fact may be added or disappear, but this does not change the oracle's answer). In the body, we argue that indeed $L^{\Psi'} \in \mathsf{NP} \cap \mathsf{coNP}[\Psi']$, where we strongly rely on the fact that arbitrary behavior of Eval is permitted on invalid obfuscations.

Once again, we show that through local changes that go undetected by Decide^{Ψ}, we can move to an ideal world where inverting the IOWF or breaking IO can be easily shown to be impossible. We refer the reader to Sect. 3 for further details.

Implied Separations. As a result of the two separations discussed above, we can rule out black-box constructions of hard problems in SZK or $\mathsf{NP} \cap \mathsf{coNP}$ from various cryptographic primitives or complexity classes. This essentially includes all primitives that have fully black-box constructions from OWPs (or IOWFs) and IO for circuits with OWP (or IWOF) gates. This includes public-key encryption, oblivious transfer, deniable encryption [SW14], functional encryption [Wat15], delegation, [BGL+15, CHJV15, KLW15], hard (on-average) PPAD instances [BPR15], and more.

We note that there a few applications of IO that do not fall under this characterization. For instance, the construction of IO for Turing machines from IO-based succinct randomized encodings [BGL+15, CHJV15, KLW15] involves obfuscating a circuit that itself outputs (smaller) obfuscated circuits. To capture this, we would need to extend the above model to IO for circuits that can also make IO oracle calls (on smaller circuits). Another example is the construction of non-interactive witness indistinguishable proofs from IO [BP15]. There an obfuscated circuit may get as input another obfuscated circuit and would have to internally run it; furthermore, in this application, the code of the obfuscator is used in a (non-black-box) ZAP. Extending the above model to account for this type of IO applications is an interesting question that we leave for future exploration.

The Positive Result: Collision-Resistance from IO and SZK*-Hardness.* We now described the main ideas behind our construction of collision-resistant hash functions. The starting point for the construction is the work of Ishai et al. [IKO05] that shows how to construct collision-resistant hash functions from commitments that are additively homomorphic (for simplicity, say over $\mathbb{F}_2$). The idea is simple: we can hash ℓ bits to m bits, where m is the size of a single bit commitment and ℓ can be arbitrarily longer, as follows. The hash key is a commitment $\gamma := (\mathsf{com}(\beta_1), \ldots, \mathsf{com}(\beta_\ell))$ to a random vector $\beta \in \mathbb{F}_2^\ell$, and hashing $x \in \mathbb{F}_2^\ell$, is done by homomorphically computing a commitment to the inner product

$\mathsf{CRH}_\gamma(x) = \mathsf{com}(\langle \beta, x \rangle)$. Intuitively, the reason this works is that any collision in CRH_γ reveals a vector that is orthogonal to β and thus leaks information about it and violating the hiding of the commitment.

At a high-level, we aim to mimic the above construction based on obfuscation. As a key for the collision-resistant hash we can obfuscate a program Π_β associated with a random vector β that given x outputs a commitment $\mathsf{com}(\langle \beta, x \rangle)$, where the commitment is derandomized using a PRF.[9] The obfuscation $i\mathcal{O}(\Pi_\beta)$ can be thought of as the commitment to β, and evaluating this program at x, corresponds to homomorphic evaluation. Despite the clear intuition behind this construction, it is not clear how to prove its security based on IO. In fact, by the work of Asharov and Segev [AS15], it cannot be proven based on a black-box reduction as long as plain statistically-binding commitments are used, as these can be constructed from OWPs in a fully black-box manner, and [AS15] rule out black-box constructions of collision-resistant hashing from OWPs and IO for circuits with OWP gates.

We show, however, that relying on a relaxed notion of perfectly-hiding commitments, as well as subexponential hardness of IO and puncturable PRFs, the construction can be proven secure. The perfect hiding of the commitment is leveraged in a probabilistic IO argument [CLTV15] that involves a number of hybrids larger than the overall number of commitments. We then observe that these relaxed commitments follow from average-case hardness of the polar statistical difference problem $\mathbf{SD}^{0,1}$.[10]

2 One-Way Permutations, Indistinguishability Obfuscation, and Hardness in SZK

In this section, we ask which cryptographic primitives imply hardness in the class statistical zero-knowledge (SZK). Roughly speaking, we show that one-way permutations (OWPs) and indistinguishability obfuscation (IO), for circuits with OWP-gates, do not give rise to a black-box construction of hard problems in SZK. This, in turn implies that many cryptographic primitives (e.g., public-key encryption, functional encryption, and delegation), and hardness in certain low-level complexity classes (e.g. PPAD), also do not yield black-box constructions of hard problems in SZK.

We first motivate and define a framework of SZK relative to oracles, define fully black-box constructions of hard SZK problems, and then move on to the actual separation.

2.1 SZK and Statistical Difference

The notion of statistical zero-knowledge proofs was introduced in the seminal work of Goldwasser et al. [GMR85]. The class of promise problems with

[9] In the body, we describe a slightly more abstract construction where inner product is replaced by an arbitrary 2-universal hash function.

[10] Similar SZK-hardness is known to imply statistically-hiding commitments against malicious receivers, but with a larger (constant) number of rounds [OV08].

statistical zero-knowledge proofs (SZK) can be characterized by several complete problems, such as *statistical difference* [SV03] and *entropy difference* [GV99] (see also [Vad99] and references within). We shall focus on the characterization of SZK by the statistical difference problem. Here an instance is a pair of circuit samplers $C_0, C_1 : \{0,1\}^n \to \{0,1\}^m$ with the promise that the statistical distance $s = \Delta(\boldsymbol{C}_0, \boldsymbol{C}_1)$ of the corresponding distributions is either large (say, $s \geq 2/3$) or small (say, $s \leq 1/3$). The problem is to decide which is the case.

Hard Statistical Difference Problems from Cryptography: Motivation. SZK hardness, and in particular hard statistical difference problems, are known to follow from various number-theoretic and lattice problems that are commonly used in cryptography, such as Decision Diffie-Hellman, Quadratic Residuosity, and Learning with Errors. We ask more generally which cryptographic primitives can be shown to imply such hardness, with the intuition that such primitives are *structured* in a certain way. In particular, whereas one would not expect a completely unstructured object like one-way functions to imply such hardness, what can we say for instance about public-key encryption, or even indistinguishability obfuscation (which has proven to be structured enough to yield almost any known cryptographic goal).

We prove that none of these primitives imply such hardness through the natural class of black-box constructions and security reductions. To understand what a black-box construction of a hard statistical difference problem means, let us look at a specific example of the construction of such a problem from *rerandomizable encryption*. In a (say, symmetric-key) rerandomizable encryption scheme, on top of the usual encryption and decryption algorithms $(\mathsf{Enc}, \mathsf{Dec})$ there is a ciphertext rerandomization algorithm ReRand that can statistically refresh ciphertexts. Namely, for any ciphertext CT encrypting a bit b, $\mathsf{ReRand}(\mathsf{CT})$ produces a ciphertext that is statistically close to a fresh encryption $\mathsf{Enc}(b)$. Note that this immediately gives rise to a hard statistical difference problem: given a pair of ciphertexts $(\mathsf{CT}, \mathsf{CT}')$, decide whether the corresponding rerandomized distributions given by the circuits $(C_0(\cdot), C_1(\cdot)) := (\mathsf{ReRand}(\mathsf{CT}; \cdot), \mathsf{ReRand}(\mathsf{CT}'; \cdot))$ are statistically far or close. Indeed, this corresponds to whether they encrypt the same bit or not, which is hard to decide by the security of the encryption scheme.

A feature of this construction of hard statistical difference instances is that, similarly to most constructions in cryptography, it is *fully black-box* [RTV04] in the sense that the circuits C_0, C_1 only make black-box use of the encryption scheme's algorithms, and can in fact be represented as oracle-aided circuits $(C_0^{\mathsf{ReRand}(\cdot)}, C_1^{\mathsf{ReRand}(\cdot)})$. Furthermore, "hardness" can be shown by a black-box reduction that can use any decider for the problem in a black-box way to break the underlying encryption scheme. More generally, one can consider the statistical difference problem relative to different oracles implementing different cryptographic primitives and ask when can hardness be shown based on a black-box reduction. We will rule out such reductions relative to IO and OWPs (and everything that follows from these in a fully black-box way).

2.2 Fully Black-Box Constructions of Hard SD Problems from IO and OWPs

We start by defining statistical difference problem relative to oracles. In the following definition, for an oracle-aided (sampler) circuit $C^{(\cdot)}$ with n-bit input and an oracle Ψ, we denote by $\boldsymbol{C}^{\Psi}$ the output distribution $C^{\Psi}(r)$ where $r \leftarrow \{0,1\}^n$. For two distributions $\mathbf{X}$ and $\mathbf{Y}$ we denote their statistical distance by $\Delta(\mathbf{X}, \mathbf{Y})$.

Definition 2.1 (Statistical difference relative to oracles). *For an oracle Ψ, the statistical difference promise problem relative to Ψ, denoted as $\mathbf{SD}^{\Psi} = (\mathbf{SD}^{\Psi}_Y, \mathbf{SD}^{\Psi}_N)$, is given by*

$$\mathbf{SD}^{\Psi}_Y = \left\{ (C_0, C_1) \;\middle|\; \Delta(\boldsymbol{C}^{\Psi}_0, \boldsymbol{C}^{\Psi}_1) \geq \frac{2}{3} \right\},$$
$$\mathbf{SD}^{\Psi}_N = \left\{ (C_0, C_1) \;\middle|\; \Delta(\boldsymbol{C}^{\Psi}_0, \boldsymbol{C}^{\Psi}_1) \leq \frac{1}{3} \right\}.$$

We now formally define the class of constructions and reductions ruled out. That is, *fully black-box* constructions of hard statistical distance problems from OWPs and IO for OWP-aided circuits. The definition is similar in spirit to those in [AS15, AS16], adapted to our context of SZK-hardness.

Definition 2.2. *A fully black-box construction of a hard statistical distance problem from OWPs and IO for the class $\mathcal{C}$ of circuits with OWP-gates consists of a collection of oracle-aided circuit pairs $\Pi^{(\cdot)} = \left\{ \Pi^{(\cdot)}_n = \left\{ (C^{(\cdot)}_0, C^{(\cdot)}_1) \in \{0,1\}^{n \times 2} \right\} \right\}_{n \in \mathbb{N}}$ and a probabilistic oracle-aided reduction $\mathcal{R}$ that satisfy:*

- ***Black-box security proof:*** *There exist functions $q_{\mathcal{R}}(\cdot), \varepsilon_{\mathcal{R}}(\cdot)$ such that the following holds. Let f be any distribution on permutations and let $i\mathcal{O}$ be any distribution on functions such that $\widehat{C}^f \equiv C^f$ for any $C^{(\cdot)}$ and r, where $\widehat{C}^{(\cdot)} := i\mathcal{O}(C^{(\cdot)}, r)$. Then for any probabilistic oracle-aided $\mathcal{A}$ that* decides *Π* in the worst-case*, namely, for all $n \in \mathbb{N}$*

$$\Pr_{f, i\mathcal{O}, \mathcal{A}} \left[\mathcal{A}^{f, i\mathcal{O}}(C_0, C_1) = B \quad \textit{for all} \quad \begin{array}{c} (C_0, C_1) \in \Pi_n, B \in \{Y, N\} \\ \textit{such that } (C_0, C_1) \in \mathbf{SD}^{f, i\mathcal{O}}_B \end{array} \right] = 1$$

  the reduction breaks either f or $i\mathcal{O}$*, namely, for infinitely many $n \in \mathbb{N}$ either*

$$\Pr_{\substack{x \leftarrow \{0,1\}^n \\ f, i\mathcal{O}, \mathcal{A}}} \left[\mathcal{R}^{\mathcal{A}, f, i\mathcal{O}}(f(x)) = x \right] \geq \varepsilon_{\mathcal{R}}(n),$$

  or

$$\left| \Pr \left[\mathsf{Exp}^{\mathsf{iO}}_{(f, i\mathcal{O}), i\mathcal{O}, \mathcal{C}, \mathcal{R}^{\mathcal{A}}}(n) = 1 \right] - \frac{1}{2} \right| \geq \varepsilon_{\mathcal{R}}(n),$$

where in both $\mathcal{R}$ makes at most $q_{\mathcal{R}}(n)$ queries to any of its oracles $(\mathcal{A}, f, i\mathcal{O})$, and any query $(C_0^{(\cdot)}, C_1^{(\cdot)})$ it makes to $\mathcal{A}$ consists of circuits that also make at most $q_{\mathcal{R}}(n)$ queries to their oracles $(f, i\mathcal{O})$. The random variable $\mathsf{Exp}^{\mathsf{iO}}_{(f,i\mathcal{O}),i\mathcal{O},\mathcal{C},\mathcal{R}^{\mathcal{A}}}(n)$ represents the reductions winning probability in the IO security game relative to $(f, i\mathcal{O})$.

We make several remarks about the definition:

- **Correctness.** Typically, we also require certain *correctness* from the black-box construction. For instance, in the next section, we shall require that the construction always satisfies the $\mathsf{NP} \cap \mathsf{coNP}$ structure. In the above definition, the construction is allowed to yield instances $(C_0^{f,i\mathcal{O}}, C_1^{f,i\mathcal{O}})$ that do not satisfy the SZK promise; namely $(C_0^{f,i\mathcal{O}}, C_1^{f,i\mathcal{O}}) \notin \mathbf{SD}_Y^{f,i\mathcal{O}} \cup \mathbf{SD}_N^{f,i\mathcal{O}}$. It is natural to think of more stringent definitions that require that the corresponding problem $\Pi^{f,i\mathcal{O}}$ is non-trivial, in the sense that $\Pi^{f,i\mathcal{O}} \cap \mathbf{SD}_Y^{f,i\mathcal{O}} \neq \emptyset$ and $\Pi^{f,i\mathcal{O}} \cap \mathbf{SD}_N^{f,i\mathcal{O}} \neq \emptyset$ (which is the case for known constructions of SZK hardness from cryptographic primitives). Our impossibility is more general and would, in particular, rule out such definitions as well.
- **Worst-Case vs. Average-Case Hardness.** In the above, we address *worst-case hardness*, in the sense that the reduction $\mathcal{R}$ has to break the underlying primitives only given a decider $\mathcal{A}$ that is always correct. One could further ask whether IO and OWPs even imply average-case hardness in SZK (as do many of the algebraic hardness assumptions in cryptography). Ruling out worst-case hardness (as we will do shortly) in particular rules out such average-case hardness as well.
- **IO for Oracle-Aided Circuits.** Following [AS15, AS16], we consider indistinguishability obfuscation for oracle-aided circuits C^f that can make calls to the one-way permutation oracle. This model captures constructions where IO is applied to circuits that use pseudo-random generators, puncturable pseudo-random functions, or injective one-way functions as all of those have fully black-box constructions from one-way permutations (see further discussion in [AS15]). This includes almost all known constructions from IO, including public-key encryption, deniable encryption [SW14], functional encryption [Wat15], delegation [BGL+15, CHJV15, KLW15], and hard (on-average) PPAD instances [BPR15]. Accordingly, separating SZK from IO and OWPs in this model, results in a similar separation between SZK and any one of these primitives.

  We note that there a few applications though that do not fall under this model. The first is in applications where the obfuscated circuit might itself output (smaller) obfuscated circuit, for instance in the construction of IO for Turing machines from IO-based succinct randomized encodings [BGL+15, CHJV15, KLW15]. To capture such applications, one would have to extend the model to also account for circuits with IO gates (and not only OWP gates). A second example is the construction of non-interactive witness indistinguishable proofs from IO [BP15]. There an obfuscated circuit may get as input another obfuscated circuit and would have to internally run it;

furthermore, in this application, the code of the obfuscator is used in a (non-black-box) ZAP. Extending our results (and those of [AS15, AS16]) to these models is an interesting question, left for future work.

– **Security Loss.** In the above definition the functions $q_{\mathcal{R}}$ and $\varepsilon_{\mathcal{R}}$ capture the *security loss* of the reduction. Most commonly in cryptography, the query complexity is polynomial $q_{\mathcal{R}}(n) = n^{O(1)}$ and the probability of breaking the underlying primitive is inverse polynomial $\varepsilon_{\mathcal{R}}(n) = n^{-O(1)}$. Our lower-bounds will in-fact apply for *exponential* $q_{\mathcal{R}}, \varepsilon_{\mathcal{R}}^{-1}$. This allows capturing also constructions that rely on subexponentially secure primitives (e.g., [BGL+15, CHJV15, KLW15, BPR15, BPW16]).

Ruling Out Fully Black-Box Constructions: A Road Map. Our main result in this section is that a fully black-box construction of a hard statistical difference problem from IO and OWPs does not exist. Furthermore, this holds even if the latter primitives are exponentially secure.

Theorem 2.3. *Any fully black-box construction of a statistical difference problem Π from OWPs and IO for circuits with OWP gates has an exponential security loss:* $\max(q_{\mathcal{R}}(n), \varepsilon_{\mathcal{R}}^{-1}(n)) \geq \Omega(2^{n/12})$.

The proof of the theorem follows a common methodology (applied for instance in [HR04, HHRS15, AS15]). We exhibit two (distributions on) oracles $(\Psi, \mathsf{StaDif}^{\Psi})$, where Ψ realizes OWPs and IO for circuits with OWP gates, and StaDif^{Ψ} that decides $\mathbf{SD}^{\Psi}$, the statistical difference problem relative to Ψ, in the worst case. Since $\mathbf{SD}$ is complete for SZK in a relativizing manner, solving $\mathbf{SD}^{\Psi}$ suffices to break SZK^{Ψ}. We then show that the primitives realized by Ψ are (exponentially) secure even in the presence of StaDif^{Ψ}. Then viewing StaDif as a worst-case decider $\mathcal{A}$ (as per Definition 2.2) directly implies Theorem 2.3, ruling out fully black-box constructions with a subexponential security loss. We defer the oracle description and the proof to the full version.

3 One-Way Functions, Indistinguishability Obfuscation, and Hardness in NP ∩ coNP

In this section, we show that injective one-way functions (IOWFs) and indistinguishability obfuscation (IO), for circuits with IOWF-gates, do not give rise to a black-box construction of hard problems in $\mathsf{NP} \cap \mathsf{coNP}$. This can be seen as a generalization of previous separations by Rudich [Rud88], showing that OWFs do not give hardness in $\mathsf{NP} \cap \mathsf{coNP}$, by Matsuda and Matsuura [MM11], showing that IOWFs do not give one-way permutations (which are a special case of hardness $\mathsf{NP} \cap \mathsf{coNP}$), and by Asharov and Segev [AS16], showing that OWFs and IO do not give one-way permutations. As in the previous section, the result implies that many cryptographic primitives and hardness in PPAD, also do not yield black-box constructions of hard problems in $\mathsf{NP} \cap \mathsf{coNP}$.

We first define the framework of $\mathsf{NP} \cap \mathsf{coNP}$ relative to oracles, define fully black-box constructions of hard $\mathsf{NP} \cap \mathsf{coNP}$ problems, and then move on to the actual separation.

3.1 NP ∩ coNP

Throughout, we shall canonically represent languages $L \in \mathsf{NP} \cap \mathsf{coNP}$ by their corresponding non-deterministic poly-time verifiers V_1, V_0, where

$$L = \left\{x \in \{0,1\}^\star \;\middle|\; \exists w : V_1(x,w) = 1\right\},$$
$$\overline{L} = \left\{x \in \{0,1\}^\star \;\middle|\; \exists w : V_0(x,w) = 1\right\} = \{0,1\}^\star \setminus L.$$

Hardness in $\mathsf{NP} \cap \mathsf{coNP}$ *from Cryptography - Motivation.* Hard (on average) problems in $\mathsf{NP} \cap \mathsf{coNP}$ are known to follow based on certain number-theoretic problems in cryptography, such as Discrete Log and Factoring. As in the previous section for SZK, we are interested in understanding which cryptographic primitives would imply such hardness, again with the intuition that these should be appropriately structured. For instance, it is known [Bra79] that any one-way permutation $f : \{0,1\}^n \to \{0,1\}^n$ implies a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$, e.g. given an index $i \in [n]$ and an image $f(x)$ find the i-th pre-image bit x_i. In contrast, in his seminal work, Rudich [Rud88] proved that completely unstructured objects like one-way functions cannot construct even worst-case hard instances by fully black-box constructions. Here a fully black-box construction essentially means that the non-deterministic verifiers only make black-box use of the OWF (or OWP in the previous example) and the reduction establishing the hardness is also black-box (in both the adversary and the OWF).

But what about more structured primitives such as public-key encryption, oblivious transfer, or even indistinguishability obfuscation. Indeed, IO (plus OWFs) has-been shown to imply hardness in PPAD and more generally in the class TFNP of total search problems, which is often viewed as the search analog of $\mathsf{NP} \cap \mathsf{coNP}$ [MP91]. We will show, however, that fully black-box constructions do not give rise to a hard problem in $\mathsf{NP} \cap \mathsf{coNP}$ from OWFs (or even injective OWFs) and IO for circuits with OWF gates.

3.2 Fully Black-Box Constructions of Hardness in NP ∩ coNP from IO and IOWFs

We start by defining $\mathsf{NP} \cap \mathsf{coNP}$ relative to oracles [Rud88]. This, in particular, captures black-box constructions of such languages from cryptographic primitives, such as one-way functions in [Rud88] or indistinguishability obfuscation, which we will consider in this work.

Definition 3.1 ($\mathsf{NP} \cap \mathsf{coNP}$ **relative to oracles).** *Let* $\mathfrak{S}$ *be a family of oracles and let* $V_1^{(\cdot)}, V_0^{(\cdot)}$ *be a pair of oracle-aided non-deterministic polynomial-time verifiers. We say that* V_1, V_0 *define a collection of languages* $L^{\mathfrak{S}} = \left\{L^\Gamma \;\middle|\; \Gamma \in \mathfrak{S}\right\}$ *in* $\mathsf{NP} \cap \mathsf{coNP}$ *relative to* $\mathfrak{S}$ *if for any* $\Gamma \in \mathfrak{S}$*, the machines* V_1^Γ, V_0^Γ *define a language* $L^\Gamma \in \mathsf{NP}^\Gamma \cap \mathsf{coNP}^\Gamma$*. That is*

$$L^\Gamma = \left\{x \in \{0,1\}^\star \;\middle|\; \exists w : V_1^\Gamma(x,w) = 1\right\},$$
$$\overline{L}^\Gamma = \left\{x \in \{0,1\}^\star \;\middle|\; \exists w : V_0^\Gamma(x,w) = 1\right\} = \{0,1\}^\star \setminus L.$$

We now formally define the class of constructions and reductions ruled out. That is, *fully black-box* constructions of hard problems in $\mathsf{NP} \cap \mathsf{coNP}$ from injective one-way functions (IOWFs) and IO for IOWF-aided circuits. The definition is similar in spirit to those in [AS15, AS16] and in the Sect. 2, adapted to the context of $\mathsf{NP} \cap \mathsf{coNP}$ hardness.

Definition 3.2. *A fully black-box construction of a hard* $\mathsf{NP} \cap \mathsf{coNP}$ *problem* L *from IOWFs and IO for the class* $\mathcal{C}$ *of circuits with IOWF-gates is given by two oracle aided poly-time machines* (V_0, V_1) *and a probabilistic oracle-aided reduction* $\mathcal{R}$ *that satisfy:*

1. ***Structure:*** *Let* $\mathfrak{S}$ *be the family of all oracles* $(f, i\mathcal{O})$ *such that* f *is injective and* $i\mathcal{O}$ *is a function such that* $\widehat{C}^f \equiv C^f$ *for any* $C^{(\cdot)} \in \mathcal{C}$*,* r*, and* $\widehat{C}^{(\cdot)} := i\mathcal{O}(C, r)$*. Then* (V_0, V_1) *define a language* $L^{f,i\mathcal{O}} \in \mathsf{NP}^{f,i\mathcal{O}} \cap \mathsf{coNP}^{f,i\mathcal{O}}$ *relative to any oracle* $(f, i\mathcal{O}) \in \mathfrak{S}$ *(as per Definition 3.1).*
2. ***Black-box security proof:*** *There exist functions* $q_{\mathcal{R}}(\cdot), \varepsilon_{\mathcal{R}}(\cdot)$ *such that the following holds. Let* $(f, i\mathcal{O})$ *be any distribution supported on the family* $\mathfrak{S}$ *defined above. Then for any probabilistic oracle-aided* $\mathcal{A}$ *that* decides $L^{f,i\mathcal{O}}$ in the worst-case*, namely, for all* $n \in \mathbb{N}$

$$\Pr_{f,i\mathcal{O},\mathcal{A}}\left[\mathcal{A}^{f,i\mathcal{O}}(x) = b \quad \text{for all} \quad \begin{array}{c} x \in \{0,1\}^n, b \in \{0,1\} \\ \text{such that } V_b(x) = 1 \end{array}\right] = 1$$

the reduction breaks either f or $i\mathcal{O}$*, namely, for infinitely many* $n \in \mathbb{N}$ *either*

$$\Pr_{\substack{x \leftarrow \{0,1\}^n \\ f,i\mathcal{O},\mathcal{A}}}\left[\mathcal{R}^{\mathcal{A},f,i\mathcal{O}}(f(x)) = x\right] \geq \varepsilon_{\mathcal{R}}(n),$$

or

$$\left|\Pr\left[\mathsf{Exp}^{\mathsf{iO}}_{(f,i\mathcal{O}),i\mathcal{O},\mathcal{C},\mathcal{R}^{\mathcal{A}}}(n) = 1\right] - \frac{1}{2}\right| \geq \varepsilon_{\mathcal{R}}(n),$$

where in both $\mathcal{R}$ *makes at most* $q_{\mathcal{R}}(n)$ *queries to any of its oracles* $(\mathcal{A}, f, i\mathcal{O})$*, and for any query* x *made to* $\mathcal{A}$*, the non-deterministic verifiers* $V_0^{f,i\mathcal{O}}(x), V_1^{f,i\mathcal{O}}(x)$ *make at most* $q_{\mathcal{R}}(n)$ *queries to their oracles (for any non-deterministic choice of a witness* w*). The random variable* $\mathsf{Exp}^{\mathsf{iO}}_{(f,i\mathcal{O}),i\mathcal{O},\mathcal{C},\mathcal{R}^{\mathcal{A}}}(n)$ *represents the reductions winning probability in the IO security game relative to* $(f, i\mathcal{O})$*.*

Remark about Correct Structure. We note that here we explicitly do put a *correctness* requirement, which we refer to as *structure*; namely, that the construction yields a language in $\mathsf{NP} \cap \mathsf{coNP}$ for any implementation of OWPs and IO. This is different from the setting from Definition 2.2 where we considered *promise problems* and allowed the construction not to satisfy the promise occasionally.

Concretely, we require that V_0, V_1 give a language in $\mathsf{NP} \cap \mathsf{coNP}$ for *every* oracle implementing IOWFs and IO. This follows the modeling of [BI87],[11] and

[11] Rudich [Rud88] also considered a slight relaxation of constructions that are correct for an overwhelming fraction of oracles rather than all.

aligns with how we usually think about *correctness* of black-box constructions of cryptographic primitives. For instance, the construction of public-key encryption from trapdoor permutations is promised to be correct, for all oracles implementing the trapdoor permutation. Similarly, the construction of hard $\mathsf{NP} \cap \mathsf{coNP}$ languages from one-way permutations, give an $\mathsf{NP} \cap \mathsf{coNP}$ language for any oracle implementing a permutation.

We also note that as in Definition 2.2, our definition addresses *worst-case hardness*, which makes our impossibility result stronger. See further discussion after Definition 2.2.

Ruling out Fully Black-Box Constructions: A Road Map. Our main result in this section is that fully black-box constructions of a hard $\mathsf{NP} \cap \mathsf{coNP}$ problem from IO and IOWFs do not exist. Furthermore, this holds even if the latter primitives are exponentially secure.

Theorem 3.3. *Any fully black-box construction of an* $\mathsf{NP} \cap \mathsf{coNP}$ *problem* L *from IOWFs and IO for circuits with IOWF gates has an exponential security loss:*

$$\max(q_{\mathcal{R}}(n), \varepsilon_{\mathcal{R}}^{-1}(n)) \geq \Omega(2^{n/6})$$

The proof of the theorem follows a similar methodology to the proof of Theorem 2.3. We exhibit two (distributions on) oracles $(\Psi, \mathsf{Decide}^{\Psi})$, where Ψ realizes IOWFs and IO for circuits with IOWF gates, and Decide^{Ψ} that decides $L^{\Psi} \in \mathsf{NP}^{\Psi} \cap \mathsf{coNP}^{\Psi}$ in the worst case. We then show that the primitives realized by Ψ are (exponentially) secure even in the presence of Decide^{Ψ}. Then viewing Decide as a worst-case decider $\mathcal{A}$ (as per Definition 3.2) directly implies Theorem 3.3, ruling out fully black-box constructions with a subexponential security loss.

We defer the formal treatment to the full version.

4 Collision-Resistance from IO and SZK-Hardness

Asharov and Segev [AS15] showed that collision-resistant hashing cannot be constructed from (even subexponentially hard) indistinguishability obfuscation (IO) and one-way permutations (OWPs) relying on common IO techniques. Slightly more accurately, they rule out fully black-box constructions where (as in previous sections) IO is defined with respect to circuits with OWP oracle gates. In this section, we show that, assuming IO and a strong form of SZK-hardness, there is indeed a construction of collision-resistant hashing (CRH).

The High-Level Idea Behind the Construction. The starting point for our construction is the work of Ishai et al. [IKO05] that shows how to construct collision-resistant hash functions from commitments that are additively homomorphic (for simplicity, say over $\mathbb{F}_2$). The idea is simple: we can hash ℓ bits to m bits, where m is the size of a single bit commitment and ℓ can be arbitrarily longer, as follows. The hash key is a commitment $\gamma := (\mathsf{com}(\beta_1), \ldots, \mathsf{com}(\beta_\ell))$ to a random

vector $\beta \in \mathbb{F}_2^\ell$, and hashing $x \in \mathbb{F}_2^\ell$, is done by homomorphically computing a commitment to the inner product $\mathsf{CRH}_\gamma(x) = \mathsf{com}(\langle \beta, x \rangle)$.

This idea can, in fact, be abstracted to work with any commitment scheme wherein given a commitment $\mathsf{com}(\beta)$ for a random key for a 2-universal hash allows to homomorphically compute a commitment $\mathsf{com}(2\mathsf{UH}_\beta(x))$ to the hash at any point x, so that the resulting commitment is compact in the sense that it depends only on the size of $2\mathsf{UH}_\beta(x)$ and not on the size of x. Intuitively, the reason this works is that any collision in CRH_γ implies a collision in the underlying 2-universal hash $2\mathsf{UH}_\beta$, which leaks information about the hash key β (concretely, any fixed x, x' form a collision in a random hash function with small probability) thereby violating the hiding of the commitment.

At a high-level, we aim to mimic the above construction based on obfuscation. As a key for the collision-resistant hash we can obfuscate a program Π_β associated with a secret hash key β that given x outputs a commitment $\mathsf{com}(2\mathsf{UH}_\beta(x))$, where the commitment is derandomized using a PRF. The obfuscation $i\mathcal{O}(\Pi_\beta)$ can be thought of as the commitment to β, and evaluating this program at x, corresponds to homomorphic evaluation. Despite the clear intuition behind this construction, it is not clear how to prove its security based on IO. In fact, by [AS15], it cannot be proven based on a black-box reduction as long as plain statistically-binding commitments are used, as these can be constructed from OWPs in a fully black-box manner.

We show, however, that relying on a relaxed notion of perfectly-hiding commitments, as well as subexponential hardness of IO and puncturable PRFs, the construction can be proven secure. The perfect hiding of the commitment is leveraged in a probabilistic IO argument [CLTV15] that involves a number of hybrids larger than the overall number of commitments. We then observe that these relaxed commitments follow from appropriate average-case hardness of SZK.[12]

Acknowledgements. We thank Gil Segev, Iftach Haitner and Mohammad Mahmoody for elaborately answering our questions regarding existing separation results in cryptography. We also thank the anonymous reviewers for their valuable comments.

References

[ABW10] Applebaum, B., Barak, B., Wigderson, A.: Public-key cryptography from different assumptions. In: Proceedings of 42nd ACM Symposium on Theory of Computing, STOC 2010, USA, 5–8 June 2010, Cambridge, Massachusetts, pp. 171–180 (2010)

[AGGM06] Akavia, A., Goldreich, O., Goldwasser, S., Moshkovitz, D.: On basing one-way functions on NP-hardness. In: Kleinberg [Kle06], pp. 701–710 (2006)

[12] Similar SZK-hardness is known to imply statistically-hiding commitments against malicious receivers, but with a larger (constant) number of rounds [OV08].

[AH91] Aiello, W., Hastad, J.: Statistical zero-knowledge languages can be recognized in two rounds. J. Comput. Syst. Sci. **42**(3), 327–345 (1991)

[Ale03] Alekhnovich, M., More on average case vs approximation complexity. In: 44th Symposium on Foundations of Computer Science (FOCS 2003), 11–14 October 2003, Cambridge, MA, USA, Proceedings [DBL03], pp. 298–307 (2003)

[AR04] Aharonov, D., Regev, O.: Lattice problems in NP cap coNP. In: 45th Symposium on Foundations of Computer Science (FOCS 2004), 17–19 October 2004, Rome, Italy, Proceedings, pp. 362–371. IEEE Computer Society (2004)

[AR16] Applebaum, B., Raykov, P.: From private simultaneous messages to zero-information arthur-merlin protocols and back. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9563, pp. 65–82. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49099-0_3

[AS15] Asharov, G., Segev, G.: Limits on the power of indistinguishability obfuscation and functional encryption. In: Symposium on the Foundations of Computer Science (2015)

[AS16] Asharov, G., Segev, G.: On constructing one-way permutations from indistinguishability obfuscation. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9563, pp. 512–541. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49099-0_19

[Bar13] Barak, B.: Structure vs. combinatorics in computational complexity (2013). http://windowsontheory.org/2013/10/07/structure-vs-combinatorics-in-computational-complexity/

[BB15] Bogdanov, A., Brzuska, C.: On basing size-verifiable one-way functions on NP-hardness. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9014, pp. 1–6. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46494-6_1

[BBF13] Baecher, P., Brzuska, C., Fischlin, M.: Notions of black-box reductions, revisited. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 296–315. Springer, Heidelberg (2013). doi:10.1007/978-3-642-42033-7_16

[BGI+01] Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S., Yang, K.: On the (im)possibility of obfuscating programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 1–18. Springer, Heidelberg (2001). doi:10.1007/3-540-44647-8_1

[BGL+15] Bitansky, N., Garg, S., Lin, H., Pass, R., Telang, S.: Succinct randomized encodings and their applications. In: Symposium on Theory of Computing, STOC 2015 (2015)

[BHZ87] Boppana, R.B., Hastad, J., Zachos, S.: Does co-NP have short interactive proofs? Inf. Process. Lett. **25**(2), 127–132 (1987)

[BI87] Blum, M., Impagliazzo, R.: Generic oracles and oracle classes. In: Proceedings of 28th Annual Symposium on Foundations of Computer Science, SFCS 1987, pp. 118–126. IEEE Computer Society, Washington (1987)

[BKSY11] Brakerski, Z., Katz, J., Segev, G., Yerukhimovich, A.: Limits on the power of zero-knowledge proofs in cryptographic constructions. In: Ishai [Ish11], pp. 559–578 (2011)

[BL13] Bogdanov, A., Lee, C.H.: Limits of provable security for homomorphic encryption. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 111–128. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40041-4_7

[BM09] Barak, B., Mahmoody-Ghidary, M.: Merkle puzzles are optimal—an $O(n^2)$-query attack on any key exchange from a random oracle. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 374–390. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_22

[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). doi:10.1007/978-3-662-46497-7_16

[BPR15] NBitansky, ., Paneth, O., Rosen, A.: On the cryptographic hardness of finding a nash equilibrium. In: Guruswami, V. (ed.) IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, 17–20 October 2015, Berkeley, CA, USA, pp. 1480–1498. IEEE Computer Society (2015)

[BPW16] Bitansky, N., Paneth, O., Wichs, D.: Perfect structure on the edge of chaos. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 474–502. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49096-9_20

[Bra79] Brassard, G.: Relativized cryptography. In: 20th Annual Symposium on Foundations of Computer Science, 29–31 October 1979, San Juan, Puerto Rico, pp. 383–391. IEEE Computer Society (1979)

[BT03] Bogdanov, A., Trevisan, L.: On worst-case to average-case reductions for NP problems. In: 44th Symposium on Foundations of Computer Science (FOCS 2003), 11–14 October 2003, Cambridge, MA, USA, Proceedings [DBL03], pp. 308–317 (2003)

[BV11] Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Ostrovsky, R. (ed.) FOCS, pp. 97–106. IEEE (2011). (Invited to SIAM Journal on Computing)

[CDT09] Chen, X., Deng, X., Teng, S.-H.: Settling the complexity of computing two-player nash equilibria. J. ACM **56**(3), 14 (2009)

[CHJV15] Canetti, R., Holmgren, J., Jain, A., Vaikuntanathan, V.: Succinct garbling and indistinguishability obfuscation for RAM programs. In: Proceedings of 47th Annual ACM on Symposium on Theory of Computing, STOC 2015, 14–17 June 2015, Portland, OR, USA, pp. 429–437 (2015)

[CLTV15] Canetti, R., Lin, H., Tessaro, S., Vaikuntanathan, V.: Obfuscation of probabilistic circuits and applications. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9015, pp. 468–497. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46497-7_19

[Cra12] Cramer, R. (ed.): Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, 19–21 March 2012, Taormina, Sicily, Italy, Proceedings. LNCS vol. 7194. Springer, Heidelberg (2012)

[DBL00] Prceedings of 41st Annual Symposium on Foundations of Computer Science, FOCS 2000: 12–14 November 2000. IEEE Computer Society, Redondo Beach (2000)

[DBL03] Prceedings of 44th Symposium on Foundations of Computer Science (FOCS 2003: 11–14 October 2003. IEEE Computer Society, Cambridge (2003)

[DGP06] Daskalakis, C., Goldberg, P.W., Papadimitriou, C.H.: The complexity of computing a nash equilibrium. In: Kleinberg [Kle06], pp. 71–78 (2006)

[DH76] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)

[DHT12] Dodis, Y., Haitner, I., Tentes, A.: On the instantiability of hash-and-sign RSA signatures. In: Cramer [Cra12], pp. 112–132 (2012)

[DLMM11] Dachman-Soled, D., Lindell, Y., Mahmoody, M., Malkin, T.: On the black-box complexity of optimally-fair coin tossing. In: Ishai [Ish11], pp. 450–467 (2011)

[ESY84] Even, S., Selman, A.L., Yacobi, Y.: The complexity of promise problems with applications to public-key cryptography. Inf. Control **61**(2), 159–173 (1984)

[Fis12] Fischlin, M.: Black-box reductions and separations in cryptography. In: Mitrokotsa, A., Vaudenay, S. (eds.) AFRICACRYPT 2012. LNCS, vol. 7374, pp. 413–422. Springer, Heidelberg (2012). doi:10.1007/978-3-642-31410-0_26

[For89] Fortnow, L.J.: Complexity-theoretic aspects of interactive proof systems. Ph.D. thesis, Massachusetts Institute of Technology (1989)

[Gen09] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: STOC, pp. 169–178 (2009)

[GG98] Goldreich, O., Goldwasser, S.: On the possibility of basing cryptography on the assumption that $p \neq NP$. IACR Cryptology ePrint Archive, 1998:5 (1998)

[GGH+13a] Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: 54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26–29 October 2013, Berkeley, CA, USA, pp. 40–49. IEEE Computer Society (2013)

[GGH+13b] Garg, S., Gentry, C., Halevi, S., Sahai, A., Raikova, M., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: FOCS (2013)

[GGKT05] Gennaro, R., Gertner, Y., Katz, J., Trevisan, L.: Bounds on the efficiency of generic cryptographic constructions. SIAM J. Comput. **35**(1), 217–246 (2005)

[GK93] Goldreich, O., Kushilevitz, E.: A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm. J. Cryptol. **6**(2), 97–116 (1993)

[GKLM12] Goyal, V., Kumar, V., Lokam, S.V., Mahmoody, M.: On black-box reductions between predicate encryption schemes. In: Cramer [Cra12], pp. 440–457 (2012)

[GKM+00] Gertner, Y., Kannan, S., Malkin, T., Reingold, O., Viswanathan, M.: The relationship between public key encryption and oblivious transfer. In: 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12–14 November 2000, Redondo Beach, California, USA [DBL00], pp. 325–335 (2000)

[GM82] Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information. In: Lewis, H.R., Simons, B.B., Burkhard, W.A., Landweber, L.H. (eds.) Proceedings of 14th Annual ACM Symposium on Theory of Computing, 5–7 May 1982, San Francisco, California, USA, pp. 365–377. ACM (1982)

[GMM07] Gertner, Y., Malkin, T., Myers, S.: Towards a separation of semantic and CCA security for public key encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 434–455. Springer, Heidelberg (2007). doi:10.1007/978-3-540-70936-7_24

[GMR85] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems (extended abstract). In: Sedgewick, R. (ed.) Proceedings of 17th Annual ACM Symposium on Theory of Computing, 6–8 May 1985, Providence, Rhode Island, USA, pp. 291–304. ACM (1985)

[GMR01] Gertner, Y., Malkin, T., Reingold, O.: On the impossibility of basing trapdoor functions on trapdoor predicates. In: 42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14–17 October 2001, Las Vegas, Nevada, USA, pp. 126–135. IEEE Computer Society (2001)

[GMW91] Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. J. ACM **38**(3), 691–729 (1991)

[Gol06] Goldreich, O.: On promise problems: a survey. In: Goldreich, O., Rosenberg, A.L., Selman, A.L. (eds.) Theoretical Computer Science. LNCS, vol. 3895, pp. 254–290. Springer, Heidelberg (2006). doi:10.1007/11685654_12

[GT00] Gennaro, R., Trevisan, L.: Lower bounds on the efficiency of generic cryptographic constructions. In: 41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12–14 November 2000, Redondo Beach, California, USA [DBL00], pp. 305–313 (2000)

[GV99] Goldreich, O., Vadhan, S.P.: Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In: Proceedings of 14th Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, USA, 4–6 May 1999, p. 54 (1999)

[Has88] Hastad, J.: Dual vectors and lower bounds for the nearest lattice point problem. Combinatorica **8**(1), 75–81 (1988)

[HH09] Haitner, I., Holenstein, T.: On the (im)possibility of key dependent encryption. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 202–219. Springer, Heidelberg (2009). doi:10.1007/978-3-642-00457-5_13

[HHRS15] Haitner, I., Hoch, J.J., Reingold, O., Segev, G.: Finding collisions in interactive protocols—tight lower bounds on the round and communication complexities of statistically hiding commitments. SIAM J. Comput. **44**(1), 193–242 (2015)

[HMX10] Haitner, I., Mahmoody, M., Xiao, D.: A new sampling protocol and applications to basing cryptographic primitives on the hardness of NP. In: 2010 IEEE 25th Annual Conference on Computational Complexity (CCC), pp. 76–87. IEEE (2010)

[HR04] Hsiao, C.-Y., Reyzin, L.: Finding collisions on a public road, or do secure hash functions need secret coins? In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 92–105. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_6

[IKO05] Ishai, Y., Kushilevitz, E., Ostrovsky, R.: Sufficient conditions for collision-resistant hashing. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 445–456. Springer, Heidelberg (2005). doi:10.1007/978-3-540-30576-7_24

[IR89] Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Proceedings of 21st Annual ACM Symposium on Theory of Computing, pp. 44–61. ACM (1989)

[Ish11] Ishai, Y. (ed.): Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA. LNCS, 28–30 March 2011. Proceedings, vol. 6597. Springer, Heidelberg (2011)

[Kle06] Kleinberg, J.M. (ed.): Proceedings of 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, 21–23 May 2006. ACM (2006)

[KLW15] Koppula, V., Lewko, A.B., Waters, B.: Indistinguishability obfuscation for turing machines with unbounded memory. In: Proceedings of 47th Annual ACM on Symposium on Theory of Computing, STOC 2015, 14–17 June 2015, Portland, OR, USA, pp. 419–428 (2015)

[KMN+14] Komargodski, I., Moran, T., Naor, M., Pass, R., Rosen, A., Yogev, E.: One-way functions and (im)perfect obfuscation. In: 55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, 18–21 October 2014, Philadelphia, PA, USA, pp. 374–383. IEEE Computer Society (2014)

[KSS11] Kahn, J., Saks, M.E., Smyth, C.D.: The dual BKR inequality and rudich's conjecture. Comb. Probab. Comput. **20**(2), 257–266 (2011)

[KST99] Kim, J.H., Simon, D.R., Tetali, P.: Limits on the efficiency of one-way permutation-based hash functions. In: 40th Annual Symposium on Foundations of Computer Science, FOCS 1999, 17–18 October 1999, New York, NY, USA, pp. 535–542. IEEE Computer Society (1999)

[LLJS90] Lagarias, J.C., Lenstra Jr., H.W., Schnorr, C.-P.: Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica **10**(4), 333–348 (1990)

[LV16] Liu, T., Vaikuntanathan, V.: On basing private information retrieval on NP-hardness. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 372–386. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49096-9_16

[MM11] Matsuda, T., Matsuura, K.: On black-box separations among injective one-way functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 597–614. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19571-6_36

[MP91] Megiddo, N., Papadimitriou, C.H.: On total functions, existence theorems and computational complexity. Theor. Comput. Sci. **81**(2), 317–324 (1991)

[MV03] Micciancio, D., Vadhan, S.P.: Statistical zero-knowledge proofs with efficient provers: lattice problems and more. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 282–298. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45146-4_17

[MX10] Mahmoody, M., Xiao, D.: On the power of randomized reductions and the checkability of sat. In: 2010 IEEE 25th Annual Conference on Computational Complexity (CCC), pp. 64–75. IEEE (2010)

[Ost91] Ostrovsky, R.: One-way functions, hard on average problems, and statistical zero-knowledge proofs. In: Proceedings of 6th Annual Structure in Complexity Theory Conference, pp. 133–138. IEEE (1991)

[OV08] Ong, S.J., Vadhan, S.: An equivalence between zero knowledge and commitments. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 482–500. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78524-8_27

[Pap94] Papadimitriou, C.H.: On the complexity of the parity argument and other inefficient proofs of existence. J. Comput. Syst. Sci. **48**(3), 498–532 (1994)

[Pas06] Pass, R.: Parallel repetition of zero-knowledge proofs and the possibility of basing cryptography on NP-hardness. In: 21st Annual IEEE Conference on Computational Complexity (CCC 2006), 16–20 July 2006, Prague, Czech Republic, pp. 96–110. IEEE Computer Society (2006)

[Pas13] Pass, R.: Unprovable security of perfect NIZK and non-interactive non-malleable commitments. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 334–354. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36594-2_19

[RAD78] Rivest, R., Adleman, L., Dertouzos, M.: On data banks and privacy homomorphisms. In: Foundations of Secure Computation, pp. 169–177. Academic Press (1978)

[RSA78] Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)

[RSS16] Rosen, A., Segev, G., Shahaf, I.: Can PPAD hardness be based on standard cryptographic assumptions? In: Electronic Colloquium on Computational Complexity (ECCC), vol. 23, p. 59 (2016)

[RTV04] Reingold, O., Trevisan, L., Vadhan, S.: Notions of reducibility between cryptographic primitives. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 1–20. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24638-1_1

[Rud88] Rudich, S.: Limits on the provable consequences of one-way functions. Ph.D. thesis, University of California, Berkeley (1988)

[Rud91] Rudich, S.: The use of interaction in public cryptosystems. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 242–251. Springer, Heidelberg (1992). doi:10.1007/3-540-46766-1_19

[Sim98] Simon, D.R.: Finding collisions on a one-way street: can secure hash functions be based on general assumptions? In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 334–345. Springer, Heidelberg (1998). doi:10.1007/BFb0054137

[SV03] Sahai, A., Vadhan, S.: A complete problem for statistical zero knowledge. J. ACM (JACM) **50**(2), 196–249 (2003)

[SW14] Sahai, A., Waters, B.: How to use indistinguishability obfuscation: deniable encryption, and more. In: Shmoys, D.B. (ed.) Symposium on Theory of Computing, STOC 2014, New York, NY, USA, 31 May–03 June 2014, pp. 475–484. ACM (2014)

[Vad99] Vadhan, S.P.: A study of statistical zero-knowledge proofs. Ph.D. thesis, Massachusetts Institute of Technology (1999)

[Wat15] Waters, B.: A punctured programming approach to adaptively secure functional encryption. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 678–697. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48000-7_33