Batch Proofs are Statistically Hiding

Nir Bitansky[1], Chethan Kamath[2], Omer Paneth[1], Ron D. Rothblum[3], and Prashant Nalini Vasudevan[4]

[1]Tel Aviv University, nirbitan@tau.ac.il,omerpa@tauex.tau.ac.il
[2]IIT Bombay, ckamath@protonmail.com
[3]Technion, rothblum@cs.technion.ac.il
[4]National University of Singapore, prashant@comp.nus.edu.sg

December 4, 2023

Abstract

Batch proofs are proof systems that convince a verifier that $x_1, \dots, x_t \in \mathcal{L}$, for some NP language $\mathcal{L}$, with communication that is much shorter than sending the t witnesses. In the case of *statistical soundness* (where the cheating prover is unbounded but the honest prover is efficient given the witnesses), interactive batch proofs are known for UP, the class of *unique-witness* NP languages. In the case of computational soundness (where both honest and dishonest provers are efficient), *non-interactive* solutions are now known for all of NP, assuming standard lattice or group assumptions.

We exhibit the first negative results regarding the existence of batch proofs and arguments:

- Statistically sound batch proofs for $\mathcal{L}$ imply that $\mathcal{L}$ has a statistically witness indistinguishable (SWI) proof, with inverse polynomial SWI error, and a non-uniform honest prover. The implication is unconditional for obtaining honest-verifier SWI or for obtaining full-fledged SWI from public-coin protocols, whereas for private-coin protocols full-fledged SWI is obtained assuming one-way functions.

  This poses a barrier for achieving batch proofs beyond UP (where witness indistinguishability is trivial). In particular, assuming that NP does not have SWI proofs, batch proofs for all of NP do not exist.

- Computationally sound batch proofs (a.k.a batch arguments or BARGs) for NP, together with one-way functions, imply statistical zero-knowledge (SZK) arguments for NP with roughly the same number of rounds, an inverse polynomial zero-knowledge error, and non-uniform honest prover.

  Thus, constant-round interactive BARGs from one-way functions would yield constant-round SZK arguments from one-way functions. This would be surprising as SZK arguments are currently only known assuming constant-round statistically-hiding commitments.

We further prove new positive implications of non-interactive batch arguments to non-interactive zero knowledge arguments (with explicit uniform prover and verifier):

- Non-interactive BARGs for NP, together with one-way functions, imply non-interactive computational zero-knowledge arguments for NP. Assuming also dual-mode commitments, the zero knowledge can be made statistical.

Both our negative and positive results stem from a new framework showing how to transform a batch protocol for a language $\mathcal{L}$ into an SWI protocol for $\mathcal{L}$.

Contents

1 Introduction **3**
- 1.1 Our Results . . . 4
- 1.2 Additional Related Works . . . 6
- 1.3 Technical Overview . . . 7

2 Definitions **12**
- 2.1 Interactive Protocols: Soundness, Privacy and Batching . . . 13
- 2.2 Non-Interactive Protocols: Soundness, Privacy and Batching . . . 14
- 2.3 List of Proof Systems . . . 17

3 Statistical Witness Indistinguishability from Batching **18**
- 3.1 Witness Indistinguishability . . . 20
- 3.2 Non-Interactive Protocols . . . 24
- 3.3 Corollaries . . . 28

4 NISZKA from NIBARG and Dual-Mode Commitments **34**
- 4.1 Dual-Mode Commitments . . . 34
- 4.2 Dual-Mode NISZKA from Dual-Mode NIDSZKA and DMC . . . 35
- 4.3 Privacy Amplification Using DMC and MPC . . . 40

5 NICWIA from NIBARG and OWF **48**
- 5.1 Instance-Dependent Primitives . . . 48
- 5.2 ID-NISZKA from Dual-Mode NIDSZKA and CIDC . . . 51
- 5.3 Privacy Amplification using CIDC and MPC . . . 54
- 5.4 Corollaries . . . 56

Acknowledgements **57**

References **57**

A Proof of Lemma 4.19 **63**
- A.1 Good Distributions . . . 66

B LPKE via Somewhere Extractable NIBARGs **66**
- B.1 PIR from Somewhere Extractability . . . 67
- B.2 Honest Somewhere Extractability . . . 70

1 Introduction

Batch proofs are interactive proof-systems that enable a prover to convince a verifier that input statements $x_1, \dots, x_t$ all belong to a language $\mathcal{L} \in \mathsf{NP}$, with communication that is much shorter than sending the t witnesses. Batch proofs have been studied recently in two main threads: depending on whether the soundness property is required to hold against arbitrary cheating prover strategies, or only against computationally bounded ones.

The Statistical Setting. In the *statistical setting*, we require that even a computationally unbounded prover cannot convince the verifier to accept a false statement (other than with some bounded probability). On the other hand, we require that there is an *efficient honest prover* strategy (given the witnesses as an auxiliary input) for convincing the verifier of true statements. Such batch proofs systems are known as *doubly efficient* (see [Gol18] for a recent survey on doubly efficient interactive proofs).

A recent sequence of works by Reingold *et al.* [RRR21, RRR18, RR20] construct doubly-efficient batch proofs for any language in the class UP (consisting of NP languages in which YES instances have a *unique* accepting witness). In particular, Rothblum and Rothblum [RR20] give such a protocol with communication $\mathsf{poly}(m, \log(t))$, where m is the length of a single witness and poly is a polynomial that depends only on the UP language. Doubly-efficient batch proofs beyond UP remain unknown, leading to a natural question [RRR21]:

Does every language $\mathcal{L} \in \mathsf{NP}$ have a statistically sound doubly-efficient batch proof? Do there exist other subclasses of NP (beyond UP) that have such proofs?

If we waive the restriction that the honest prover is efficient, there is a simple answer to this question. Specifically, there is a space $\mathsf{poly}(n, m) + \log(t)$ algorithm for deciding whether $x_1, \dots, x_t \in \mathcal{L}$, where n is the instance length and m is the witness length. Thus, via the $\mathsf{IP} = \mathsf{PSPACE}$ theorem [LFKN92, Sha92], there is an interactive proof for this problem with communication $\mathsf{poly}(n, m, \log(t))$. However, this protocol is entirely impractical as the honest prover runs in time $2^{\Omega(n)}$.

The Computational Setting. A natural relaxation of the statistical soundness condition is to only require *computational soundness*, which means that soundness is guaranteed only against *efficient* cheating provers. Such proof systems are commonly called *argument systems*. The seminal work of Kilian [Kil92] gives general-purpose succinct arguments for all of NP, assuming the existence of collision-resistant hash functions (CRH). In more detail, Kilian's protocol is a four-message argument-system with communication $\mathsf{poly}(\lambda, \log(n))$, where λ is the security parameter, for any language $\mathcal{L} \in \mathsf{NP}$. In particular, for any $\mathcal{L} \in \mathsf{NP}$, we can apply Killian's result to the related NP language

$$\mathcal{L}^{\otimes t} = \left\{ (x_1, \dots, x_t) \in (\{0,1\}^n)^t : x_1, \dots, x_t \in \mathcal{L} \right\}$$

and obtain a *batch argument* (BARG) for $\mathcal{L}$ with communication $\mathsf{poly}(\lambda, \log(n), \log(t))$.

Kilian's protocol relies on collision-resistant hash functions (or certain relaxations thereof [BKP18, KNY18a]). However, it is unclear whether such hash functions are also necessary. This gives rise to the following question:

What are the minimal assumptions needed for succinct arguments for NP? Can BARGs be constructed based solely on the existence of one-way functions?

We remark that it is not clear that the existence of one-way functions is even *necessary* for general purpose succinct arguments for NP. The only result that we are aware of is by Wee [Wee05], who showed that 2-message succinct arguments imply the existence of a hard-on-average search problem in NP.

The Non-Interactive (Computational) Setting. As noted above, Kilian's protocol requires four messages. Reducing the number of messages in succinct arguments is a major open question in the field.[1] Restricting to the case of BARGs though, we have a much better understanding due to recent breakthrough works. In particular, a sequence of works [BHK17, CJJ21, CJJ22, WW22, HJKS22, PP22, KLVW22] construct BARGs consisting of a single message, given a common reference string (equivalently, 2-message publicly verifiable arguments in the plain model), assuming specific cryptographic assumptions such as LWE or assumptions related to discrete log.

This raises the question of whether one can make do with a general assumption as in Kilian's protocol. In particular:

Can non-interactive BARG*s be constructed from collision-resistant hash functions?*

1.1 Our Results

In this work, with the above questions in mind, we exhibit the first barriers for the existence of batch proofs and arguments. In the non-interactive setting, our results also have positive applications, giving rise to new non-interactive zero knowledge protocols.

Our main contribution is a new transformation that compiles a batch protocol (proof or argument) Π, for verifying that $x_1, \ldots, x_t \in \mathcal{L}$, into a protocol Π', for a single instance, which has a secrecy property. Specifically, we consider batch protocols Π where the communication for proving that $x_1, \ldots, x_t \in \mathcal{L}$ is $t^{1-\epsilon} \cdot \mathsf{poly}(m)$, for some $\epsilon > 0$, witness length m, and a polynomial poly that does not depend on t. We show that any such Π can be transformed into a protocol Π' for a single instance satisfying *statistical witness indistinguishability* (SWI) against an honest verifier. Recall that a protocol for an NP relation $\mathcal{R}$ is SWI, if for every input x and witnesses $w_0, w_1 \in \{w : \mathcal{R}(x, w) = 1\}$, the view of the verifier when the prover uses w_0 and when the prover uses w_1 are statistically close. We say that the protocol is *honest-verifier* SWI if the SWI property only holds in an honest execution of the protocol. The transformation preserves the soundness of the original protocol; namely, if Π is computationally (resp., statistically) sound then the resulting protocol Π' is computationally (resp., statistically) sound. If Π has r-rounds then Π' has $r + 1$ rounds.

The transformation does have two caveats: First, the statistical WI error ε is inverse polynomial and not negligible. Specifically, the statistical distance between the view of the verifier when the prover uses w_0 and when the prover uses w_1 can be set to any ε, at the cost of increasing the communication complexity polynomially in $1/\varepsilon$. The second caveat is that the efficient honest prover strategy of Π' is non-uniform, where the non-uniform advice depends on the specification of the protocol Π. Even given these two caveats, the transformation is a meaningful tool for deriving barriers (in terms of complexity or cryptographic assumptions) on the existence of batch proofs. On the positive side, in the setting of *non-interactive* protocols, we show an improved transformation that overcomes both caveats, thereby giving rise to new explicit protocols.

We next elaborate on our results in each of the settings discussed above. See Figure 1.1 for a summary of the different implications we prove.

A Barrier for Statistically Sound Batch Proofs. Our first application of the above transformation is in the statistical setting. Given a statistically sound batch proof, we obtain SWI against malicious verifiers, in which the SWI error is inverse polynomial. In case we start from a public-coin batch proof the result is unconditional. Otherwise, we need to assume one-way functions (or settle for honest-verifier SWI).[2]

Theorem 1 (Informally Stated, see Theorem 3.1 and Corollaries 3.18 and 3.19)**.** *Suppose that $\mathcal{L} \in$ NP has a statistically sound r-round public-coin batch proof. Then, for any polynomial p, the language $\mathcal{L}$ has an $O(r)$-round* SWI *proof with* SWI *error $\frac{1}{p}$ and a non-uniform honest prover.*

[1]We note that in the *random oracle model* succinct non-interactive arguments for NP (and in particular BARGs) exist unconditionally [Mic94]. We focus on the plain model, where given a common reference string (CRS) proofs can be generated and verified non-interactively.

[2]Note that the Goldwasser and Sipser [GS89] transformation from private-coin to public-coin protocols is inapplicable, since it results in an inefficient honest prover (see also [AR21]).

Furthermore, for general (i.e., private-coin) statistically sound batch proofs we achieve the weaker conclusion of honest-verifier SWI*, or, assuming the existence of a one-way function, malicious verifier* SWI*.*

It is worth pointing out that Theorem 1 is also applicable to languages in UP (for which batch proofs are known), but there the conclusion is meaningless since UP has a trivial SWI proof - just send the witness! In contrast, the existence of SWI proofs for all of NP would be surprising. In particular, there are no known languages with SWI proofs beyond $\mathsf{UP} \cup \mathsf{SZK}$. Here SZK is the class of languages with *statistical zero-knowledge* proofs, and it is known not to contain NP (assuming the polynomial hierarchy does not collapse [For89, AH91]).[3]

Corollary 2 (Informally Stated)**.** *Assume that the class of languages with an* SWI *proof (as in Theorem 1) does not contain* NP*. Then* NP *does not have statistically-sound batch proofs.*

We do not take for granted the fact that NP does not have SWI proofs, and we find this to be an intriguing open question. Indeed, while we have a very deep understanding of the structure of SZK (see [Vad99]), to the best of our knowledge, the structure of the class of languages having SWI proofs has not been explored. Theorem 1 provides concrete motivation for a similar study of the class SWI, which we leave to future work.

A Barrier for Computationally Sound Batch Proofs. Applying our framework in the computational setting, and assuming one-way functions, we are able to derive the stronger hiding property of *statistical zero-knowledge*.

Theorem 3 (Informally Stated, See Theorem 3.1 and Corollary 3.19)**.** *Assume the existence of one-way functions. Suppose that every $\mathcal{L} \in$ NP has an r-round* BARG*. Then, for every polynomial p, every $\mathcal{L} \in$ NP has an $O(r)$-round statistical zero-knowledge argument-system (*SZKA*) with* ZK *error $\frac{1}{p}$ and a non-uniform honest prover.*

Recall that constant-round SZKA for NP are only known to exist assuming constant-round statistically-hiding commitments, which in turn are only known based on primitives that are seemingly stronger than one-way functions, such as collision-resistant hash functions (or variants thereof [BKP18, BDRV18, KNY18b, BHKY19]). In fact, there are known black-box separations between constant-round statistically-hiding commitments and one way functions [HHRS15]. Thus, Theorem 3 can be seen as a barrier toward basing constant-round BARGs for NP on one-way functions.

In this context, a related positive result was obtained recently by Amit and Rothblum [AR23], who constructed constant-round succinct arguments for deterministic languages (specifically for the class NC) from one-way functions. Theorem 3 poses a barrier toward extending their result to BARGs for NP.

Explicit Proof Systems from Non-Interactive BARGs. In the context of *non-interactive* BARG*s* we are able to push the transformation further, constructing explicit (uniform) protocols with a negligible WI error. In particular, while one may still take a negative perspective and view these results as barriers on non-interactive BARGs, they can also be viewed positively, as a new route to constructing non-interactive WI (and in fact ZK) protocols.

One subtlety in applying our transformation in the non-interactive setting concerns adaptive soundness (in the interactive setting we do away with this concern by adding a round of interaction). Here we assume that the BARGs we start from satisfy a weak form of adaptive soundness called *somewhere soundness*, which is a relaxation of *somewhere extractability* [CJJ22], achieved by recent BARG constructions.

We obtain the following result:

Theorem 4 (Informally Stated, See Corollaries 4.11 and 5.10)**.** *Assume that* NP *has somewhere-sound non-interactive* BARG*s. Then, assuming also one-way functions,* NP *has non-interactive computational zero-knowledge arguments (*NICZKA*), with a negligible non-adaptive soundness error, a negligible zero-knowledge*

[3] Recall that *statistical zero-knowledge* (SZK) requires that for every efficient verifier strategy there is an efficient simulator that generates a view that is statistically close to that in the actual interaction (for instances in the language). SWI can be thought of as a relaxation of SZK in which the simulator can be unbounded.

error, and a uniform honest prover. Assuming also the existence of dual-mode commitments,[4] *the same implications holds for statistical zero knowledge (*NISZKA*).*

Like non-interactive BARGs, non-interactive ZK (computational or statistical) is currently only known to exist based on trapdoor permutations or specific algebraic and number-theoretic assumptions. Accordingly, one (negative) perspective on Theorem 4 is as evidence that constructing non-interactive BARGs from "relatively weak" assumptions, such as one-way functions or collision-resistant hash functions, would be difficult. From a positive perspective, construction of non-interactive BARGs from new assumptions would yield analogous results for NICZKA.

Toward proving Theorem 4 we prove two general enhancement theorems for NISZKA that we find valuable on their own. The first is a reduction between average-case and worst-case notions of SZK, and the second is an amplification theorem that reduces SZK error.

Remark 1.1 (Lossy Encryption from BARGs)**.** *We also observe that lossy public-key encryption follows from a variant of somewhere extractable BARGs, which guarantees that it is possible to extract the specific witness that was used in some predefined index in an honest proof. This is in contrast to the standard notion of somewhere extractability guaranteeing that* some *witness can be extracted (even from maliciously generated accepting proofs). Furthermore, we show that the standard notion of somewhere extractable BARGs imply* private information retrieval *and thus also* statistically sender-private oblivious transfer *and lossy public-key encryption. while perfectly-correct lossy public key encryption would imply dual-mode commitments, lossy public-key encryption obtained has (negligible) decryption errors (which is not sufficient for Theorem 4). See further details in Appendix B.*

Remark 1.2 (Hiding for Batch Protocols)**.** *All of the results listed above start with a batch protocol for a language $\mathcal{L}$ and derive a protocol with hiding properties (i.e., either* SWI *or* SZK*) for a single instance of $\mathcal{L}$. We note that all of the results can be used to obtain similar hiding properties also for a* batch *protocol for $\mathcal{L}$ via the following simple transformation: rather than applying the basic result to $\mathcal{L}$, we can apply it to $\mathcal{L}^{\otimes t'}$ for any $t' \ll t$.*

Remark 1.3 (On the Possibility of Weak Batching)**.** *All of our results assume a batch protocol for t instances, with communication $t^{1-\epsilon}$.*[5] *Thus, our results are inapplicable to very weakly compressing batch protocols that have slightly non-trivial communication such as say, $t \cdot \sqrt{m} + \mathsf{poly}(m)$, where m is the witness length. Such weak batch protocols can nevertheless be quite useful (see [RRR21]) and we leave the study of this setting as an interesting open problem.*

1.2 Additional Related Works

The study of the minimal necessary communication in statistically sound interactive proofs, focusing on the prover to verifier communication, was initiated in [GH98, GVW02]. In particular, Goldreich *et al.* [GVW02] transform interactive proofs with a *single bit* of communication to be SZK. We emphasize that the results in [GH98, GVW02] are inapplicable in the setting of batch proofs. For example, the main result in [GH98] says that proofs with short communication can be emulated in time that is exponential in the communication, but this merely indicates that the communication in batch proofs for NP needs to be $\Omega(m + \log t)$, where m is the witness length.

[4]Loosely speaking, dual-mode commitments are commitment schemes defined with respect to a common reference string, which can be generated in one of two modes: (1) *hiding*, in which case the commitment is statistically hiding, or (2) *binding*, in which case it is statistically binding. The two types of CRS's are computationally indistinguishible. We emphasize that we do not require efficient extraction and so such commitments do not necessarily require the existence of public-key encryption. In particular, they can be constructed for instance from a variant of the statistical difference problem in which NO instances are disjoint circuits (see [Vad99])

[5]We remark that Kalai *et al.* [KLVW22] show how to amplify weak non-interactive BARGs into BARGs with very good compression but they assume the existence of rate-1 OT, whereas we are seeking transformations that rely only on the existence of the weak BARG.

Kaslasi *et al.* [KRR+20, KRV21] consider batch verification of protocols that are *a priori* statistical zero-knowledge, while retaining the zero-knowledge property. The constructions of [KRR+20, KRV21] are *not* doubly-efficient and so our results are inapplicable in their context.

Batch verification is also related to the problem of *AND instance compression* [HN10, FS08]. In AND instance compression, the goal is, given formulas $\phi_1, \dots, \phi_k$, to generate in polynomial time a new formula ϕ that is satisfiable if and only if $\phi_1, \dots, \phi_k$ are all satisfiable, and so that the length of ϕ is less than k. Batch verification considers the dual problem of compressing the *witnesses.* We note that strong infeasibility results for AND instance compression were shown by Drucker [Dru15]. Despite the differences, a main technical lemma used by Drucker (and a subsequent simplification by Dell [Del16]) is a key inspiration for our analysis. We note that this lemma has previously been used for identifying sufficient conditions for obtaining cryptographic primitives from average-case hardness [BBD+20]. A closely related lemma was established even earlier in the context of constructing an oblivious transfer protocol from any private information retrieval scheme [DMO00].

The minimax theorem has found several applications in cryptography: see [VZ13] for the references. The work of [CLP15] also establishes (among other results) a result of the form "succinctness implies hiding" using the minimax theorem. To be specific, they showed that for a proof system with a *laconic prover*, i.e, where the communication from the prover is $O(\log(n))$ bits, [GVW02] implies *distributional* computational zero knowledge. It is also worth pointing out that the usage of the minimax theorem there is for a different purpose compared to us: it is used there to switch the order of quantifiers of the simulator and distinguisher to obtain (normal) zero knowledge from weak zero knowledge .

Lastly, we mention a recent result of Kitagawa *et al.* [KMY20], who show how to transform any (adaptively-secure) SNARG (a much stronger notion than non-interactive BARG, and not known based on standard assumptions) into a NICZKA, assuming one-way functions. We show a similar result from a weaker proof system (in particular, one that is known based on various standard assumptions).

Comparison with [CW23]. In a concurrent and independent work, Champion and Wu [CW23] constructed *computational* NIZK arguments assuming non-interactive BARGs, extractable dual-mode commitments (a.k.a lossy encryption) and sub-exponentially-secure *local* pseudorandom generators. Our Theorem 4 is a strict improvement of their result, it achieves the same implication assuming only one-way functions (on top of the BARG), or a stronger implication (*statistical* zero knowledge) assuming (non-extractable) dual-mode commitments. Since [CW23] build on the result of Kitagawa *et al.* [KMY20], their approach is quite different from ours.

In the first posting of our paper, which was concurrent to [CW23] we obtained a weaker NIZK result which was technically incomparable to that [CW23] since our prover was *non-uniform.* Subsequently to the first posting and that of [CW23], we obtained the stronger Theorem 4.

1.3 Technical Overview

Let $\mathcal{R}$ be an NP relation, and let

$$\mathcal{R}^{\otimes t} = \Big\{ \Big((x_1, \dots, x_t), (w_1, \dots, w_t) \Big) : |x_1| = \cdots = |x_t| \text{ and } \forall i \in [t],\ (x_i, w_i) \in \mathcal{R} \Big\}$$

be the corresponding batch relation. We start by assuming a batch protocol for $\mathcal{R}^{\otimes t}$ (without specifying yet whether soundness is statistical or computational). For simplicity, let us assume that $\mathcal{R}^{\otimes t}$ has an entirely non-interactive protocol - that is, a single message sent from the prover to the verifier. We view the prover message in this case as a "compression function" f that takes as input $(x_1, \dots, x_t, w_1, \dots, w_t)$ and outputs a short proof string π that convinces the verifier.

Since f outputs a short string, of length less than t, its output cannot contain all of the witnesses. Thus, intuitively at least, a large portion of the information about the witnesses must be lost. This leads us to the following natural idea for a protocol, for a single instance of $\mathcal{R}$,[6] that has hiding properties.

[6]By this we mean for an instance corresponding to $\mathcal{L}(\mathcal{R})$, the language corresponding to the relation $\mathcal{R}$.

$\underline{\mathsf{P}(x, w):}$ (where x is an input and w is a corresponding witness)

1. Choose a random index $i^* \in [t]$.
2. Select input/witness pairs $(x_i, w_i) \in \mathcal{R}$ for all $i \in [t] \backslash \{i^*\}$, in some yet-to-be-specified way.
3. Generate $\pi = f(x_1, \ldots, x_t, w_1, \ldots, w_t)$, where we fix $x_{i^*} = x$ and $w_{i^*} = w$.
4. Send $(x_1, \ldots, x_t, i^*, \pi)$ to the verifier.

The verifier V accepts if (1) $x_{i^*} = x$ and (2) the batch verifier accepts the input $(x_1, \ldots, x_t)$ with the proof π. Completeness and soundness of this protocol follow immediately from the completeness and soundness of the batch protocol (notice that for soundness, it suffices that x is a NO instance for $\mathcal{R}$ to make $(x_1, \ldots, x_t)$ a NO instance for $\mathcal{R}^{\otimes t}$.

The key question is how to choose the instance-witness pairs in Step 2 in such a way that π hides w_{i^*}. This choice is crucial. To see this, consider a contrived compression function whose goal is to be maximally non-hiding for some specific input x^*. For example, the compression function, in addition to outputting a convincing proof, might check if one of the t inputs is equal to x^*. If so, it also outputs the corresponding witness as part of the proof. Notice that this strategy is still highly compressing. While this is clearly a contrived strategy, since we seek to give a general result, that compiles *any* batch proof, we have to consider such strategies as well.

The above contrived strategy is a major concern for SWI as there exists a specific input, namely x^*, for which the prover always reveals the witness. A natural approach to circumvent this attack is to consider a distributional notion of SWI. That is, consider some efficiently sampleable distribution $\mathcal{D}$ supported over triples (x, w_0, w_1), where $(x, w_0), (x, w_1) \in \mathcal{R}$. Suppose we only want SWI to hold for random instance/witness pairs sampled from $\mathcal{D}$. In such a case, P can choose each (x_i, w_i) from $\mathcal{D}$ independently. Now, for inputs (x, w_0, w_1) that are also generated from $\mathcal{D}$, by symmetry, the function f will be unable to discover whether w_0 or w_1 was guessed (other than with inverse polynomial probability). Intuitively, and this can be formalized, this leads to a distributional-SWI protocol (with an SWI error that decreases polynomially with t).

While the distributional approach described above works, it is weaker than what we aim to achieve in two ways. First, it is restricted to NP languages that have a solved instance generator (recall that if the language is also hard with respect to this distribution then the sampler is a one-way function). Second, the SWI property is distributional - it only holds with respect to instance-witness pairs sampled from $\mathcal{D}$ (rather than the usual worst-case guarantee).

At this point we face a problem. If we aim to get a worst-case SWI guarantee, the contrived compression function f that targets some specific x^* seems like a non-starter. Indeed, using f as a blackbox, it is hopeless to try to discover x^*. Still, if we happened to know that the compression function is precisely the contrived one described above, we could fix the same x^* as part of prover P and then use x^* (with corresponding random witnesses that are also hardwired) in *all* of the coordinates of f. Doing so would hide the specific witness that P uses in the i-th coordinate. But what about a general compression function f? Can we somehow fix specific instance/witness pairs that are specifically good for fooling f? Somewhat surprisingly the answer turns out to be yes.

How to find instance-witness pairs. We prove that for every compression function f there exists a polynomial-size multiset $S \subseteq \mathcal{R}^{\otimes t}$ (i.e. a polynomial number of instance-witness t-tuples), so that if the tuple $((x_1, w_1), \ldots, (x_t, w_t))$ used in the above protocol is sampled uniformly from S, then the resulting protocol is SWI (with error that depends on how compressing f is).

Central to our approach is a lemma of Dell [Del16] (building on work by Drucker [Dru15] and related to a result of [DMO00]) about information lost by compressing functions. Consider a function $g : \{0,1\}^t \to \{0,1\}^{\rho t}$ for some $\rho < 1$. Intuitively, as the function is compressing, it must be losing information about some of its input bits. Dell formalized this by showing that the output distribution of g when its input bits are chosen uniformly at random is not affected much by arbitrarily fixing the bit at a randomly chosen location. Let

B be the uniform distribution over $\{0,1\}^t$, and denote by $B|_{j\leftarrow b}$ the variable corresponding to sampling B and setting the j^{th} co-ordinate to b. Dell showed that in terms of statistical distance:

$$(j, g(B|_{j\leftarrow 0})) \approx_{\sqrt{\rho}} (j, g(B|_{j\leftarrow 1}))\,.$$

Suppose g is a function parameterized by triples (x_i, w_i^0, w_i^1), where $(x_i, w_i^0), (x_i, w_i^1) \in \mathcal{R}$, and uses its input bits b_i to select witness $w_i^{b_i}$, and outputs f computed with these instance-witness pairs $(x_i, w_i^{b_i})$. The above lemma would then say that picking a random $j \in [t]$ and fixing the witness used for x_j to be either of w_j^0 or w_j^1 would not make much of a difference to the output distribution of f. Denoting $(x_1, \ldots, x_t)$ by $\boldsymbol{x}$ and $(w_1, \ldots, w_t)$ by $\boldsymbol{w}$, with $j \leftarrow [t]$ and each w_i sampled uniformly from $\{w_i^0, w_i^1\}$, this implies that:

$$\left(j, \boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{w}|_{j\leftarrow w_j^0})\right) \approx \left(j, \boldsymbol{x}, f(\boldsymbol{x}, \boldsymbol{w}|_{j\leftarrow w_j^1})\right)$$

This is already reminiscent of witness-indistinguishability, though the property here only holds for a randomly chosen instance among a set of t instances. We can, in fact, use this to get the distributional version of SWI discussed above. Consider any distribution D over (x, w_0, w_1) such that $(x, w_0), (x, w_1) \in \mathcal{R}$. Now, with (x, w_0, w_1) and all the (x_i, w_i^0, w_i^1) sampled from $\mathcal{D}$, we have:

$$(j, \boldsymbol{x}|_{j\leftarrow x}, f(\boldsymbol{x}|_{j\leftarrow x}, \boldsymbol{w}|_{j\leftarrow w_0})) \approx (j, \boldsymbol{x}|_{j\leftarrow x}, f(\boldsymbol{x}|_{j\leftarrow x}, \boldsymbol{w}|_{j\leftarrow w_1}))$$

Note that in the protocol above, when the prover inserts the given (x, w) at location j and uses instances x_i and witnesses w_i in the remaining locations, the view of the verifier is precisely $(j, \boldsymbol{x}|_{j\leftarrow x}, f(\boldsymbol{x}|_{j\leftarrow x}, \boldsymbol{w}|_{j\leftarrow w}))$. So the above implies that the *expected* SWI *error* for the protocol when everything is sampled as specified is small.

In other words, for every distribution D over (x, w_0, w_1), there is a distribution over $\left((x_i, w_i^0, w_i^1)\right)$ such that with samples from these, the expected SWI error in our protocol is small. We can view this process as a 2-player zero-sum game: the row player chooses (x, w_0, w_1) and the column player chooses a distribution D over all such tuples. The payoff is the expected SWI error in our protocol. The above argument shows that for every strategy D for the column player there is a mixed strategy for the row player (specifically, the strategy D), for which we can bound the expected payoff. The minimax theorem now implies that there is a *single* distribution D' over tuples $\left((x_i, w_i^0, w_i^1)\right)$ such that *for every* (x, w_0, w_1), if the prover uses a sample from D' to populate the other inputs to f, the SWI error is small. Using a sparse minimax theorem [LY94] now implies the existence of a polynomial-sized multiset of $\left((x_i, w_i^0, w_i^1)\right)$'s such that sampling from this leads to almost the same SWI error. This implies the existence of the set we want, which we hard-code into the prover's algorithm as a non-uniform advice.[7]

Remark 1.4. *The $O(\sqrt{\rho})$ error in our analysis is tight for some functions (e.g., if g is the majority function).*

Handling Multi-round Protocols. To handle multi-round protocols we follow the same basic strategy, running the underlying batch protocol using tailor-made instance/witness pairs. While we are unable to show that this approach satisfies *malicious-verifier* SWI, we manage to show that it is *honest-verifier* SWI. We do so by first extending the above analysis to 2-message protocols (i.e. a verifier message followed by a prover message). To handle protocols with more messages, we observe that when analyzing *honest-verifier* SWI, we can imagine that the verifier sends to the prover all of its randomness in advance and reduce back to the 2-message case.

Augmenting the Basic Result in The Interactive Setting. At this point we have a transformation from any batch protocol into an honest-verifier SWI protocol with inverse polynomial SWI error and a non-uniform prover. In the interactive setting, we improve this state of affairs as follows:

[7]It seems tempting to try to use a uniform minimax theorem, as in [VZ13], to obtain a uniform honest prover. A key bottleneck however is that our payoff function does not seem to be efficiently computable. See also Remark 3.10.

1. In the case of statistical soundness, if the batch proof is *public-coin*, we can rely on an information-theoretic coin-flipping protocol due to Goldreich *et al.* [GSV98] which leads to malicious-verifier SWI.[8] For the case of private-coin protocols, following an approach of [BMO90, OVY93, Oka96], we show that assuming the existence of a one-way function, we can transform any honest-verifier SWI protocol to be malicious-verifier SWI. We emphasize that despite the usage of a one-way function, both soundness and hiding properties are *statistical*.

2. In the case of computational soundness, assuming the existence of a one-way function, we can rely on the celebrated "FLS trick" of Feige *et al.* [FLS90] to bootstrap the honest-verifier SWI argument to an honest-verifier SZK argument.[9] Then, using the [GMW86] compiler from honest-verifier to malicious verifier we obtain a full-fledged malicious verifier zero-knowledge argument (using the [FS90a] constant-round private-coin argument-system as the underlying zero-knowledge proof).

Explicit Proof Systems in the Non-Interactive Setting. We now discuss our results in the non-interactive setting, where we are able to construct new *explicit* proof systems from BARGs. Recall that here we provide a computational ZK system based on one-way functions, or a statistical ZK system based on dual-mode commitments. We start by addressing a challenge common to both, then we address the techniques required for each of the proof systems.

Somewhere Soundness. In the non-interactive setting, the prover sends a single message that depends on the common random string (CRS). While in the interactive setting, our transformation required that the prover sends its choice of $(x_1, \ldots, x_t)$ before starting the batch protocol, now these have to be chosen after the CRS is generated, which may foil soundness. One obvious solution is to rely on adaptively-sound BARGs. However, that is a rather strong requirement that is not met by existing non-interactive BARGs (in fact, adaptively-sound BARGs of knowledge would already imply full-fledged succinct non-interactive arguments [BHK17]). Instead, we use the notion of *somewhere soundness*, which is a relaxation of the *somewhere extractability* notion that is satisfied by all existing non-interactive BARGs. Somewhere soundness requires that the CRS can be programmed with a specific index i, so that adaptive soundness is guaranteed only with respect to the instance x_i, furthermore the programmed CRS is indistinguishable from a normal one. This notion is already sufficient to obtain soundness of the resulting non-interactive SWI (in the CRS model).

Given the above, we can already apply a similar minmax argument to before, and obtain a non-interactive system with a non-uniform prover and inverse polynomial WI error. We next explain how we avoid both caveats. We start with the construction of the second (statistical ZK) system based on lossy encryption, as it is simpler to describe and already contains most of the machinery needed.

From Distributional ZK to Worst-Case ZK, Uniformly. Our starting point is the *distributional* SWI protocol we obtain from the basic transformation. Indeed, for efficiently uniformly samplable instance-witness distributions, this protocol is uniform. Before, to enhance the distributional SWI requirement to *worst-case* SWI requirement, we invoked the minmax theorem, which led to non-uniformity. Now, we take a different route – we show a general transformation from the distributional setting to the worst-case setting that, assuming lossy encryption, preserves statistical security. It will be easier to describe the transformation (as well as the next one) for SZK rather than SWI; this is w.l.o.g as the gap between the two can be bridged using one-way functions, using the well-known FLS trick [FLS90].

The distributional to worst-case transformation is inspired by local to global transformations from the zero knowledge literature such as reducing general ZK to ZK for fixed-length statements (c.f. [Gol01, Section 4.10]) or the NIZK of [GOS06]. Specifically, in the constructed (worst-case) NIZK, the prover commits to

[8] Note that we cannot use the honest-to-malicious transformation of Hubácek *et al.* [HRV18] (which works also in the private-coin setting) because that result relies on the connection of SZK to instance dependent commitments. Thus, it is not clear how to apply their result in the setting of SWI.

[9] In a nutshell, the verifier sends to the prover $z = G(s)$, where G is a PRG and s is a random seed, and the prover then proves that either $x \in \mathcal{L}$ or z is in the image of the PRG. Computational soundness can be argued by switching to a truly random z, and SZK by having the simulator use s as the witness.

all the wires of the NP verification circuit, and proves local consistency of each gate using distributional NISZKA. Specifically, for each gate, we consider the distribution of *random* commitments of *random* wire values satisfying the gate. While the prover actually uses a specific (worst-case) wire assignment for the gate, this only skews the distribution by a constant factor, as the total number of assignments is constant. As the commitment we use dual-mode commitments where for computationally indistinguishable common reference strings, we get either statistical hiding or statistical binding. The actual proof system uses the statistically-hiding mode, and accordingly preserves statistical ZK. In the soundness analysis, we use the binding mode.

Reducing the SWI Error. Recall that our distributional SWI system has an inverse polynomial WI error, accordingly so does the worst-case SZK system resulting from the last transformation. We prove a statistical amplification theorem that enables us to reduce this error. Previously, an amplification theorem was shown in the computational setting by [GJS19] (assuming subexponential public-key encryption). The statistical transformation we show follows a similar blueprint to the computational one — we construct a combiner based on MPC-in-the-head (in our case, an information-theoretic one, such as [BGW88]). The analysis in the statistical setting is different. We show based on a coupling proof, similar to the one in [LM20], that the combiner is in fact also an amplifier. This transformation too uses dual mode commitments as a building block.

Computational Zero Knowledge from One-Way Functions. The only assumption used in the above transformations (on top of BARGs) is dual-mode commitments. The first question that comes to mind is whether the dual-mode commitments can be replaced with plain statistically-hiding commitments (which can be constructed, for instance, based on collision-resistant hashing). However, this turns out to be insufficient for soundness. If we replace the dual-mode commitment with a plain statistically-binding commitment (which can be constructed from one-way functions) then soundness can be proven. Since such commitments are only computationally hiding, we can no longer hope for statistical ZK of the final scheme, but one could hope that this would achieve computational ZK. However, while we are able to prove that the distributional ZK to worst-case ZK work also in the computational setting, we are unable to do the same for the second application that reduces the SWI error to negligible. Also, we wish to avoid the computational amplification of [GJS19], which requires also sub-exponential public-key encryption.

We overcome this difficulty using the notion of *computationally instance-dependent commitments* (CIDC) [FS90b]. Such commitments are parameterized by an instance z of a given NP language $\mathcal{L}$. When $z \notin \mathcal{L}$ they guarantee statistical binding. When $z \in \mathcal{L}$, there is a way to generate fake commitments $\widetilde{c}$ that are perfectly hiding. Specifically, given any witness for z, it is possible to efficiently generate a fake commitment and opening $(\widetilde{c}, \widetilde{d})$ for message m such that $\widetilde{c}, \widetilde{d}$ are *computationally* indistinguishable from a real commitment to m with its decommitment c, d. Such commitments are known to exist for all of NP assuming one-way functions [FS90b].[10]

We replace the commitments in the previous two transformations with CIDC depending on an NP language $\mathcal{L}'$. This essentially allows us to construct a $\mathcal{L}'$-dependent NIZK for proving membership in any NP language $\mathcal{L}$. Here soundness is guaranteed when the system is parameterized by $z \notin \mathcal{L}'$ and computational ZK is guaranteed when $z \in \mathcal{L}'$. Indeed, when $z \notin \mathcal{L}'$, the corresponding commitments are statistical binding as required for soundness. When $z' \in \mathcal{L}'$, we can switch (in the analysis) to a computationally-indistinguishable world where the commitments are statistically hiding, and where accordingly the previous described transformations do hold. To obtain our final proof system we choose $\mathcal{L}'$ to be the same NP language $\mathcal{L}$ for which we prove membership.

Remark 1.5 (On Using the Above in the Interactive Setting)**.** *A natural question is whether we can use similar transformations as above to also achieve uniform protocols in the interactive setting. While the answer is generally "yes", the resulting interactive protocols are not as interesting, as they are subsumed by*

[10]The above notion of instance-dependent commitments should not be confused with that of Ong and Vadhan [OV08], where when $z \in \mathcal{L}$, real commitments (rather than fake ones) are statistically hiding. Indeed, this notion only exists for languages in SZK.

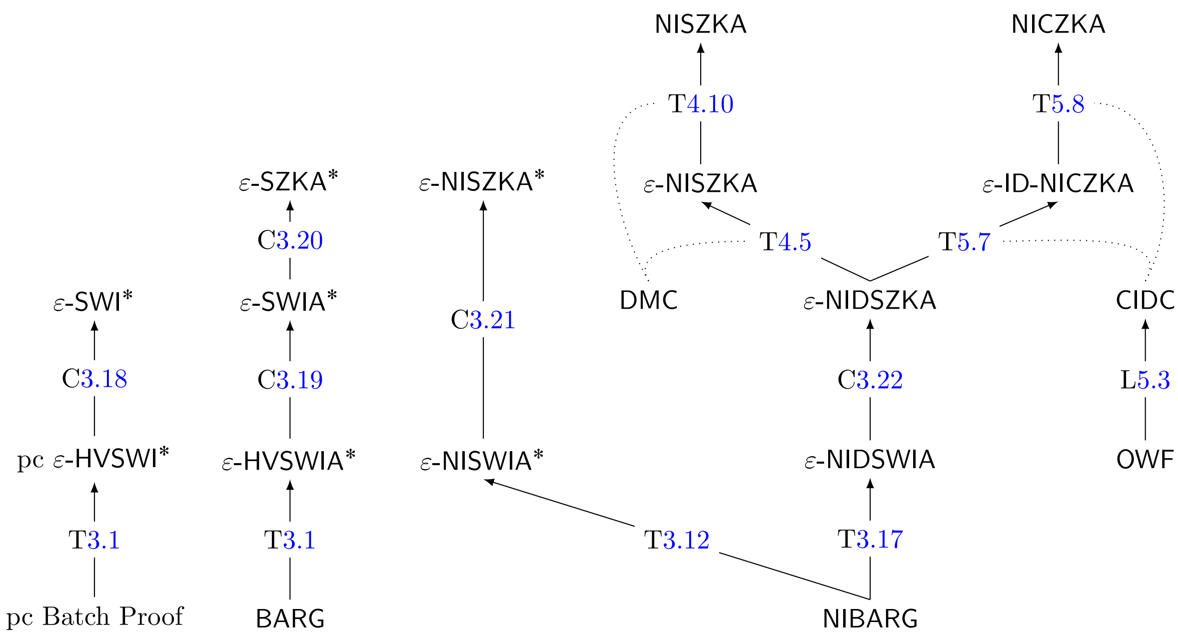

Figure 1.1: Schematic diagram showing our results. Nodes correspond to primitives. When a proof system is suffixed with an asterisk, it indicates that its prover is *non-uniform*. When a proof system is prefixed with ε, its ZK or WI error is only inverse polynomial. When an interactive proof systems is prefixed with "pc", then it is public-coin. Edges capture relationship between primitives. A solid arrow from primitive A to B indicates that A implies B, with the theorem (T), lemma (L) or corollary (C) that proves this implication linked on the arrow. Additional computational assumptions required for this implication are indicated by dotted lines. Corollaries 3.19 to 3.22 require also the existence of one-way functions.

known results. In particular, constant round computational ZK *is already known from one-way functions [FLS90], and constant round* statistical ZK *is already known from statistically-hiding commitments (c.f. [BP19]), which in turn follow from lossy encryption.*

2 Definitions

We rely on standard computational concepts and notation:

- A binary relation $\mathcal{R} \subseteq \{0,1\}^* \times \{0,1\}^*$ is said to be *polynomially balanced* if there is a polynomial p such that for any strings $x, y \in \{0,1\}^*$, if $(x,y) \in \mathcal{R}$ then $|y| \leqslant p(|x|)$. For a (polynomially-balanced) relation $\mathcal{R}$ and $\lambda \in \mathbb{N}$, $\mathcal{R}_\lambda$ denotes $\mathcal{R} \cap (\{0,1\}^\lambda \times \{0,1\}^*)$. For a (polynomially-balanced) relation $\mathcal{R}$, we use $\mathcal{L}(\mathcal{R})$ to denote the language defined by $\mathcal{R}$, i.e., $\{x \in \{0,1\}^* : \exists w \in \{0,1\}^* \text{ s.t. } (x,w) \in \mathcal{R}\}$. $\mathcal{L}(\mathcal{R}_\lambda) \subseteq \{0,1\}^\lambda$ is defined similarly, but with respect to $\mathcal{R}_\lambda$.

- We say that a function $f : \mathbb{N} \to \mathbb{R}$ is *negligible* if for all constants $c > 0$, there exists $N \in \mathbb{N}$ such that for all $n > N$, $f(n) < n^{-c}$. We sometimes denote negligible functions by negl. We say that a function $f : \mathbb{N} \to \mathbb{R}$ is *overwhelming* if $1 - f$ is negligible.

- A PPT algorithm is a probabilistic polynomial-time algorithm. A family of circuits $\mathsf{A} = (\mathsf{A}_\lambda)_{\lambda \in \mathbb{N}}$ is *polynomial-sized* if there exists a polynomial p such that for all $\lambda \in \mathbb{N}$, $|\mathsf{A}_\lambda| \leqslant p(\lambda)$. We follow the common practice of modelling any efficient adversary as a family of polynomial-size circuits $\mathsf{A} = (\mathsf{A}_\lambda)_{\lambda \in \mathbb{N}}$. We also say that such an A runs in *non-uniform polynomial time*.

- For a distribution X over a set Ω and $x \in \Omega$, we use $x \leftarrow X$ to denote the result of sampling from X. For a random variable X over Ω and $x \in \Omega$, we use $X(x)$ to denote the probability that the value of the random variable is x. We denote *statistical distance* by SD. For two random variables X, Y and $\varepsilon \in [0,1]$, we write $X \approx_\varepsilon Y$ to denote the fact that $\mathsf{SD}(X,Y) \leqslant \varepsilon$ and say that X is *ε-statistically indistinguishable* from Y. For two ensembles $\mathcal{X} = (X_\lambda)_{\lambda\in\mathbb{N}}$ and $\mathcal{Y} = (Y_\lambda)_{\lambda\in\mathbb{N}}$ and function ε, we write $\mathcal{X} \approx_\varepsilon \mathcal{Y}$ if for all large enough λ, $X_\lambda \approx_{\varepsilon(\lambda)} Y_\lambda$. For $\mathcal{X}$, $\mathcal{Y}$ and ε as above, we write $\mathcal{X} \overset{c}{\approx}_\varepsilon \mathcal{Y}$ to denote that the *computational distance* is at most ε. That is, for every polynomial-sized family of distinguishers $\mathsf{D} = (\mathsf{D}_\lambda)_{\lambda\in\mathbb{N}}$ and large enough $\lambda \in \mathbb{N}$

$$\left| \Pr_{x\leftarrow X_\lambda}[\mathsf{D}_\lambda(x) = 1] - \Pr_{y\leftarrow Y_\lambda}[\mathsf{D}_\lambda(y) = 1] \right| \leqslant \epsilon(\lambda).$$

  In both cases, we drop ε from subscript when it is a negligible function. Therefore, $\mathcal{X} \overset{c}{\approx} \mathcal{Y}$ denotes that $\mathcal{X}$ is *computationally indistinguishable* from $\mathcal{Y}$.

- We say that an ensemble of distributions $\mathcal{D} = (D_\lambda)_{\lambda\in\mathbb{N}}$ is *efficiently sampleable* if there exists a polynomial-sized family of circuits $\mathsf{S} = (\mathsf{S}_\lambda)_{\lambda\in\mathbb{N}}$ such that the distribution of the outputs of S_λ, on input a uniformly random string, is D_λ. We also use the stronger *uniform* notion of efficient sampleability, where there exists a PPT algorithm S such that the output distribution of $\mathsf{S}(1^\lambda)$ is D_λ.

- We denote by $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ an interactive protocol between two parties P and V. For common input x and auxiliary input w for P, by $\langle \mathsf{P}(w) \leftrightarrows \mathsf{V} \rangle(x)$ we denote the *view* of V in the protocol, including all received messages and random coins (if V is randomized). We abuse notation and write $\langle \mathsf{P}(w) \leftrightarrows \mathsf{V} \rangle(x) = 1$ to denote the fact that V accepts. A similar convention applies also to non-interactive protocols, which are denoted by $\langle \mathsf{P} \rightarrow \mathsf{V} \rangle$.

2.1 Interactive Protocols: Soundness, Privacy and Batching

In this paper, we are mainly interested in *doubly-efficient* interactive protocols [Gol18] as defined below.

Definition 2.1 (Doubly-Efficient Interactive Protocols)**.** *Let $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ be an interactive protocol for an* NP *relation $\mathcal{R}$, i.e., the common input is a statement $x \in \mathcal{R}$ and the auxiliary input for the (honest) prover* P *is a witness w for x. The protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is* doubly efficient *if both* P *and* V *are PPT algorithms.*

Remark 2.2. *We will also consider doubly-efficient interactive protocols where the prover is non-uniform (i.e., a polynomial-sized family of circuits), in which case we will always explicitly point this out. In the rest of the paper, we drop "doubly efficient", and by interactive protocols we always refer to doubly-efficient interactive protocols.*

We next define the relevant notions of completeness, soundness and privacy. In the following definitions $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is a (doubly-efficient) protocol for an NP relation $\mathcal{R}$.

Definition 2.3 (Completeness)**.** *$\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is* complete *with (completeness) error ε if for all large-enough $\lambda \in \mathbb{N}$ and every $(x,w) \in \mathcal{R}_\lambda$*

$$\Pr\left[\langle \mathsf{P}(w) \leftrightarrows \mathsf{V} \rangle(x) = 1\right] \geqslant 1 - \varepsilon(\lambda) \ .$$

Definition 2.4 (Statistical Soundness)**.** *The protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is* statistically sound *with (soundness) error ε if for every (unbounded) prover P^*, all large enough $\lambda \in \mathbb{N}$ and every $x \in \{0,1\}^\lambda \backslash \mathcal{L}(\mathcal{R})$,*

$$\Pr\left[\langle \mathsf{P}^* \leftrightarrows \mathsf{V} \rangle(x) = 1\right] \leqslant \varepsilon(\lambda) \ .$$

A statistically sound protocol is also called a proof.

Definition 2.5 (Computational Soundness)**.** $\langle \mathsf{P} \leftrightarrows \mathsf{V}\rangle$ *is* computationally sound *if for every polynomial-size circuit family of provers* $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda\in\mathbb{N}}$*, there exists a negligible function* μ*, such that for every* $\lambda \in \mathbb{N}$ *and every* $x \in \{0,1\}^\lambda \backslash \mathcal{L}(\mathcal{R})$,

$$\Pr[\langle \mathsf{P}^*_\lambda \leftrightarrows \mathsf{V}\rangle(x) = 1] \leqslant \mu(\lambda) \ .$$

A computationally-sound protocol is also called an argument.

Definition 2.6 (SWI: Statistical Witness Indistinguishability)**.** $\langle \mathsf{P} \leftrightarrows \mathsf{V}\rangle$ *is* statistically witness-indistinguishable *with error* ε *if for every polynomial-size circuit family* $\mathsf{V}^* = (\mathsf{V}^*_\lambda)_{\lambda\in\mathbb{N}}$,

$$(\langle \mathsf{P}(w_0) \leftrightarrows \mathsf{V}^*_\lambda\rangle(x))_{\substack{(x,w_0,w_1)\in\mathcal{R}\\ |x|=\lambda}} \approx_\varepsilon (\langle \mathsf{P}(w_1) \leftrightarrows \mathsf{V}^*_\lambda\rangle(x))_{\substack{(x,w_0,w_1)\in\mathcal{R}\\ |x|=\lambda}} \ ,$$

where $(x, w_0, w_1) \in \mathcal{R}$ *is an abuse of notation to be interpreted as* $(x, w_0), (x, w_1) \in \mathcal{R}$*. If the above indistinguishability is only guaranteed for the honest verifier* V*, then* $\langle \mathsf{P} \leftrightarrows \mathsf{V}\rangle$ *is* honest-verifier *statistically witness-indistinguishable.*

Definition 2.7 (SZK and CZK: Statistical and Computational Zero Knowledge)**.** $\langle \mathsf{P} \leftrightarrows \mathsf{V}\rangle$ *is* statistically zero-knowledge *with error* ε *if there exists an* expected *PPT simulator* S *such that for every polynomial-size circuit family* $\mathsf{V}^* = (\mathsf{V}^*_\lambda)_{\lambda\in\mathbb{N}}$,

$$(\langle \mathsf{P}(w) \leftrightarrows \mathsf{V}^*_\lambda\rangle(x))_{\substack{(x,w)\in\mathcal{R}\\ |x|=\lambda}} \approx_\varepsilon (\mathsf{S}(x, \mathsf{V}^*_\lambda))_{\substack{(x,w)\in\mathcal{R}\\ |x|=\lambda}} \ . \tag{1}$$

The definition of computational *ZK is obtained by replacing statistical distance in Eq.* (1) *with computational distance (i.e.,* $\approx_\varepsilon$ *with* $\overset{c}{\approx}_\varepsilon$*). The protocol is* honest-verifier *statistical or computational zero-knowledge if the above is only guaranteed for the honest verifier* V.

Interactive Batching. Here we define interactive batch protocols.

Definition 2.8 (Interactive Batch Protocol)**.** *A* batch protocol *for* $\mathcal{R}$ *is an interactive protocol for* $\bigcup_{t\in\mathbb{N}} \mathcal{R}^{\otimes t}$*, where:*

$$\mathcal{R}^{\otimes t} := \{(x_1, \ldots, x_t), (w_1, \ldots, w_t) : |x_1| = \cdots = |x_t|, (x_1, w_1), \ldots, (x_t, w_t) \in \mathcal{R}\} \ . \tag{2}$$

- *The protocol's completeness and soundness errors (*$\delta(\lambda, t)$ *and* $\varepsilon(\lambda, t)$*) are defined to be its largest completeness and soundness errors, respectively, on any* t *instances (and any of their witnesses) of size* λ
- *The protocol has compression rate* $\rho = \rho(\lambda, t)$*, for instance length* λ *and number of instances* t*, if maximum total length of prover messages (over all such sets of instances) is* ρt

2.2 Non-Interactive Protocols: Soundness, Privacy and Batching

In this paper, we only consider *doubly-efficient* non-interactive protocols in the *common reference string* (CRS) model. Below we define this primitive and the different notions of soundness and privacy that we need.

Definition 2.9 (Non-Interactive Protocol in CRS model)**.** *A* non-interactive protocol $\langle \mathsf{P} \to \mathsf{V}\rangle$ in CRS model *for an* NP *relation* $\mathcal{R}$ *is a triple of algorithms* $(\mathsf{Gen}, \mathsf{P}, \mathsf{V})$*, with the following syntax:*

- $crs \leftarrow \mathsf{Gen}(1^\lambda)$*: Given the instance size* λ*, the randomised* set-up *algorithm* Gen *outputs a CRS* crs*.*
- $\pi \leftarrow \mathsf{P}(crs, x, w)$*: Given CRS* crs*, instance* x*, and witness* w*, the randomised* prover *outputs a proof* π
- $b := \mathsf{V}(crs, x, \pi)$*: Given CRS* crs*, instance* x*, and proof* π*, the deterministic* verifier *returns a bit* b *representing accept or reject.*

In the following definitions, $\langle \mathsf{P} \to \mathsf{V} \rangle$ is a non-interactive protocol in CRS model for an NP relation $\mathcal{R}$.

Definition 2.10 (Completeness for Non-Interactive Protocols). $\langle \mathsf{P} \to \mathsf{V} \rangle$ *has* completeness error δ *if for all large enough* $\lambda \in \mathbb{N}$ *and* $(x, w) \in \mathcal{R}_\lambda$,

$$\Pr_{\substack{crs \leftarrow \mathsf{Gen}(1^\lambda) \\ \pi \leftarrow \mathsf{P}(crs, x, w)}} [\mathsf{V}(crs, x, \pi) = 1] \geqslant 1 - \delta(\lambda).$$

For soundness, we will need the following notions.

Definition 2.11 (Non-Adaptive Computational Soundness). $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* non-adaptively computationally sound *if for every polynomial-size circuit family of provers* $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda \in \mathbb{N}}$*, there is a negligible function* μ*, such that for all* $\lambda \in \mathbb{N}$ *and all* $x \in \{0,1\}^\lambda \backslash \mathcal{L}(\mathcal{R})$*:*

$$\Pr_{crs \leftarrow \mathsf{Gen}(1^\lambda)} [\mathsf{V}(crs, x, \mathsf{P}^*_\lambda(crs, x)) = 1] \leqslant \mu(\lambda).$$

Definition 2.12 (Adaptive Computational Soundness). $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* adaptively computationally sound *if, for every polynomial-size circuit family of provers* $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda \in \mathbb{N}}$*, there is a negligible function* μ*, such that for all* $\lambda \in \mathbb{N}$*:*

$$\Pr_{crs \leftarrow \mathsf{Gen}(1^\lambda)} [x \notin \mathcal{L}(\mathcal{R}_\lambda) \wedge \mathsf{V}(crs, x, \pi) = 1] \leqslant \mu(\lambda),$$

where $(x, \pi) := \mathsf{P}^*_\lambda(crs)$*.*

We will need the following notions of (worst-case) hiding.

Definition 2.13 (SWI and CWI). $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* non-adaptively SWI *with error* ε *if*

$$(crs, \pi_0)_{\substack{(x, w_0, w_1) \in \mathcal{R} \\ |x| = \lambda}} \approx_\varepsilon (crs, \pi_1)_{\substack{(x, w_0, w_1) \in \mathcal{R} \\ |x| = \lambda}}, \tag{3}$$

where $crs \leftarrow \mathsf{Gen}(1^\lambda)$*,* $\pi_0 \leftarrow \mathsf{P}(crs, x, w_0)$*, and* $\pi_1 \leftarrow \mathsf{P}(crs, x, w_1)$*. The definition of non-adaptive* CWI *is obtained by replacing statistical distance in Eq.* (3) *with computational distance.*

Definition 2.14 (SZK and CZK). $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* non-adaptively statistically zero-knowledge *with error* ε *if there exists a PPT simulator* S *such that:*

$$((crs, \pi))_{\substack{(x, w) \in \mathcal{R} \\ |x| = \lambda}} \approx_\varepsilon (\mathsf{S}(x))_{\substack{(x, w) \in \mathcal{R} \\ |x| = \lambda}} . \tag{4}$$

where $crs \leftarrow \mathsf{Gen}(1^\lambda)$ *and* $\pi \leftarrow \mathsf{P}(crs, x, w)$*. The definition of non-adaptive* CZK *is obtained by replacing statistical distance in Eq.* (4) *with computational distance.*

We will also need *distributional* notions of hiding [Gol93, DNRS99].

Definition 2.15 (DSWI: Distributional SWI for Non-Interactive Protocols). *Let* $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$ *be an efficiently-sampleable distribution, where* D_λ *is supported over triples* (x, w_0, w_1) *such that* $(x, w_0), (x, w_1) \in \mathcal{R}_\lambda$*.* $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* distributionally *SWI for* $\mathcal{D}$ *with error* ε *if for all large enough* $\lambda \in \mathbb{N}$

$$\mathop{\mathbb{E}}_{(x, w_0, w_1) \leftarrow D_\lambda} [\mathsf{SD}((crs, \pi_0), (crs, \pi_1))] \leqslant \varepsilon(\lambda),$$

where $crs \leftarrow \mathsf{Gen}(1^\lambda)$*,* $\pi_0 \leftarrow \mathsf{P}(crs, x, w_0)$*, and* $\pi_1 \leftarrow \mathsf{P}(crs, x, w_1)$*.*

Definition 2.16 (DSZK: Distributional SZK for Non-Interactive Protocols). *Let* $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$ *be an efficiently-sampleable distribution, where* D_λ *is supported over* $\mathcal{R}_\lambda$*.* $\langle \mathsf{P} \to \mathsf{V} \rangle$ *is* distributionally *SZK for* $\mathcal{D}$ *with error* ε *if there exists a PPT simulator* S *such that for all large enough* $\lambda \in \mathbb{N}$

$$\mathop{\mathbb{E}}_{(x, w) \leftarrow D_\lambda} [\mathsf{SD}((crs, \pi), \mathsf{S}(x))] \leqslant \varepsilon(\lambda),$$

where $crs \leftarrow \mathsf{Gen}(1^\lambda)$ *and* $\pi \leftarrow \mathsf{P}(crs, x, w)$*.*

Dual-Mode Non-Interactive Protocols. It will be useful to define non-interactive protocols where the set-up algorithm has two different, indistinguishable modes [GOS12].

Definition 2.17 (Dual-Mode Non-Interactive Protocol)**.** *A* dual-mode *non-interactive protocol for an* NP *relation* $\mathcal{R}$ *is a four-tuple of algorithms* $(\mathsf{Gen}_1, \mathsf{Gen}_2, \mathsf{P}, \mathsf{V})$*, such that both* $(\mathsf{Gen}_1, \mathsf{P}, \mathsf{V})$ *and* $(\mathsf{Gen}_2, \mathsf{P}, \mathsf{V})$ *are non-interactive protocols for* $\mathcal{R}$ *with syntax as defined in Definition 2.9. We require the protocol to satisfy the following basic properties:*

1. $(\mathsf{Gen}_1, \mathsf{P}, \mathsf{V})$ *and* $(\mathsf{Gen}_2, \mathsf{P}, \mathsf{V})$ *are both* complete *(Definition 2.10).*
2. *The CRS generated by the two set-up modes* Gen_1 *and* Gen_2 *must be computationally indistinguishable. We refer to this property as* mode-indistinguishability*.*

We need three instantiations of Definition 2.17, presented in Definitions 2.18 and 2.19.

Definition 2.18 (Dual-Mode NISZKA and NISWIA)**.** *A dual-mode non-interactive protocol* $(\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}, \mathsf{V})$ *for an* NP *relation* $\mathcal{R}$ *is a* dual-mode ε-NISZKA *(resp.,* ε-NISWIA*) for* $\mathcal{R}$ *if the following additional requirements are satisfied:*

1. $(\mathsf{SHGen}, \mathsf{P}, \mathsf{V})$ *is statistically ZK (resp., WI) with error* ε*. Therefore, we refer to this mode as the* statistically-hiding *mode.*
2. $(\mathsf{ASGen}, \mathsf{P}, \mathsf{V}))$ *is* adaptively *computationally sound with negligible soundness error. Therefore, we refer to this mode as the* adaptively-sound *mode.*

In the *distributional* formulation, i.e., dual-mode ε-$\mathsf{NIDSZKA}$ (resp., ε-$\mathsf{NIDSWIA}$), the hiding requirement in Item 1 is relaxed to its distributional formulation, i.e., Definition 2.16 (resp., Definition 2.15).

Definition 2.19 (Dual-Mode $\mathsf{NIDSZKA}$ and $\mathsf{NIDSWIA}$)**.** *Let* $\mathcal{R}$ *be an* NP *relation, and let* $\mathcal{D}$ *be an efficiently-sampleable distribution as in Definition 2.16 (resp., Definition 2.15). A dual-mode non-interactive protocol* $(\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}, \mathsf{V})$ *for* $\mathcal{R}$ *is a* dual-mode ε-$\mathsf{NIDSZKA}$ *(resp.,* ε-NIDSWI*) for* $\mathcal{D}$ *if the following additional requirements are satisfied:*

1. $(\mathsf{SHGen}, \mathsf{P}, \mathsf{V})$ *is distributionally SZK (resp., SWI) for* $\mathcal{D}$ *with error* ε*. We refer to this mode as the* statistically-hiding *mode.*
2. $(\mathsf{ASGen}, \mathsf{P}, \mathsf{V}))$ *is* adaptively *computationally sound with negligible soundness error.*[11] *We refer to this mode as the* adaptively-sound *mode.*

Remark 2.20 (On Definitions 2.18 and 2.19)**.** *The following remarks are stated for dual-mode* NISZKA*, but it applies to all the other instantiations of Definition 2.17.*

1. *Whenever we say that a dual-mode* NISZKA *is statistically ZK (resp., adaptively sound), we are implicitly referring to its statistically-hiding (resp., adaptively-sound) mode.*
2. *As a consequence of mode-indistinguishability, if one of the modes has negligible correctness error, then so does the other.*

The following remarks are stated for dual-mode NISZKA*, but it applies also to dual-mode* NISWIA*.*

3. *As a consequence of mode-indistinguishability, we can infer that:*
   (a) *the statistically-hiding mode has* non-adaptive *computational soundness (with negligible soundness error),*
   (b) *the adaptive-soundness mode is computationally ZK with error* $\varepsilon + \mathrm{negl}(\lambda)$

[11] Note that the soundness requirement here is worst case, with respect to the relation $\mathcal{R}$.

Remark 2.21 (On Adaptive ZK)**.** *Throughout the paper we focus on non-adaptive* ZK*, both in the statistical and computational settings. We note here that the guarantee can be strengthened to adaptive* ZK*:*

1. *Non-adaptive statistical ZK with error ε implies adaptive statistical ZK with error $\varepsilon \cdot 2^n$. Accordingly, if ε can be made small enough, one gets adaptive statistical ZK (this will be the case in our construction). For dual-mode* NISZKA*, mode indistinguishability also implies* adaptive *computational ZK in the adaptively-sound mode.*

2. *In the case of computational zero knowledge, it is known [KMY23] that assuming one-way functions, any adaptively-sound* NICZKA *can be turned into one with adaptive* CZK*.*

Remark 2.22 (Multi-Instance ZK)**.** *We restrict attention to single-instance non-interactive ZK. We note that assuming one-way functions, this can be strengthened to multi-instance (in both the statististical and computational settings) [FLS90].*

Non-Interactive Batching. Here we define non-interactive batch protocols and the notion of soundness we need.

Definition 2.23 (Non-Interactive Batch Protocol in the CRS Model)**.** *A non-interactive* batch *protocol is a four-tuple of algorithms* $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *with the following syntax::*

- $crs \leftarrow \mathsf{Gen}(1^\lambda, 1^t)$*: Given the instance size λ and the number of instances t, the randomised* set-up *algorithm outputs a CRS crs*
- $(crs^*, td) \leftarrow \mathsf{TGen}(1^\lambda, 1^t, i^*)$*: Given in addition an index $i^* \in [t]$, the* trapdoored set-up *algorithm outputs a CRS crs^* together with a trapdoor td*
- $\pi \leftarrow \mathsf{P}(crs, (x_1, \ldots, x_t), (w_1, \ldots, w_t))$*: Given CRS crs, instances x_i, and witnesses w_i, the randomised* prover *outputs a proof π*
- $b := \mathsf{V}(crs, (x_1, \ldots, x_t), \pi)$*: Given CRS crs, instances x_i, and proof π, the deterministic* verifier *outputs a bit b representing accept or reject*

Here, the prover's communication is just the proof π, and the compression rate is defined with respect to this.

The following definitions of soundness properties are adapted from [CJJ22], though they have been simplified and slightly weakened as this is sufficient for our purposes.

Definition 2.24 (CRS Indistinguishability)**.** *A batch protocol* $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *is* CRS-indistinguishable *if for every polynomial t and every $i(\lambda) \in [t(\lambda)]$, the distributions of* $\mathsf{Gen}(1^\lambda, 1^{t(\lambda)})$ *and crs^* sampled from* $\mathsf{TGen}(1^\lambda, 1^{t(\lambda)}, i(\lambda))$ *are computationally indistinguishable.*

Definition 2.25 (Somewhere Soundness)**.** *A batch protocol* $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *for a relation $\mathcal{R}$ is* somewhere computationally sound *if it satisfies CRS indistinguishability, and for every polynomial t and polynomial-size circuit family of provers $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda \in \mathbb{N}}$, there is a negligible function μ such that for all $\lambda \in \mathbb{N}$, letting $t = t(\lambda)$, and for every $i^* \in [t]$:*

$$\Pr_{crs}\left[x_{i^*} \notin \mathcal{L}(\mathcal{R}_\lambda) \wedge \mathsf{V}(crs, (x_1, \ldots, x_t), \pi) = 1\right] \leqslant \mu(\lambda),$$

where $(crs, td) \leftarrow \mathsf{TGen}(1^\lambda, 1^t, i^*)$*, and* $((x_1, \ldots, x_t), \pi) := \mathsf{P}^*_\lambda(crs, i^*)$*.*

2.3 List of Proof Systems

The proof systems that are relevant to this paper are listed below.

- Batch proof: Interactive batch protocol (Definition 2.8) satisfying Definitions 2.3 and 2.4.

- BARG – Batch ARGument: Interactive batch protocol satisfying Definitions 2.3 and 2.5.
- NIBARG – Non-Interactive Batch ARGument: Non-interactive batch protocol (Definition 2.23) satisfying Definitions 2.10 and 2.25.
- SWI (resp., SWIA) – Statistical Witness-Indistinguishable proof (resp., Argument): Interactive protocol satisfying Definitions 2.3 and 2.6 and Definition 2.5 (resp., Definition 2.4).
- HVSWI (resp., HVSWIA) – Honest-Verifier SWI proof (resp., Argument): Interactive protocol satisfying Definition 2.3, Definition 2.6 restricted to *honest verifiers* and Definition 2.4 (resp., Definition 2.5).
- SZKA – Statistical Zero-Knowledge Argument: Interactive protocol (Definition 2.1) satisfying Definitions 2.3, 2.5 and 2.7.
- Dual-Mode NISZKA (resp., NISWIA) – Dual-Mode Non-Interactive SZKA (resp., SWIA): Definition 2.18.
- Dual-mode $\mathsf{NIDSZKA}$ (resp., $\mathsf{NIDSWIA}$) – Dual-mode Non-Interactive Distributional SZKA (resp., SWIA): Definition 2.19
- NICZKA (resp., NICWIA) – Non-Interactive Computational ZK (resp., WI) Argument: Non-interactive protocol (Definition 2.9) satisfying Definitions 2.10, 2.12 and 2.14 (resp., Definition 2.13).
- Dual-Mode $\mathsf{ID\text{-}NICZKA}$ (resp., $\mathsf{ID\text{-}NICWIA}$) – Dual-Mode Instance-Dependent NICZKA (resp., NICWIA): Definition 5.4.

3 Statistical Witness Indistinguishability from Batching

In this section, we prove that a sufficiently shrinking batch protocol for a relation can be used to construct an honest-verifier statistically witness-indistinguishable protocol for it with the same soundness properties. This is captured by the following theorem. In Section 3.2, we prove a related theorem that preserves non-interactivity and stronger notions of computational soundness, which is required for our results for non-interactive BARGs. Recall that for a relation $\mathcal{R}$ and polynomial t, the relation $\mathcal{R}^{\otimes t}$ denotes the product relation (as in Definition 2.8).

Theorem 3.1. *Consider an* NP *relation* $\mathcal{R}$*. Suppose it has a batch protocol* $\Pi = \langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ *that, when run on some polynomial* $t = t(\lambda)$ *instances of size* λ*, has compression rate* $\rho = \rho(\lambda) < 1$*. Then,* $\mathcal{R}$ *has a protocol* $\Pi_{\mathsf{WI}} = \langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ *with the following properties (on instances of size* λ*):*

- Π_{WI} *is* HVSWI *with error* $O\left(\sqrt{\rho}\right)$*.*
- Π_{WI} *has the same completeness error as* Π *run on* t *instances.*
- *If* Π *is statistically sound, then so is* Π_{WI}*, with the same soundness error as* Π *run on* t *instances.*
- *If* Π *is computationally sound, then so is* Π_{WI}*.*
- *If* P *is computed by a family of polynomial-sized circuits, then so is* P_{WI}*; and* V_{WI} *runs in uniform polynomial-time given blackbox access to* V*.*
- *The communication and round complexity in* Π_{WI} *are the same as those of* Π*, plus an additional message sent by* P_{WI} *at the start that is* $(\lambda \cdot t + \log t)$ *bits long.*

Fix some relation $\mathcal{R}$ for which there is a batch protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ with compression rate ρ as hypothesized. We will show how to construct from this a protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ for $\mathcal{R}$ that inherits its soundness properties and is, in addition, HVSWI. This protocol follows the template in Fig. 3.1, which is parameterized by an ensemble of distributions $\mathcal{D}$ and a function t, which we will instantiate later.

Given a batch protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$, a function $t : \mathbb{N} \to \mathbb{N}$, and an ensemble of distributions $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$, where the support of D_λ is contained in $(\{0,1\}^\lambda \times \{0,1\}^*)^{t(\lambda)}$, the protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle^{(\mathcal{D},t)}$ works as follows given an instance $x \in \{0,1\}^\lambda$ and a witness $w \in \{0,1\}^*$:

1. P_{WI} generates a sample $\{(x_i, w_i)\}_{i \in [t(\lambda)]}$ from D_λ, and samples $j \leftarrow [t(\lambda)]$
2. P_{WI} sends all the x_i's and j to V_{WI}
3. P_{WI} and V_{WI} run the protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ on the input $(x_1, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_{t(\lambda)})$, with P_{WI} using $(w_1, \ldots, w_{j-1}, w, w_{j+1}, \ldots, w_{t(\lambda)})$ as the witnesses
4. V_{WI} accepts iff the verifier V in the above execution accepts

Figure 3.1: Template for constructing HVSWI protocols from batch protocols

We next state lemmas capturing the properties of this protocol, and use them to prove Theorem 3.1. The proof of Lemma 3.2 is included below, and Lemma 3.3 is proven in Section 3.1.

Lemma 3.2 (Completeness and Soundness)**.** *Suppose $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is a batch protocol for a relation $\mathcal{R}$. Let t be any polynomial and $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$ be such that the support of D_λ is contained within $\mathcal{R}_\lambda^{\otimes t(\lambda)}$. Then, the protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ in Fig. 3.1, when instantiated with $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$, $\mathcal{D}$ and t, is a protocol for $\mathcal{R}$ that satisfies the following:*

1. *If $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ has completeness error $\delta(\lambda)$ when run with $t(\lambda)$ instances of size λ, then $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle^{(\mathcal{D},t)}$ has completeness error $\delta(\lambda)$.*
2. *If $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ has statistical soundness error $\epsilon(\lambda)$ when run with $t(\lambda)$ instances of size λ, then $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle^{(\mathcal{D},t)}$ has statistical soundness error $\epsilon(\lambda)$.*
3. *If $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is computationally sound, then $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle^{(\mathcal{D},t)}$ is also computationally sound.*

Proof. Fix any x such that $|x| = \lambda$, and denote $t(\lambda)$ by t. As all the (x_i, w_i)'s sampled from D_λ are contained in $\mathcal{R}$, the input $(x_1, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_t)$ is contained in $\mathcal{R}^{\otimes t}$ if and only if there is some w such that $(x, w) \in \mathcal{R}$. The completeness and statistical soundness errors of $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ thus carry over immediately to $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ as stated in the theorem.

For computational soundness, suppose there is a malicious prover $\mathsf{P}^*_{\mathsf{WI}}$ that can make V_{WI} accept with probability μ given an $x \notin \mathcal{R}$. Then, without loss of generality, there exists a $j \in [t]$ and $(x_1, \ldots, x_t)$ such that $\mathsf{P}^*_{\mathsf{WI}}$ can make V_{WI} accept with probability μ with the first message being $(x_1, \ldots, x_{j-1}, x, x_{j+1}, \ldots, x_t)$ and j. As V_{WI} is just emulating the verifier V, this means there is a P^* that emulates $\mathsf{P}^*_{\mathsf{WI}}$ and makes V accept on this input with probability μ. Further, if $\mathsf{P}^*_{\mathsf{WI}}$ is polynomial-time, so is P^*, as t is a polynomial. If $\mu(\lambda)$ is non-negligible, this breaks computational soundness of $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$, proving the theorem. □

Lemma 3.3 (Witness Indistinguishability)**.** *Consider a batch protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ for a relation $\mathcal{R}$ that has polynomial-sized witnesses. For a polynomial t, when the protocol is run with $t(\lambda)$ instances of size λ, suppose the total communication from the prover is at most $\rho(\lambda)t(\lambda)$ bits for some function ρ. Then, there is an efficiently sampleable ensemble of distributions $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$, where D_λ is supported in $\mathcal{R}_\lambda^{\otimes t(\lambda)}$, such that the protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ in Fig. 3.1, when instantiated with $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$, $\mathcal{D}$, and t, is HVSWI with error $O\left(\sqrt{\rho(\lambda)}\right)$.*

Using Lemmas 3.2 and 3.3 (the latter is proved in Section 3.1), we are ready to prove Theorem 3.1.

Proof of Theorem 3.1. Consider a relation $\mathcal{R}$ with polynomial-sized witnesses and a batch protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ that, for some polynomial t, when run on $t(\lambda)$ instances of size λ, has completeness error $\delta(\lambda)$, statistical soundness error $\epsilon(\lambda)$, and at most $\rho(\lambda)t(\lambda)$ bits of communication from the prover for some function ρ. Let $\mathcal{D}$ be the ensemble guaranteed by Lemma 3.3, and consider the protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ as described in Fig. 3.1 instantiated with this $\mathcal{D}$ and t. This protocol has the following properties:

- Lemma 3.3 implies that this protocol is HVSWI with WI error $O\left(\sqrt{\rho(\lambda)}\right)$.
- Lemma 3.2 implies that its completeness and statistical soundness errors are $\delta(\lambda)$ and $\epsilon(\lambda)$, respectively.
- Lemma 3.2 implies that if $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is computationally sound, then so is $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$.
- All V_{WI} does is run V on an input provided by P_{WI} and accept iff it accepts. P_{WI} also simply runs P on an input and witnesses, and in addition computes samples from D_λ and $[t(\lambda)]$, which can be done in non-uniform polynomial time since $\mathcal{D}$ is efficiently sampleable.
- In addition to the messages of $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$, the only additional communication in $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ is the initial prover message consisting of $t(\lambda)$ instances and an element of $[t(\lambda)]$.

The above arguments prove the respective properties of the protocol promised by the theorem. $\square$

3.1 Witness Indistinguishability

In this section, we prove Lemma 3.3 about the witness indistinguishability of the protocol from Fig. 3.1. We will first come up with an ensemble of distributions $\mathcal{D}$ that, when used to instantiate this protocol, will make the protocol witness-indistinguishable. Fix any batch protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ for a relation $\mathcal{R}$, an instance length λ, witness length m, and the number of batch instances t. Suppose that when $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is run on t instances of length λ, each with witness of length m, the total prover communication is at most ρt, where the compression rate ρ is less than 1.

Compressing Functions. We will use the fact that compressing functions necessarily lose information to make such a prover lose information about the witness we want to hide. This property of compression is captured by the following lemma by Dell, building on the work of Drucker [Dru15]. Similar consequences of compression have been used in the context of cryptography in the past, for instance to construct Oblivious Transfer from Private Information Retrieval protocols [DMO00, Lemma 1].

Lemma 3.4 ([Del16, Lemma 9])**.** *Let $t \in \mathbb{N}$, $\rho \in [0,1)$, and B be the uniform distribution over $\{0,1\}^t$. For any randomized mapping $f : \{0,1\}^t \to \{0,1\}^{\rho t}$, with $j \leftarrow [t]$, we have:*

$$\mathop{\mathbb{E}}_{j \leftarrow [t]} \left[\mathsf{SD}\left(f\left(B|_{j\leftarrow 0}\right), f\left(B|_{j\leftarrow 1}\right)\right)\right] \leqslant \sqrt{2\ln 2 \cdot \rho},$$

where $B|_{j\leftarrow b}$ is the result of drawing a sample $(b_1, \ldots, b_t) \leftarrow B$ and then replacing b_j with b.

We now define a function that captures the knowledge gained by the honest verifier by interacting with the honest prover in the protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$. Its input consists of t instances $x_1, \ldots, x_t \in \{0,1\}^\lambda$, potential witnesses $w_1, \ldots, w_t \in \{0,1\}^m$, and potential random string r of V. We use $\boldsymbol{x}$ to denote $(x_1, \ldots, x_t)$ for brevity.

$\underline{f((x_1, \ldots, x_t), (w_1, \ldots, w_t), r)}$:

1. Run $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ with input $(x_1, \ldots, x_t)$, using r as randomness for V, and with $(w_1, \ldots, w_t)$ as the witnesses provided to P
2. Output the sequence of prover messages in the above execution

In addition, for any pair of tuples of t potential witnesses $y_1, \ldots, y_t \in \{0,1\}^m$ and $z_1, \ldots, z_t \in \{0,1\}^m$, we define the following function on bits b_i.

$\underline{g_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},r}(b_1, \ldots, b_t)}$:

1. For each $i \in [t]$, set $w_i = y_i$ if $b_i = 0$, and $w_i = z_i$ if $b_i = 1$
2. Output $f(\boldsymbol{x}, \boldsymbol{w}, r)$

The proposition below follows immediately from Lemma 3.4 and the compression of the protocol.

Proposition 3.5. *For any tuple of $x_i \in \{0,1\}^\lambda$, $y_i, z_i \in \{0,1\}^m$, and any r of the appropriate length, letting B be the uniform distribution over $\{0,1\}^t$,*

$$\mathop{\mathbb{E}}_{j \leftarrow [t]} \left[\mathsf{SD}\left(g_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},r}\left(B|_{j\leftarrow 0}\right), g_{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},r}\left(B|_{j\leftarrow 1}\right)\right)\right] \leqslant \sqrt{2\ln 2 \cdot \rho}.$$

Interpreting the function g in terms of the function f then gives the following.

Proposition 3.6. *Consider any t-tuple of $x_i \in \{0,1\}^\lambda$, $y_i, z_i \in \{0,1\}^m$, and any r of the appropriate length. For $i \in [t]$, let W_i be set to y_i or z_i uniformly at random. Then,*

$$\mathop{\mathbb{E}}_{j \leftarrow [t]} \left[\mathsf{SD}\left(f\left(\boldsymbol{x}, \boldsymbol{W}|_{j\leftarrow y_j}, r\right), f\left(\boldsymbol{x}, \boldsymbol{W}|_{j\leftarrow z_j}, r\right)\right)\right] \leqslant \sqrt{2\ln 2 \cdot \rho}.$$

Two-Player Zero-Sum Games. Consider a two-player zero-sum game $G = (R, C, p)$, where R is the set of pure strategies for the "row" player, C the same for the "column" player, and $p : R \times C \to \mathbb{R}$ is the payoff function. Let ρ and κ denote mixed strategies for the two players, which are distributions over R and C, respectively. The *value* of this game is defined as:

$$val(G) = \min_\rho \max_\kappa \mathop{\mathbb{E}}_{\substack{r\leftarrow\rho \\ c\leftarrow\kappa}} \left[p(r,c)\right] = \max_\kappa \min_\rho \mathop{\mathbb{E}}_{\substack{r\leftarrow\rho \\ c\leftarrow\kappa}} \left[p(r,c)\right].$$

where the equality follows from von Neumann's minimax theorem [vN28]. Lipton and Young prove the following sparse minimax theorem that will be useful for us to infer sampleable mixed strategies.

Lemma 3.7 ([LY94])**.** *Consider any two-player zero-sum game $G = (R, C, p)$ such that $p(r, c) \in [0, 1]$ for any (r, c). For any $\epsilon > 0$, there is multiset $S \subseteq R$ of size $\Theta(\log |C|/\epsilon^2)$ such that for every $c \in C$:*

$$\mathop{\mathbb{E}}_{r\leftarrow S} \left[p(r,c)\right] \leqslant val(G) + \epsilon.$$

That is, there is a sparse mixed strategy that is almost as good as the optimal strategy over R. We will now define a game that captures the witness indistinguishability of the protocol described in Fig. 3.1, and use the above lemma to find a distribution $\mathcal{D}_\lambda$ with which to instantiate the protocol. Note that this is the first point in the proof where we involve the relation $\mathcal{R}$ that the protocols are for.

The game $G_W = (R, C, p)$ is defined with the following sets of pure strategies:

- $R = \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})\}$, where each vector is of length t, $x_i \in \{0,1\}^\lambda$, $y_i, z_i \in \{0,1\}^m$, and $(x_i, y_i), (x_i, z_i) \in \mathcal{R}$
- $C = \{(x, y, z)\}$, where $x \in \{0,1\}^\lambda$, $y, z \in \{0,1\}^m$, and $(x, y), (x, z) \in \mathcal{R}$

Given $r = (\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in R$, for each $i \in [t]$, define a random variable W_i that is set to y_i or z_i uniformly at random. The payoff function $p : R \times C \to [0,1]$ is then defined as follows, with r distributed uniformly over the appropriate domain:

$$p\left((\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}), (x, y, z)\right) = \mathop{\mathbb{E}}_{j \leftarrow [t], r}\left[\mathsf{SD}\left(f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow y}, r\right), f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow z}, r\right)\right)\right]$$

Proposition 3.8. *The value of the game G_W defined above is at most $\sqrt{2 \ln 2 \cdot \rho}$.*

Proof. It is sufficient to show that for any distribution (X, Y, Z) over C, there is a distribution $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$ over R such that the expected payoff under these strategies is at most the required bound. Given such a distribution (X, Y, Z), consider $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$ defined by $(x_i, y_i, z_i) \leftarrow (X, Y, Z)$ for $i \in [t]$. The expected payoff is then as follows, with each W_i set to y_i or z_i at random:

$$\mathop{\mathbb{E}}_{\substack{(x_1,y_1,z_1) \leftarrow (X,Y,Z) \\ \cdots \\ (x_t,y_t,z_t) \leftarrow (X,Y,Z)}} \mathop{\mathbb{E}}_{(x,y,z) \leftarrow (X,Y,Z)} \mathop{\mathbb{E}}_{j \leftarrow [t], r}\left[\mathsf{SD}\left(f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow y}, r\right), f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow z}, r\right)\right)\right].$$

Noting that r and j are sampled independently of all the other quantities[12], by linearity of expectation, the above is the same as:

$$\mathop{\mathbb{E}}_{j \leftarrow [t], r}\left[\mathop{\mathbb{E}}_{\substack{(x_1,y_1,z_1) \leftarrow (X,Y,Z) \\ \cdots \\ (x_t,y_t,z_t) \leftarrow (X,Y,Z)}} \mathop{\mathbb{E}}_{(x,y,z) \leftarrow (X,Y,Z)}\left[\mathsf{SD}\left(f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow y}, r\right), f\left(\boldsymbol{x}|_{j \leftarrow x}, \boldsymbol{W}|_{j \leftarrow z}, r\right)\right)\right]\right].$$

As (x, y, z) and (x_j, y_j, z_j) are identically distributed and are independent of all other variables, this is the same as:

$$\mathop{\mathbb{E}}_{j \leftarrow [t], r}\left[\mathop{\mathbb{E}}_{\substack{(x_1,y_1,z_1) \leftarrow (X,Y,Z) \\ \cdots \\ (x_t,y_t,z_t) \leftarrow (X,Y,Z)}}\left[\mathsf{SD}\left(f\left(\boldsymbol{x}, \boldsymbol{W}|_{j \leftarrow y_j}, r\right), f\left(\boldsymbol{x}, \boldsymbol{W}|_{j \leftarrow z_j}, r\right)\right)\right]\right].$$

By Proposition 3.6 and linearity of expectation, the above is at most $\sqrt{2 \ln 2 \cdot \rho}$, which proves the proposition. □

By Lemma 3.7 and Proposition 3.8, we have the following proposition.

Proposition 3.9. *For every $\epsilon > 0$, there is a multiset $S = \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})\}$ of size $\Theta((\lambda + m)/\epsilon^2)$ such that:*

- *for every $i \in [t]$, both (x_i, y_i) and (x_i, z_i) are in $\mathcal{R}$*

[12] This requirement of independence, specifically between r and x, is why this proof only provides honest-verifier SWI and does not work for a malicious verifier. The WI of our protocol could potentially be broken by a malicious verifier that chooses r based on x.

- *for every* $x \in \{0,1\}^\lambda$ *and* $y, z \in \{0,1\}^m$ *such that* $(x,y),(x,z) \in \mathcal{R}$,

$$\mathop{\mathbb{E}}_{\substack{(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\leftarrow S\\ w_i\leftarrow\{y_i,z_i\}\\ j\leftarrow[t],r}}\left[\mathsf{SD}\left(f\left(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow y},r\right),f\left(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow z},r\right)\right)\right] \leqslant \sqrt{2\ln 2\cdot\rho}+\epsilon.$$

Proof of Lemma 3.3. We can now describe the distribution D_λ that we will instantiate the protocol in Fig. 3.1 with. Recall that $\rho(\lambda)$ is the compression rate of the batch protocol we started with when run on $t(\lambda)$ instances of size λ.

Let S be the multiset guaranteed by Proposition 3.9 for $\epsilon = \sqrt{\rho(\lambda)}$. The distribution D_λ is sampled as follows:

1. Sample $(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) \leftarrow S$.
2. For each $i \in [t(\lambda)]$, set w_i to y_i or z_i uniformly at random.
3. Output $\{(x_i, w_i)\}_{i\in[t(\lambda)]}$.

As S is of size $\Theta((\lambda+m(\lambda))/\epsilon^2) = \Theta((\lambda+m(\lambda))/\rho(\lambda))$, which is polynomial in λ, the distribution D_λ can be sampled non-uniformly in $\mathsf{poly}(\lambda)$ time. In any element $(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})$ of S, we are guaranteed that each (x_i,y_i) and (x_i,z_i) is in $\mathcal{R}$. So the support of D_λ is contained in $\mathcal{R}_\lambda^{\otimes t(\lambda)}$, as required.

To argue HVSWI of the protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ when instantiated with this distribution, we need to show that for every possible pair $(x,y),(x,z) \in \mathcal{R}_\lambda$, the views of the verifier V_{WI} on input x when P_{WI} uses y or z as the witness are statistically close. Fix any such pair.

Note that for any $(\boldsymbol{x},\boldsymbol{w})$ sampled from D_λ, the view of V_{WI} on input x, when P uses witness w, is completely determined by the following quantities: $\boldsymbol{x}$, j, r, and $f(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow w},r)$ – all this is missing is the sequence of verifier messages in the protocol, which can be reconstructed efficiently given the verifier randomness r and the prover messages $f(\cdots)$. Thus, by the data processing inequality, the statistical distance between the views of V_{WI} in the cases where P_{WI} uses witness y or z is at most the following, where $(\boldsymbol{x},\boldsymbol{w}) \leftarrow D_\lambda$, $j \leftarrow [t(\lambda)]$, and r is over the appropriate domain:

$$\mathsf{SD}\left((\boldsymbol{x},j,r,f(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow y},r)),(\boldsymbol{x},j,r,f(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow z},r))\right).$$

Taking into account the definition of D_λ, this is equal to:

$$\mathop{\mathbb{E}}_{\substack{(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\leftarrow S\\ w_i\leftarrow\{y_i,z_i\}\\ j\leftarrow[t],r}}\left[\mathsf{SD}\left(f(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow y},r),f(\boldsymbol{x}|_{j\leftarrow x},\boldsymbol{w}|_{j\leftarrow z},r)\right)\right],$$

which, by Proposition 3.9, is at most $\sqrt{2\ln 2\cdot\rho(\lambda)}+\epsilon = O(\sqrt{\rho(\lambda)})$, proving the lemma. □

Remark 3.10. *The prover* P_{WI} *in protocol* $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ *we construct is non-uniform even if the prover* P *from the original batch protocol is uniform. This is because the minimax theorem we use (Lemma 3.7), while constructive, is not uniform. An interesting question here is whether a uniform version of the minimax theorem can be used instead to preserve uniformity of the prover. As far as we can tell, existing uniform minimax theorems ([VZ13], for instance) do not seem useful for this purpose. They require the payoff of the game to be efficiently computable given the strategies, which does not seem to be the case here as it involves computing the statistical distance between two rather arbitrary distributions.*

Remark 3.11. *The bound of* $O(\sqrt{\rho})$ *in the statements above (and particularly in Lemma 3.4) is optimal upto constant factors. In the case of Lemma 3.4, a function* g *that splits its input into blocks of size* $\Theta(1/\rho)$ *and outputs the majority of the bits in each block witnesses this optimality. This can then be extended to proof systems, where the bits may represent predicates that distinguish between two witnesses.*

3.2 Non-Interactive Protocols

In this section, we focus on non-interactive protocols. In Theorem 3.12 below, we prove the counterpart of Theorem 3.1 for non-interactive protocols. We also observe that if we only require a distributional notion of SWI, then we can avoid the non-uniformity of the prover in Theorem 3.12. We refer the readers to Definitions 2.17 and 2.18 for definitions pertaining to dual-mode non-interactive protocols.

Theorem 3.12. *Suppose an* NP *relation* $\mathcal{R}$ *has a non-interactive batch protocol* $\Pi = (\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *that, when run on some polynomial* $t = t(\lambda)$ *instances of size* λ*, has compression rate* $\rho = \rho(\lambda) < 1$*. Then,* $\mathcal{R}$ *has a dual-mode non-interactive protocol* $\Pi_{\mathsf{WI}} = (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$*, which is described in Fig. 3.2, with the following properties (on instances of size* λ*):*

- In statistically-hiding mode*,* Π_{WI} *is* SWI *with error* $O\left(\sqrt{\rho}\right)$*.*
- *Assume* Π *is CRS-indistinguishable. Then* Π_{WI}*, in both modes, has completeness error negligibly close to that of* Π *run on* t *instances. In addition,* Π_{WI} *is mode-indistinguishable.*
- *If* Π *is somewhere computationally sound, then* Π_{WI} in adaptively-sound mode *is adaptively computationally sound.*
- *If* P *is computed by a family of polynomial-sized circuits, then so is* P_{WI}*; and* V_{WI}*,* $\mathsf{SHGen}_{\mathsf{WI}}$*, and* $\mathsf{ASGen}_{\mathsf{WI}}$ *run in uniform polynomial-time given blackbox access to* V *and* TGen*, respectively.*
- *The length of the proof in* Π_{WI} *is that in* Π *plus an additional* $\lambda \cdot t$ *bits. The length of the CRS is that in* Π *plus an additional* $\log t$ *bits.*

Fix some relation $\mathcal{R}$ for which there is a non-interactive batch protocol $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ with compression rate ρ as hypothesized. We will show how to construct from this a dual-mode non-interactive SWI protocol $(\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ for $\mathcal{R}$ in a manner similar to that earlier in this section for general interactive protocols. This protocol follows the template in Fig. 3.2, which is parametrised by an ensemble of distributions $\mathcal{D}$ and a function t, which we will instantiate later.

Given a non-interactive batch protocol $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$, a function $t : \mathbb{N} \to \mathbb{N}$, and an ensemble of distributions $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$, where the support of D_λ is contained in $(\{0,1\}^\lambda \times \{0,1\}^*)^{t(\lambda)}$, the dual-mode non-interactive protocol $(\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ is as follows.

$\underline{\mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)}$:

- Sample $j, j' \leftarrow [t(\lambda)]$, and $crs \leftarrow \mathsf{TGen}(1^\lambda, 1^{t(\lambda)}, j')$.
- Output (j, crs).

$\underline{\mathsf{ASGen}_{\mathsf{WI}}(1^\lambda)}$:

- Sample $j \leftarrow [t(\lambda)]$, and $crs \leftarrow \mathsf{TGen}(1^\lambda, 1^{t(\lambda)}, j)$.
- Output (j, crs).

$\underline{\mathsf{P}_{\mathsf{WI}}((j, crs), x, w)}$:

- Sample $\{(x_i, w_i)\}_{i \in [t(\lambda)]}$ from D_λ.
- Compute $\pi \leftarrow \mathsf{P}(crs, (x_1, \dots, x_{j-1}, x, x_{j+1}, \dots, x_{t(\lambda)}), (w_1, \dots, w_{j-1}, w, w_{j+1}, \dots, w_{t(\lambda)}))$.
- Output $(\boldsymbol{x}, \pi)$.

$\underline{\mathsf{V}_{\mathsf{WI}}((j, crs), x, (\boldsymbol{x}, \pi))}$:

- Accepts iff $\mathsf{V}(crs, (x_1, \dots, x_{j-1}, x, x_{j+1}, \dots, x_{t(\lambda)}), \pi)$ accepts.

Figure 3.2: Template for constructing dual-mode NISWI protocols from non-interactive batch protocols

We next state lemmas capturing the properties of this protocol, and use them to prove Theorem 3.12.

Lemma 3.13 (Completeness and Mode Indistinguishability)**.** *Suppose* $\Pi = (\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *is a non-interactive batch protocol for a relation* $\mathcal{R}$*. Let* t *be any polynomial and* $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$ *be such that the support of* D_λ *is contained within* $\mathcal{R}_\lambda^{\otimes t(\lambda)}$*. Then, the protocol* $\Pi_{\mathsf{WI}} = (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ *in Fig. 3.2, when instantiated with* Π*,* $\mathcal{D}$ *and* t*, is a dual-mode non-interactive protocol for* $\mathcal{R}$ *that satisfies the following:*

- *If* Π *has completeness error* $\delta(\lambda)$ *when run with* $t(\lambda)$ *instances of size* λ *and is CRS-indistinguishable, then* Π_{WI} *has completeness error* $\delta(\lambda) + \mathrm{negl}(\lambda)$ *in both modes.*
- *If* Π *is CRS-indistinguishable, then* Π_{WI} *is mode-indistinguishable.*

Proof. We focus on the statistically-hiding mode, since completeness for the adaptively-sound mode will follow by mode indistinguishability (see Remark 2.20.2). Let $t = t(\lambda)$. If crs in $\mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)$ had been sampled from $\mathsf{Gen}(1^\lambda, 1^t)$ instead of $\mathsf{TGen}(1^\lambda, 1^t, j)$, then the completeness of Π_{WI} in this mode follows that of Π, with the same error $\delta(\lambda)$ (by the same arguments as in Lemma 3.2). By the CRS-indistinguishability of Π, and as both P_{WI} and V_{WI} are polynomial-time algorithms, making this change in $\mathsf{SHGen}_{\mathsf{WI}}$ can only change the completeness error by a negligible amount.

Mode indistinguishability follows directly from CRS indistinguishability.

□

Lemma 3.14 (Soundness)**.** *If* Π *is somewhere computationally sound, then* adaptively-sound mode *of* Π_{WI} *is adaptively computationally sound.*

Proof. Suppose there is a malicious prover $\mathsf{P}^*_{\mathsf{WI}}$ and a non-negligible function μ such that, with $crs_{\mathsf{WI}} \leftarrow \mathsf{ASGen}_{\mathsf{WI}}(1^\lambda)$ and $(x, \pi) \leftarrow \mathsf{P}^*_{\mathsf{WI}}(crs_{\mathsf{WI}})$ we have:

$$\Pr\left[x \notin \mathcal{L}(\mathcal{R}_\lambda) \wedge \mathsf{V}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, \pi) \text{ accepts}\right] \geqslant \mu(\lambda).$$

By the definition of the protocol, the above is the same as the following: with $j \leftarrow [t]$, $crs \leftarrow \mathsf{TGen}(1^\lambda, 1^t, j)$, $(x, \boldsymbol{x}, \pi) \leftarrow \mathsf{P}^*_{\mathsf{WI}}(j, crs)$,

$$\Pr\left[x \notin \mathcal{L}(\mathcal{R}_\lambda) \wedge \mathsf{V}(crs, \boldsymbol{x}|_{j \leftarrow x}, \pi) \text{ accepts}\right] \geqslant \mu(\lambda),$$

which immediately contradicts the somewhere computational soundness of $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ if μ is non-negligible. This proves the lemma. □

Lemma 3.15 (Witness Indistinguishability)**.** *Consider a non-interactive batch protocol* $\Pi = (\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *for a relation* $\mathcal{R}$ *that has polynomial-sized witnesses. For a polynomial* t*, when the protocol is run with* $t(\lambda)$ *instances of size* λ*, suppose the length of the proof is at most* $\rho(\lambda)t(\lambda)$ *bits for some function* ρ*. Then, there is an efficiently sampleable ensemble of distributions* $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$*, where* D_λ *is supported in* $\mathcal{R}_\lambda^{\otimes t(\lambda)}$*, such that the statistically-hiding mode of the protocol* Π_{WI} *in Fig. 3.2, when instantiated with* Π*,* $\mathcal{D}$*, and* t*, is* SWI *with error* $O\left(\sqrt{\rho(\lambda)}\right)$*.*

Proof Sketch. The proof of this lemma is identical to that of Lemma 3.3, with the only difference being that instead of the verifier's random string r, here we use the CRS sampled by $\mathsf{SHGen}_{\mathsf{WI}}$ (specifically, the crs part of (j, crs) that it samples). □

Remark 3.16. *Note that the adaptively-sound mode is not necessarily statistically hiding since the CRS generated depends on the index* j*. The proof of statistical hiding in Lemma 3.15 works out only when the CRS is generated as in* SHGen*, where the index* j *is independent of the* crs *sampled from* TGen*.*

Proof of Theorem 3.12. Consider a relation $\mathcal{R}$ with polynomial-sized witnesses and a non-interactive batch protocol $\Pi = (\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ that, for some polynomial t, when run on $t(\lambda)$ instances of size λ, has completeness error $\delta(\lambda)$, statistical soundness error $\epsilon(\lambda)$, and proofs of length at most $\rho(\lambda)t(\lambda)$ bits for some function ρ. Let $\mathcal{D}$ be the ensemble guaranteed by Lemma 3.15, and consider the protocol $\Pi_{\mathsf{WI}} = (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ as described in Fig. 3.2 instantiated with this $\mathcal{D}$ and t. This protocol has the following properties:

- Lemma 3.15 implies that this protocol *in statistically-hiding mode* is SWI with WI error $O\left(\sqrt{\rho(\lambda)}\right)$.
- Lemma 3.13 implies that its completeness error in both modes is $\delta(\lambda) + \mathrm{negl}(\lambda)$.
- By Lemma 3.14, if Π is somewhere computationally sound, then the *adaptively-sound* mode of Π_{WI} is adaptively computationally sound.
- All V_{WI} does is run V on an input provided by P_{WI} and accept iff it accepts. $\mathsf{SHGen}_{\mathsf{WI}}$ and $\mathsf{ASGen}_{\mathsf{WI}}$ similarly only sample from $[t(\lambda)]$ and run TGen once. P_{WI} also simply runs P on an input and witnesses, and in addition computes samples from D_λ and $[t(\lambda)]$, which can be done in non-uniform polynomial time since $\mathcal{D}$ is efficiently sampleable.
- In addition to the proof from Π, the proof in Π_{WI} consists only of the $t(\lambda)$ instances of length λ sampled by P_{WI}. And the CRS only has an additional element from $[t(\lambda)]$.

The above arguments prove the respective properties of the protocol promised by the theorem.

□

Dual-Mode NIDSWIA with uniform prover. Finally, we show that when the hiding requirement can be weakened to *distributional* SWI (Definition 2.15), it is possible to avoid the non-uniformity of prover in Theorem 3.12.

Theorem 3.17 (Dual-Mode NIDSWIA with *uniform* prover from NIBARG)**.** *Consider an* NP *relation* $\mathcal{R}$ *and let* $\mathcal{D}' = (D'_\lambda)_{\lambda\in\mathbb{N}}$ *be a distribution where* D'_λ *is supported over triples* (x, w^0, w^1) *such that* $(x, w^0), (x, w^1) \in \mathcal{R}_\lambda$. *Consider the distribution* $\mathcal{D} = (D_\lambda)_{\lambda\in\mathbb{N}}$, *where* D_λ *is supported over* $\mathcal{R}_\lambda$ *and defined via the following sampling procedure. On input* 1^λ,

1. *Sample* $(x, w^0, w^1) \leftarrow D'_\lambda$ *and* $b \leftarrow \{0, 1\}$
2. *Output* (x, w^b).

Let $\Pi = (\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *be a non-interactive batch protocol for* $\mathcal{R}$ *that, when run on some polynomial* $t = t(\lambda)$ *instances of size* λ, *has compression rate* $\rho = \rho(\lambda) < 1$. *Then, the dual-mode non-interactive protocol* $\Pi_{\mathsf{WI}} = (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ *from Fig. 3.2 instantiated with* Π *and* $\mathcal{D}^{\otimes t}$ *has the following properties (on instances of size* λ*):*

- *If* $\mathcal{D}'$ *is* uniformly *efficiently-sampleable, then the prover* P_{WI} *is* uniform*.*
- *In statistically-hiding mode,* Π_{WI} *is* distributional SWI *for* $\mathcal{D}'$ *with error* $O\left(\sqrt{\rho}\right)$.
- *Assume* Π *is CRS-indistinguishable. Then* Π_{WI}*, in both modes, has completeness error negligibly close to that of* Π *run on* t *instances. In addition,* Π_{WI} *is mode-indistinguishable.*
- *If* Π *is somewhere computationally sound, then* Π_{WI} *in adaptively-sound mode is adaptively computationally sound.*
- *The length of the proof in* Π_{WI} *is that in* Π *plus an additional* $\lambda \cdot t$ *bits. The length of the CRS is that in* Π *plus an additional* $\log t$ *bits.*

Proof Sketch. We focus on the first two claims since the rest of the claims can be proved as in Theorem 3.12. From the description of the sampling procedure, it is clear that if $\mathcal{D}'$ is *uniformly* efficiently sampleable then $\mathcal{D}$ also is, and as a result the prover P_{WI} is *uniform*. To prove the second claim, observe that

$$\begin{aligned}
\mathop{\mathbb{E}}_{(x,w^0,w^1)\leftarrow D'_\lambda}\left[\mathsf{SD}\left((crs_{\mathsf{WI}}, \pi^0), (crs_{\mathsf{WI}}, \pi^1)\right)\right] &= \mathop{\mathbb{E}}_{(x,w^0,w^1)\leftarrow D'_\lambda}\left[\mathop{\mathbb{E}}_{j\leftarrow[t], crs}\left[\mathsf{SD}\left(\pi^0, \pi^1\right)\right]\right] \\
&= \mathop{\mathbb{E}}_{(x,w^0,w^1)\leftarrow D'_\lambda}\left[\mathop{\mathbb{E}}_{\substack{(x_1,w_1)\leftarrow D_\lambda \\ \cdots \\ (x_t,w_t)\leftarrow D_\lambda}}\left[\mathop{\mathbb{E}}_{j\leftarrow[t], crs}\left[\mathsf{SD}\left(\pi^0, \pi^1\right)\right]\right]\right] \\
&= \mathop{\mathbb{E}}_{(x,w^0,w^1)\leftarrow D'_\lambda}\left[\mathop{\mathbb{E}}_{\substack{(x_1,w_1^0,w_1^1)\leftarrow D'_\lambda \\ \cdots \\ (x_t,w_t^0,w_t^1)\leftarrow D'_\lambda}}\left[\mathop{\mathbb{E}}_{\substack{j\leftarrow[t], crs \\ b_1,\cdots,b_t\leftarrow\{0,1\}^t}}\left[\mathsf{SD}\left(\pi^0, \pi^1\right)\right]\right]\right] \\
&\leqslant O(\sqrt{\rho}),
\end{aligned}$$

where

- $crs_{\mathsf{WI}} = (j, crs) \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)$ and $\pi^b \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, w^b)$ in the first equality;
- π^b is generated using P as described within P_{WI} in Fig. 3.2 in the second and third equalities;
- the third equality follows by the definition of $\mathcal{D}$; and
- the inequality follows from the proof of Proposition 3.8 with $f(\boldsymbol{x}, \boldsymbol{w}, r) := \mathsf{P}(r, \boldsymbol{x}, \boldsymbol{w})$ and column player's mixed strategy set to $\mathcal{D}'$.

$\square$

3.3 Corollaries

In this section we state some of the known results on transforming HVSWI protocols into SWI and SZK protocols against malicious verifiers. Starting from a public-coin HVSWI proof, Corollary 3.18 gives an SWI proof against malicious verifiers without any additional assumptions. Even if the original HVSWI proof is not public coin, we can use it to obtain an SWI proof under computational assumptions. This transformation is given by Corollary 3.19. Moving on to the setting of computational soundness, assuming OWFs exist, Corollary 3.19 shows that any HVSWI argument can be transformed into an SWI argument. Under the same assumption, Corollary 3.20 gives a transformation from an SWI argument to an SZK argument. Finally, Corollary 3.21 gives a similar transformation from an SWI argument to an SZK argument for non-interactive protocols; Corollary 3.22 is its distributional counterpart.

Corollary 3.18. *If there exists a public-coin* HVSWI *proof* Π *for an* NP *relation* $\mathcal{R}$ *then there exists a public-coin* SWI *proof* Π_M *for* $\mathcal{R}$ *with the following properties:*

- Π_M *has negligible completeness and soundness error.*
- Π_M *has* WI *error* $\mathsf{poly}(\lambda) \cdot \varepsilon + 2^{-\Theta(\lambda)}$ *where* λ *is the instance length and* ε *is* WI *error of* Π.
- *If* Π *has* d *rounds then* Π_M *has* $2d$ *rounds.*
- *If the honest prover in* Π *is non-uniform then so is the honest prover in* Π_M.

Proof Sketch. The proof is based on [Vad99, Theorem 6.3.5] which gives a transformation from any public-coin HVSZK proof to a public-coin SZK proof with the following properties:

- Π_M has negligible completeness error $2^{-\lambda}$ and soundness error $1/\lambda$.
- Π_M has ZK error $\mathsf{poly}(\lambda) \cdot \varepsilon + 2^{-\Theta(\lambda)}$ where λ is the instance length and ε is ZK error of Π.
- If Π has d rounds then Π_M has $2d$ rounds.
- If the honest prover in Π is non-uniform then so is the honest prover in Π_M.

We observe that the same transformation also transforms any HVSWI proof to an SWI proof with the same properties. To see that, recall that a protocol $\langle \mathsf{P} \leftrightarrows \mathsf{V} \rangle$ is SWI with error ε if and only if there exists an (unbounded) simulator S such that for every polynomial-size circuit family $\mathsf{V}^* = (\mathsf{V}^*_\lambda)_{\lambda \in \mathbb{N}}$,

$$\{\langle \mathsf{P}(w) \leftrightarrows \mathsf{V}^*_\lambda \rangle(x)\}_{\substack{(x,w)\in\mathcal{R} \\ |x|=\lambda}} \approx_\varepsilon \{\mathsf{S}(x, \mathsf{V}^*_\lambda)\}_{\substack{(x,w)\in\mathcal{R} \\ |x|=\lambda}} .$$

Similarly, the protocol is HVSWI if and only if the above is guaranteed for the honest verifier V. The proof of [Vad99, Theorem 6.3.5] uses the polynomial time simulator of the original SZK proof to construct a polynomial-time simulator for the new proof system. By inspecting the transformation and its analysis, we conclude that if the original protocol has an unbounded simulator instead of a polynomial-time one, the simulator constructed for the new proof system is also unbounded with the same error as in the efficient case.

The SWI proof resulting from the [Vad99] transformation has a non-negligible soundness error. To get an SWI proof with the claimed properties we can repeat the resulting SWI proof in parallel $\mathsf{poly}(\lambda)$ times. This reduces the soundness error to negligible and only increases the WI error by a factor of $\mathsf{poly}(\lambda)$. $\square$

Corollary 3.19. *Let* Π *be an* HVSWI *protocol for an* NP *relation* $\mathcal{R}$ *with* d *rounds.*

- *Assume there exists a statistically hiding commitment with* d^* *rounds. If* Π *is statistically sound then there exists an* SWI *proof for* $\mathcal{R}$ *with* $O(d \cdot d^*)$ *rounds and soundness error that is negligibly close to that of* Π.

Let Com be a two-message statistically binding commitment (with canonical decommitment). Let $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ be a constant-round computational ZK argument. Let $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ be a d-round HVSWI argument where verifier's randomness is of length ℓ. Assume WLOG that d is even.
The SWI argument $\langle \mathsf{P}_M \leftrightarrows \mathsf{V}_M \rangle$ is as follows. The prover and verifier are given an instance $x \in \{0,1\}^\lambda$. The prover is also given a witness $w \in \{0,1\}^*$.

1. P_M samples a first message k for Com and sends it to V_M
2. V_M samples $r_V \leftarrow \{0,1\}^\ell$ and a commitment $c \leftarrow \mathsf{Com}_k(r_V)$, and sends c to P_M
3. P_M samples $r_P \leftarrow \{0,1\}^\ell$ sends it to V_M
4. For $i = 1, \ldots, d$:
   (a) V_M computes the next message of V_{WI} using randomness $r = r_V \oplus r_P$:
   $$\alpha_i \leftarrow \mathsf{V}_{\mathsf{WI}}(x, \alpha_1, \beta_1, \ldots, \alpha_{i-1}, \beta_{i-1}; r) \ ,$$
   and sends α_i to P_M
   (b) V_M and P_M execute the protocol $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ where V_M proves to P_M that there exist strings $\tilde{r}_V$ and σ such that:
   $$c = \mathsf{Com}_k(\tilde{r}_V; \sigma) \ \wedge \ \alpha_i = \mathsf{V}_{\mathsf{WI}}(x, \alpha_1, \beta_1, \ldots, \alpha_{i-1}, \beta_{i-1}; \tilde{r}_V \oplus r_P)$$
   (c) If $\mathsf{V}_{\mathsf{CZK}}$ rejects then P_M aborts. Otherwise, P_M computes the next message of P_{WI}:
   $$\beta_i \leftarrow \mathsf{P}_{\mathsf{WI}}(x, w, \alpha_1, \beta_1, \ldots, \alpha_i) \ ,$$
   and sends β_i to V_M

Figure 3.3: Malicious-verifier SWI argument from an HVSWI argument and OWFs

- *Assuming OWFs exist, if Π is computationally sound then there exists an* SWI *argument for $\mathcal{R}$ with $O(d)$ rounds.*

The WI *error of the new protocol is negligibly close to that of Π. If the honest prover in Π is non-uniform then so is the honest prover in the new protocol.*

Statistically-hiding commitment be constructed in two rounds from CRHFs [DPP97, FS90a, HM96], in a constant number of rounds from multi-collision resistant hash functions [BDRV18, KNY18a] or distributional CRHFs [BHKY19], and in $O(\lambda)$ rounds from OWFs [HNO+09].

Proof Sketch. The proof is based on the compiler of [GMW86]. We start with the case of computational soundness and then explain how to modify the protocol to obtain statistical soundness. The verifier starts by committing to a random string r_V using a statistically-binding commitment and the prover responds with a random string r_P. Then the prover and verifier execute the HVSWI protocol where the verifier uses the randomness $r_V \oplus r_P$. After each message, the verifier proves using a computational ZK argument that the message was generated correctly. The SWI argument $\langle \mathsf{P}_M \leftrightarrows \mathsf{V}_M \rangle$ is described in Fig. 3.3. The construction uses a two-message statistically binding commitment and a constant-round computational ZK argument, both of which can be constructed from OWFs [Nao91, FS90a]. Next, we sketch the proof of soundness and SZK.

Computational soundness. Assume towards contradiction that there exists a polynomial-size cheating prover P^* that can prove a false statement with non-negligible probability ε. We use P^* to break the computational soundness of the HVSWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$. First we consider a hybrid experiment where we emulate an execution P^* with the verifier V_M, but each execution of the ZK argument $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ is simulated. By the zero-knowledge property of the ZK argument, P^* will continue to produce accepting proofs with probability that is negligibly close to ε. In the next hybrid, we modify the value in the initial commitment sent by V_M from r_V to 0^ℓ. By the computational hiding property of the commitment, P^* will continue to produce accepting proofs with probability that is negligibly close to ε. Now we can break the soundness of the HVSWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ by emulating this final hybrid experiment and forwarding the messages of the external verifier V_{WI} to P^* instead of computing them using the randomness $r = r_V \oplus r_P$. Since the string r is uniformly distributed, we convince the external verifier of a false statement with probability that is negligibly close to ε.

SWI. Fix any polynomial-size cheating verifier V^* and statement-witness pairs $(x, w_0), (x, w_1) \in \mathcal{R}$. Let ε denote the distance between the views $\mathsf{View}_0 = \langle \mathsf{P}_M(w_0) \leftrightarrows \mathsf{V}^* \rangle(x)$ and $\mathsf{View}_1 = \langle \mathsf{P}_M(w_1) \leftrightarrows \mathsf{V}^* \rangle(x)$. Since the commitment Com is statistically binding, we can fix the first commitment message k sampled by P_M such that Com_k is perfectly binding and the distance between View_0 and View_1 remains negligibly close to ε. Let $\tilde{r}_V$ be the string that V^* commits to in its first message.

For $b \in \{0,1\}$ we consider the view of the honest verifier V_{WI} in the interaction of $\langle \mathsf{P}_{\mathsf{WI}}(w_b) \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle(x)$ which consist of the verifier's randomness r and the prover's messages $(\beta_1, \ldots, \beta_d)$. We argue that given this view we can efficiently sample from a distribution that is negligibly close to View_b (with the first commitment message fixed to k). Therefore, it follows that ε must be negligibly close to the SWI error of the HVSWI argument.

Given the view $r, (\beta_1, \ldots, \beta_d)$ we sample from a distribution close to View_b as follows. We emulate the execution of V^*, setting the first prover message to k and the second prover message to $r_P = \tilde{r}_V \oplus r$. Since r is uniform, r_P is distributed exactly as in View_b. In every one of the remaining d rounds, starting from $i = 1$ to d we interact with V^* emulating the verifier of the ZK argument $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$. If the ZK argument is accepted then we set the next prover message to β_i, otherwise the prover aborts.

Let E be the event that the verifier V^* proves a true statement in each of the accepting executions of the ZK argument $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$. Conditioned on E, the view sampled above is distributed exactly the same as View_b. By the computational soundness property of the ZK argument, E occurs with all but negligible probability. Therefore, the sampled view is negligibly close to View_b.

An SWI proof. If the original SWI protocol $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ has statistical soundness we can modify the protocol $\langle \mathsf{P}_M \leftrightarrows \mathsf{V}_M \rangle$ described in Fig. 3.3 and obtain an SWI proof. We make the following modifications:

- We replace the two-message statistically-binding commitment with a statistically-hiding commitment.
- After the verifier sends the commitment c and before the prover sends r_P, have the verifier prove that it knows an opening of c using a SZK argument of knowledge where SZK holds even against an unbounded malicious verifier.[13] (We describe how this SZK argument of knowledge is constructed below.)
- Replace each invocation of the computational ZK argument with a SZK argument of knowledge against an unbounded malicious verifier.

Since the verifier's commitment and ZK arguments are all statistical, we can show statistical soundness following the same argument as in the computational case. To prove SWI, modify the above proof as follows. Since the commitment c is statistically-hiding, the string $\tilde{r}_V$ that V^* commits to is not well defined. Instead, we invoke the knowledge extractor of the SZK argument of knowledge and extract an opening to a string $\tilde{r}_V$. To prove SWI we need to show that, with all but negligible probability, all the messages $\beta_1, \ldots, \beta_d$ are computed according to the strategy of the honest verifier in the HVSWI argument V_{WI} using the randomness

[13] This is in contrast to the weaker notion of SZK in Definition 2.7 that only considers polynomial-size malicious verifiers.

$\tilde{r}_V \oplus r_P$. If this is not the case for some β_i, we can use the knowledge extractor of the SZK argument of knowledge and obtain an opening of the commitment c to a value other than r_V with non-negligible probability, contradicting the computational binding property of the commitment.

Using a statistically-hiding commitment with d^* rounds, a SZK argument of knowledge against an unbounded malicious verifier with $O(d^*)$ rounds can be constructed following the outline of [FLS90, GK96]: Start from an SWI argument of knowledge against an unbounded verifier in $O(d^*)$ rounds. Such a protocol can be obtained by taking the parallel repetition of the ZK protocol of [Blu81, GMW86] and instantiating the commitment scheme with the statistically hiding commitment. Next, the SWI argument of knowledge is transformed into an SZK argument of knowledge using the compiler of [FLS90]. In more details, the verifier starts by committing to trapdoor statement using a statistically hiding commitment and proving that the committed statement is true using a computational ZK proof of knowledge. Then the prover uses the SWI argument of knowledge to prove that either the original statement or the committed trapdoor statement is true. The required computational ZK proof of knowledge can be constructed by combining the computational ZK proof of [GK96] (instantiated with the statistically-hiding commitment) with a computational WI proof of knowledge (given by parallel repetition of the ZK protocol of [Blu81, GMW86], instantiated with a statistically binding commitment) via the [FLS90] compiler. □

Corollary 3.20. *Assuming one-way functions exist, if there exists an* SWI *argument* Π *for an* NP*-complete relation* $\mathcal{R}$ *with* d *rounds, then there exists an* SZK *argument* Π_{ZK} *for* $\mathcal{R}$ *with* $O(d)$ *rounds and ZK error that is negligibly close to the WI error of* Π*. If the honest prover in* Π *is non-uniform then so is the honest prover in* Π_{ZK}*.*

Proof Sketch. The proof is based on the compiler of [FLS90]. The verifier starts by sending a random image y of a length-doubling PRG and proving that it knows a corresponding preimage using a computational ZK argument of knowledge. Then, the prover and verifier execute the SWI protocol proving that either the original statement is true *or* that y is in the image of the PRG. In other words, the prover and verifier execute SWI protocol to prove that $(x, y) \in \mathcal{R}_{\mathrm{OR}}$, which is the relation obtained by "ORing" $\mathcal{R}$ and the relation defined by the PRG: i.e,

$$\mathcal{R}_{\mathrm{OR}} := \{((x, y), z) : (x, z) \in \mathcal{R} \vee \mathsf{PRG}(z) = y\} \tag{5}$$

The SZK argument $\langle \mathsf{P}_{\mathsf{ZK}} \leftrightarrows \mathsf{V}_{\mathsf{ZK}} \rangle$ is described in Fig. 3.4. The construction uses a PRG and a constant-round computational ZK argument of knowledge, both of which can be constructed from OWFs [HILL99, FS90a]. Next, we sketch the proof of soundness and SZK.

Soundness. Assume towards contradiction that there exists a polynomial-size cheating prover P^* that can prove a false statement with non-negligible probability ε. We use P^* to break the computational soundness of the SWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$. First we consider a hybrid experiment where we emulate an execution P^* with the verifier V_{ZK}, but the execution of the computational ZK argument $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ is simulated. By the zero-knowledge property of the ZK argument, P^* will continue to produce accepting proofs with probability that is negligibly close to ε. In the next hybrid, we sample a uniform $y \leftarrow \{0,1\}^{2\lambda}$ instead of sampling y as a random image of the PRG. By the pseudorandomness of the generator, P^* will continue to produce accepting proofs with probability that is negligibly close to ε. Now, the statement for the SWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ is false with probability $1 - 2^{-\lambda}$. Therefore, we can break the soundness of $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ with probability that is negligibly close to ε.

SZK. We describe a simulator S. The simulator is given an instance $x \in \mathcal{L}(\mathcal{R})$ and the description of a cheating verifier V^*. S emulates an interaction with V^*. If the verifier $\mathsf{V}_{\mathsf{CZK}}$ rejects in the execution of the computational ZK argument of knowledge $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ then S outputs the transcript of the interaction with V^* up to that point. Otherwise, S invokes the knowledge extractor of $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ on the description of the residual verifier V^* after sending its first message, right before the execution of $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$. If the extractor fails to output a string r such that $y = \mathsf{PRG}(r)$ then S aborts. Otherwise, S continues to emulate

Let $\mathsf{PRG} : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG. Let $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ be a constant-round computational ZK argument of knowledge. Let $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ be an SWI argument.
The SZK argument $\langle \mathsf{P}_{\mathsf{ZK}} \leftrightarrows \mathsf{V}_{\mathsf{ZK}} \rangle$ is as follows. The prover and verifier are given an instance $x \in \{0,1\}^\lambda$. The prover is also given a witness $w \in \{0,1\}^*$.

1. V_{ZK} samples a string $r \leftarrow \{0,1\}^\lambda$ and sends $y = \mathsf{PRG}(r)$ to P_{ZK}
2. V_{ZK} proves to P using $\langle \mathsf{P}_{\mathsf{CZK}} \leftrightarrows \mathsf{V}_{\mathsf{CZK}} \rangle$ that there exists a string $\tilde{r}$ such that $y = \mathsf{PRG}(\tilde{r})$
3. If $\mathsf{V}_{\mathsf{CZK}}$ rejects then P_{ZK} aborts. Otherwise, P_{ZK} proves to V_{ZK} using $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ that there exist strings $\tilde{w}$ and $\tilde{r}$ such that:
$$(x, \tilde{w}) \in \mathcal{R} \ \vee \ y = \mathsf{PRG}(\tilde{r}) \ ,$$
using the witness $\tilde{w} = w$ and $\tilde{r} = \perp$

Figure 3.4: SZK argument from an SWI argument and a PRG

an interaction with V^* by executing the honest prover of the SWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$ using the witness $\tilde{w} = \perp$ and $\tilde{r} = r$. Finally, S outputs the transcript of the entire interaction with V^*. Fix any $(x, w) \in \mathcal{R}$ and a polynomial-size cheating verifier V^*. Since the extractor runs in time that is inverse polynomial to the probability that the proof given by V^* is accepted, it follows that S runs in expected polynomial time. By the knowledge soundness property of the computational ZK argument of knowledge the extractor fails to find a witness and the simulation aborts only with negligible probability. Conditioned on the fact that S does not abort, the only difference between the simulated view generated by $\mathsf{S}(x, \mathsf{V}^*)$ and the real view $\langle \mathsf{P}_{\mathsf{ZK}}(w) \leftrightarrows \mathsf{V}^* \rangle(x)$ is the witness used by the honest prover in the execution of $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$. Therefore, the ZK error of the SWI argument $\langle \mathsf{P}_{\mathsf{ZK}} \leftrightarrows \mathsf{V}_{\mathsf{ZK}} \rangle$ is negligibly close to the WI error of the SWI argument $\langle \mathsf{P}_{\mathsf{WI}} \leftrightarrows \mathsf{V}_{\mathsf{WI}} \rangle$. □

Non-Interactive SZK. Finally, we describe the transformation for non-interactive protocols. To be specific, building on [FLS90], we transform a dual-mode (distributional) NISWIA to a dual-mode (distributional) NISZKA.

Corollary 3.21. *Assuming one-way functions exist, if there exists a dual-mode* NISWIA Π *for an* NP*-complete relation* $\mathcal{R}$*, then there exists a* dual-mode NISZKA Π_{ZK} *for* $\mathcal{R}$ *such that:*

- *In the statistically-hiding mode, the ZK error of* Π_{ZK} *is the same as the WI error of* Π*.*
- *If the honest prover in* Π *is non-uniform then so is the honest prover in* Π_{ZK} *(otherwise* Π_{ZK} *is uniform).*

We skip the proof of this corollary and prove below the more general corollary.

Corollary 3.22 (Dual-Mode NIDSZKA with *uniform* prover from NIDSWIA and OWF)**.** *Let* PRG *be a length-doubling PRG. Consider an* NP *relation* $\mathcal{R}$ *and let* $\mathcal{D} = (D_\lambda)_{\lambda \in \mathbb{N}}$ *be any* uniformly *efficiently-sampleable distribution such that* D_λ *is supported over* $\mathcal{R}_\lambda$*. Moreover, consider the relation* $\mathcal{R}_{\mathrm{OR}}$ *defined in Eq. (5), and the (uniformly) efficiently-sampleable distribution* $\mathcal{D}_{\mathrm{OR}} = (D_{\mathrm{OR},\lambda})_{\lambda \in \mathbb{N}}$ *on* $\mathcal{R}_{\mathrm{OR}}$*, where* $D_{\mathrm{OR},\lambda}$ *is defined via the following sampling procedure. On input* 1^λ*,*

1. *Sample* $(x, w) \leftarrow D_\lambda$*,*
2. *Sample* $s \leftarrow \{0,1\}^\lambda$ *and set* $y := \mathsf{PRG}(s)$*,*
3. *Output* $((x, y), w, s)$*.*

Let PRG be a length-doubling PRG. Let $\Pi_{\mathsf{WI}} := (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ be a dual-mode NISWIA for any NP-complete relation. The dual-mode NISZKA $\Pi_{\mathsf{ZK}} := (\mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{ASGen}_{\mathsf{ZK}}, \mathsf{P}_{\mathsf{ZK}}, \mathsf{V}_{\mathsf{ZK}})$ for any NP relation $\mathcal{R}$ is defined as follows.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^\lambda)}$

1. Sample a random element $y \in \{0,1\}^{2\lambda}$ from the *image* of PRG.
2. Set up Π_{WI} in statistically-hiding mode: $crs_{\mathsf{WI}} \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)$.
3. Output $crs_{\mathsf{ZK}} := (crs_{\mathsf{WI}}, y)$ as the CRS.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{ASGen}_{\mathsf{ZK}}(1^\lambda)}$

1. Sample a random element $y \in \{0,1\}^{2\lambda}$ from the *codomain* of PRG.
2. Set up Π_{WI} in adaptively-sound mode:: $crs_{\mathsf{WI}} \leftarrow \mathsf{ASGen}_{\mathsf{WI}}(1^\lambda)$.
3. Output $crs_{\mathsf{ZK}} := (crs_{\mathsf{WI}}, y)$ as the CRS.

$\underline{\pi \leftarrow \mathsf{P}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, x, w)}$

1. Use witness w to generate a proof that $(x, y) \in \mathcal{R}_{\mathrm{OR}}$ (see Eq. (5)): $\pi \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, (x, y), w)$.
2. Output π.

$\underline{b := \mathsf{V}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, x, \pi)}$

1. Accept $(b := 1)$ if and only if $\mathsf{V}_{\mathsf{WI}}(crs_{\mathsf{ZK}}, (x, y), \pi)$ accepts.

Figure 3.5: Π_{ZK}, a dual-mode NISZKA constructed from a dual-mode NISWIA and PRG.

If Π is a dual-mode $\mathsf{NIDSWIA}$ *for $\mathcal{D}_{\mathrm{OR}}$ then Π_{ZK}, defined in Fig. 3.5, is dual-mode* $\mathsf{NIDSZKA}$ *for $\mathcal{D}$ such that*

- *In the statistically-hiding mode, the ZK error of Π_{ZK} is the same as the WI error of Π.*
- *If the honest prover in Π is uniform then so is the honest prover in Π_{ZK}.*

Proof Sketch. Completeness follows readily; below we argue adaptive soundness and statistical ZK.

Adaptive soundness. Note that the y sampled as part of (crs_{WI}, y) in ASGen lies outside the image of PRG with overwhelming probability. As a result $(x, y) \notin \mathcal{R}_{\mathrm{OR}}$ implies that $x \notin \mathcal{R}$, and we end up reducing to adaptive soundness of Π (in adaptively-sound mode).

Distributional SZK. Recall the definitions of the distributions $\mathcal{D}$ and $\mathcal{D}_{\mathrm{OR}}$. With the simulator described in Fig. 3.6, we have

$$\begin{aligned}\mathop{\mathbb{E}}_{(x,w)\leftarrow D_\lambda}[\mathsf{SD}((crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}}), \mathsf{S}(x))] = \mathop{\mathbb{E}}_{(x,w)\leftarrow D_\lambda}[\mathsf{SD}((crs_{\mathsf{WI}}, y, \pi_w), (crs_{\mathsf{WI}}, y, \pi_s))] \leqslant \\ \mathop{\mathbb{E}}_{(x,w)\leftarrow D_\lambda}[\mathsf{SD}((crs_{\mathsf{WI}}, y, s, \pi_w), (crs_{\mathsf{WI}}, y, s, \pi_s))] = \\ \mathop{\mathbb{E}}_{((x,y),w,s)\leftarrow D_{\mathrm{OR},\lambda}}[\mathsf{SD}((crs_{\mathsf{WI}}, \pi_w), (crs_{\mathsf{WI}}, \pi_s))] \quad ,\end{aligned}$$

Let PRG and Π_{WI} be as in Fig. 3.5. The simulator for statistically-hiding mode of Π_{ZK} is described below.

$\underline{(crs_{\mathsf{ZK}}, \pi) \leftarrow \mathsf{S}_{\mathsf{ZK}}(x)}$

1. Sample a random image as follows: $y := \mathsf{PRG}(s)$, where $s \leftarrow \{0,1\}^\lambda$ is the trapdoor information.
2. Set up Π_{WI} in statistically-hiding mode: $crs_{\mathsf{WI}} \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)$.
3. Use the trapdoor information to generate proof that $(x, y) \in \mathcal{R}_{\mathrm{OR}}$: $\pi \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, s)$.
4. Output (crs_{ZK}, π), where $crs_{\mathsf{ZK}} := (crs_{\mathsf{WI}}, y)$.

Figure 3.6: S_{ZK}, a simulator for NISZKA from Fig. 3.5.

where in the first equation $crs_{\mathsf{WI}} \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^\lambda)$, $s \leftarrow \{0,1\}^\lambda$, $y = \mathsf{PRG}(s)$, $\pi_w \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, (x, y), w)$ and $\pi_s \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, (x, y), s)$.

$\square$

4 NISZKA from NIBARG and Dual-Mode Commitments

The WI and ZK errors for the protocols obtained in the previous section were only inverse-polynomially small. Moreover, the prover in those protocols was non-uniform. In this section, we remedy both these issues in the *non-interactive* setting. First, in Section 4.2, assuming *dual-mode commitments* (DMC), we show that any (dual-mode) NIDSZKA for some appropriate distribution, can be transformed to (dual-mode) *worst-case* NISZKA for any NP relation $\mathcal{R}$ with inverse-polynomial SZK error. Then, in Section 4.3, assuming DMC, we boost privacy to obtain (dual-mode) NISZKA for all of NP (formally we first obtain NISWIA and then apply Corollary 3.21). Both of the above transformations are uniform, and thus plugging-in our NIDSZKA from BARGs (see Corollary 3.22), we obtain uniform proof systems.

Remark 4.1 (On the Restriction to Non-interactive Setting)**.** *We note that both steps described above crucially rely on dual-mode commitments and are hence only interesting in the non-interactive setting. Indeed, since dual-mode commitments imply two-message statistically-hiding commitments, in the interactive setting they alone would allow the construction of constant-round statistical zero knowledge arguments with a uniform prover, negligible ZK error (and no reliance on* BARG*s).*

4.1 Dual-Mode Commitments

First, we define the notion of DMC [DN02].

Definition 4.2 (DMC)**.** *A* dual-mode commitment *scheme* Δ *is a four-tuple of polynomial-time algorithms* $(\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ *with following syntax:*

- $crs \leftarrow \mathsf{BGen}(1^\lambda)$. *The randomised* binding *CRS generation algorithm, on input a security parameter* $\lambda \in \mathbb{N}$, *outputs a CRS* $crs \in \{0,1\}^{\mathsf{poly}(\lambda)}$. *When using a CRS generated by* BGen, *we say that* Δ *is set up in* binding *mode.*
- $crs \leftarrow \mathsf{HGen}(1^\lambda)$. *The randomised* hiding *CRS generation algorithm, on input a security parameter* $\lambda \in \mathbb{N}$, *outputs a CRS* $crs \in \{0,1\}^{\mathsf{poly}(\lambda)}$. *When using a CRS generated by* HGen, *we say that* Δ *is set up in* hiding *mode.*
- $(c, d) \leftarrow \mathsf{Com}(crs, m)$. *The randomised* commitment *algorithm, on input a CRS* crs *and a message* $m \in \{0,1\}^{\mathsf{poly}(\lambda)}$, *outputs a commitment* $c \in \{0,1\}^{\mathsf{poly}(\lambda)}$ *and decommitment* $d \in \{0,1\}^{\mathsf{poly}(\lambda)}$.

- $b := \mathsf{VOpen}(crs, c, d, m)$. *The deterministic* verify opening *algorithm takes as input a commitment c, decommitment d and a message m. It outputs a bit b indicating accept or reject.*

We require the following properties from Δ:

1. Perfect correctness. *For every $\lambda \in \mathbb{N}, m \in \{0,1\}^{\mathsf{poly}(\lambda)}$, crs in the support of $\mathsf{BGen}(1^\lambda) \cup \mathsf{HGen}(1^\lambda)$, and (c, d) in the support of $\mathsf{Com}(crs, m)$,*

$$\mathsf{VOpen}(crs, c, d, m) = 1 \ .$$

2. Mode indistinguishability. *The binding and hiding modes are computationally indistinguishable. Formally, for every polynomial-size circuit family $\mathsf{A} = (\mathsf{A}_\lambda)_{\lambda\in\mathbb{N}}$, there is a negligible function μ, such that for all $\lambda \in \mathbb{N}$:*

$$\left| \Pr_{(crs,td)\leftarrow\mathsf{BGen}(1^\lambda)} [1 \leftarrow \mathsf{A}_\lambda(crs)] - \Pr_{crs\leftarrow\mathsf{HGen}(1^\lambda)} [1 \leftarrow \mathsf{A}_\lambda(crs)] \right| \leqslant \mu(\lambda).$$

3. Statistical indistinguishability in hiding mode. *In the hiding mode, for a random CRS, the distribution of commitments of any two messages must be* statistically *close. To be specific, for a function $\delta(\lambda)$, we say that Δ is* δ-statistically-indistinguishable *if*

$$(crs, c_0)_{\substack{m_0,m_1\in\{0,1\}^{\mathsf{poly}(\lambda)}\\ \lambda\in\mathbb{N}}} \approx_\delta (crs, c_1)_{\substack{m_0,m_1\in\{0,1\}^{\mathsf{poly}(\lambda)}\\ \lambda\in\mathbb{N}}}$$

where $crs \leftarrow \mathsf{HGen}(1^\lambda)$ and $(c_b, d_b) \leftarrow \mathsf{Com}(crs, m_b)$ for $b \in \{0,1\}$.

4. Almost-everywhere perfect binding in binding mode. *With overwhelming probability over the choice of binding CRS, we require that every possible commitment c opens to at most one message. Formally, there exists a negligible function μ such that for all $\lambda \in \mathbb{N}$*

$$\Pr_{crs\leftarrow\mathsf{BGen}(1^\lambda)} \left[\exists c, d, d', m \neq m' \in \{0,1\}^{\mathsf{poly}(\lambda)} \text{ s.t. } \mathsf{VOpen}^z(crs, c, d, m) = \mathsf{VOpen}^z(crs, c, d', m') = 1\right] \leqslant \mu(\lambda).$$

Remark 4.3 (On Definition 4.2)**.**

- *Using standard amplification (XOR Lemma), δ can be made as small as $2^{-\mathsf{poly}(\lambda)}$ for any* poly *at the cost of polynomially increasing the size of commitments (cf. [LM20]).*
- *Our definition allows for a general* VOpen *algorithm. Following common practice, we could restrict attention to canonical opening where the decommitment information is the randomness used in commitment (in which case correctness follows automatically). Nevertheless, using the more general* VOpen *syntax, will allow us to present the next Section 5.3 more smoothly. (Specifically, there we will consider an alternative to* DMC*, where canonical opening is not necessarily possible.)*
- *A related notion to* DMC *is* extractable dual-mode commitments *a.k.a* lossy encryption*. In this related notion, in the binding mode, one can also* efficiently extract (or decrypt) *the commitment using a trapdoor associated with the CRS. In contrast, the notion of* DMC *we use requires no such efficient extraction, and in particular does not necessitate public-key encryption. It can be constructed for instance from average-case hardness of the statistical difference problem with one-sided error*

4.2 Dual-Mode NISZKA from Dual-Mode NIDSZKA and DMC

In this section, we construct dual-mode NISZKA for the circuit satisfiability relation $\mathcal{C}$ given dual-mode NIDSZKA and DMC.

Local consistency relation $\mathcal{G}_g$

- *Hardwired.* Description of the DMC $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$, and a Boolean gate g.
- *Instance.* $(crs_\Delta, c_1, c_2, c_3)$, where crs_Δ is a CRS of Δ and c_i, $i \in [1, 3]$, are commitments.
- *Witness.* $((w_1, w_2, w_3), (d_1, d_2, d_3))$, where w_i and d_i, $i \in [1, 3]$, are wire values and decommitments.
- The relation holds if following conditions hold.
  1. *Commitments are valid*: $\mathsf{VOpen}(crs_\Delta, c_i, d_i, w_i) = 1$ for all $i \in [1, 3]$
  2. *Wire values are consistent*: $g(w_1, w_2) = w_3$

Distribution $\mathcal{D}_g = (D_{g,n})$ over $\mathcal{G}_g$, where $D_{g,n}$ is defined via following sampling procedure for input 1^n:

1. Sample a random hiding CRS: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$
2. Sample a random assignment (w_1, w_2, w_3) consistent with g, i.e., such that $g(w_1, w_2) = w_3$.
3. Generate a commitment and decommitment to each wire: for $i \in [3]$, $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, w_i)$.
4. Output $(crs_\Delta, c_1, c_2, c_3)$ as the instance and $((w_1, w_2, w_3), (d_1, d_2, d_3))$ as the witness.

Figure 4.1: $\mathcal{G}_g$, the relation capturing local consistency of wire values and $\mathcal{D}_g$, the distribution supported over $\mathcal{G}_g$.

Local consistency. Before presenting our construction, we define an NP relation $\mathcal{G}_g$ that captures *local consistency* of commitments to wires associated with a gate (Fig. 4.1), and a uniformly-sampleable distribution $\mathcal{D}_g = (D_{g,\lambda})_{\lambda \in \mathbb{N}}$ supported over $\mathcal{G}_g$. Looking ahead, for every Boolean gate g, we will require the underlying protocol to be $\mathsf{NIDSZKA}$ for $\mathcal{D}_g$. The following notation will also be useful.

Notation 4.4 (Notation for circuits.)**.** *Let C be a Boolean circuit with wires labeled by $[n]$. We use the same label for wires fanning out from the same gate or input bit. We say that an assignment $\boldsymbol{w} = (w_1, \cdots, w_n) \in \{0, 1\}^n$ satisfies a gate g with input wires i, j and output wire k if $g(w_i, w_j) = w_k$. An assignment $\boldsymbol{w}$ satisfies C if it satisfies all of its gates and the value of the output wire is 1. Thus, $\mathcal{C}_n$, the circuit satisfiability relation for circuits with n wires is defined as $(C, \boldsymbol{w})$ such that $\boldsymbol{w}$ satisfies C.*

Our protocol Π_{ZK} is described formally in Fig. 4.2. The construction is similar in spirit to [GOS12] in that the prover commits to the wire values and then, for each gate in the circuit, proves *local consistency* of the commitments to that gate's wires. The main difference is that we rely on dual-mode $\mathsf{NIDSZKA}$ instead of homomorphic proof commitments to prove local consistency.

Theorem 4.5 (Dual-Mode NISZKA from Dual-Mode $\mathsf{NIDSZKA}$ and DMC)**.** *Consider the non-interactive protocol Π_{ZK} for circuit satisfiability relation $\mathcal{C}$ described in Fig. 4.2, and instantiate:*

- *Π using a dual-mode $\mathsf{NIDSZKA}$ for $\mathcal{D}_g$ with ZK error ε; and*
- *Δ using any DMC that is δ-statistically-indistinguishable.*

Then Π_{ZK} is a dual-mode $4n(\delta + \varepsilon)$-NISZKA for $\mathcal{C}$, where n denotes the number of wires in the circuit. If Π has negligible (resp., 0) completeness error then so does Π_{ZK}.

Proof. Completeness follows readily. Mode indistinguishability of Π_{ZK} follows directly by mode indistinguishability of Δ and Π. We prove soundness and zero knowledge next.

For $n \in \mathbb{N}$, let $(C, \boldsymbol{w}) \in \mathcal{C}_n$ be an instance-witness pair of circuit satisfiability (see Notation 4.4). Let

- $\Pi = (\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}, \mathsf{V})$ be the base dual-mode NIDSZKA for $\mathcal{D}_g$ over $\mathcal{G}_g$ (Fig. 4.1); and
- $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ be an DMC.

The dual-mode (worst-case) NISZKA $\Pi_{\mathsf{ZK}} = (\mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{ASGen}_{\mathsf{ZK}}, \mathsf{P}_{\mathsf{ZK}}, \mathsf{V}_{\mathsf{ZK}})$ for $\mathcal{C}_n$ is described below.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^n)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. For each gate, set up Π in *statistically-hiding* mode: for $i \in [n]$, $crs_i \leftarrow \mathsf{SHGen}(1^n)$.
3. Output $crs_{\mathsf{ZK}} := (crs_\Delta, (crs_1, \ldots, crs_n))$ as the CRS.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{ASGen}_{\mathsf{ZK}}(1^n)}$

1. Set up Δ in *binding* mode: $crs_\Delta \leftarrow \mathsf{BGen}(1^n)$.
2. For each gate, set up Π in *adaptively-sound* mode: for $i \in [n]$, $crs_i \leftarrow \mathsf{ASGen}(1^n)$.
3. Output $crs_{\mathsf{ZK}} := (crs_\Delta, (crs_1, \ldots, crs_n))$ as the CRS.

$\underline{\pi_{\mathsf{ZK}} \leftarrow \mathsf{P}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, C, \boldsymbol{w})}$

1. Use Δ to commit to the value of each wire: for $i \in [n]$, generate $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, w_i)$. (Recall that wires fanning out from the same gate or input bit have the same label and hence a single commitment.)
2. For each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$, use $((w_i, w_j, w_k), (d_i, d_j, d_k))$ as witness to generate a proof π_g that $(crs_\Delta, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g)$:
$$\pi_g \leftarrow \mathsf{P}\left(crs_g, (crs_\Delta, c_i, c_j, c_k), ((w_i, w_j, w_k), (d_i, d_j, d_k))\right).$$
3. Output $\pi_{\mathsf{ZK}} := ((c_1, \cdots, c_n), (\pi_1, \cdots, \pi_{|C|}), d_n)$.

$\underline{b := \mathsf{V}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, C, \pi_{\mathsf{ZK}})}$

1. Output $b := 1$ (accept π_{ZK}) if and only if the checks below pass.
   (a) For each gate g in C, with input wires $i, j \in [n]$ and output wire $k \in [n]$, use π_g to verify that $(crs_\Delta, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g)$: i.e., $\mathsf{V}\left(crs_g, (crs_\Delta, c_i, c_j, c_k), \pi_g\right) = 1$.
   (b) Verify that C evaluates to 1, by ensuring that c_n opens to 1: $\mathsf{VOpen}(crs_\Delta, c_n, d_n, 1) = 1$.

Figure 4.2: Π_{ZK}, a dual-mode NISZKA for circuit satisfiability.

Let C, n, $\Pi = (\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}, \mathsf{V})$ and $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ be as defined in Fig. 4.2. Let S denote the simulator for Π. The simulator S_{ZK} for Π_{ZK} from Fig. 4.2 is described below.

$\underline{(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}}) \leftarrow \mathsf{S}_{\mathsf{ZK}}(C)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. Generate *dummy* commitments for each wire: for $i \in [n]$, $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, 1)$.
3. Simulate underlying views for all gates using S. That is, for each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$ generated simulated view that $(crs_\Delta, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g)$:
$$(crs_g, \pi_g) \leftarrow \mathsf{S}((crs_\Delta, c_i, c_j, c_k)).$$
4. Set $crs_{\mathsf{ZK}} := (crs_\Delta, (crs_1, \ldots, crs_n))$ and $\pi_{\mathsf{ZK}} := ((c_1, \cdots, c_n), (\pi_1, \cdots, \pi_{|C|}), d_n)$.
5. Output $(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}})$.

Figure 4.3: S_{ZK}, a simulator for Π_{ZK} (Fig. 4.2).

Adaptive Soundness. Note that in the adaptively-sound mode of Π_{ZK}, Δ is set up in the binding mode using BGen and all instances of Π are set up in adaptively-sound mode using ASGen. Since commitments generated in binding mode of Δ act as perfectly-binding commitments with overwhelming probability, we are able to show that adaptive soundness of Π implies adaptive soundness of Π_{ZK}, as explained next.

Assume for contradiction that $\mathsf{P}^* = (\mathsf{P}^*_n)_{n \in \mathbb{N}}$, a polynomial-sized family of malicious provers, breaks Π_{ZK}'s adaptive soundness with non-negligible probability. Given a challenge CRS crs^*, the reduction generates

$$crs^*_{\mathsf{ZK}} := (crs_\Delta, (crs_1, \ldots, crs_n)),$$

by sampling crs_Δ using BGen, setting $crs_{g^*} := crs^*$ for $g^* \leftarrow [n]$, and independently and randomly sampling the remaining CRSs using ASGen. The reduction then runs P^* on crs^*_{ZK}, which outputs $(C^*, \pi^*_{\mathsf{ZK}})$ such that C^* is unsatisfiable but $\pi^*_{\mathsf{ZK}} =: ((c^*_1, \cdots, c^*_n), (\pi^*_1, \cdots, \pi^*_{|C|}), d^*_n)$ is accepted by V_{ZK}. Since the commitments $(c^*_1, \cdots, c^*_n)$ are perfectly binding, they open to certain wire values $\boldsymbol{w}^* \in \{0,1\}^n$. Since C^* is unsatisfiable, there must exist a gate g in C^* with input wires $i, j \in [n]$ and output wire $k \in [n]$ such that $(crs_\Delta, c^*_i, c^*_j, c^*_k) \notin \mathcal{L}(\mathcal{G}_g)$, i.e., the commitments are locally *inconsistent* with respect to g (recall that $C(\boldsymbol{w}^*) = 1$ for a proof to be accepted). Since V_{ZK} accepts π^*_{ZK} if and only if V accepts all the underlying proofs and $g = g^*$ holds with probability $1/n$ (since g^* is sampled randomly and independently), the reduction can output $((crs_\Delta, c^*_i, c^*_j, c^*_k), \pi^*_{g^*})$ to break Π's adaptive soundness with a $1/n$ loss. Since this is non-negligible, we contradict the assumption that Π is adaptively sound with negligible error.

Statistical Zero Knowledge. Recall from Remark 2.20.1 that when referring to statistical ZK of a dual-mode NISZKA, we are implicitly referring to its statistically-hiding mode. The simulator for Π_{ZK} is formally described in Fig. 4.3, and to prove that

$$\mathsf{SD}(\langle \mathsf{P}_{\mathsf{ZK}}(\boldsymbol{w}) \to \mathsf{V}_{\mathsf{ZK}} \rangle(C), \mathsf{S}_{\mathsf{ZK}}(C)) \leqslant 4n(\delta + \varepsilon) \tag{6}$$

for any $(C, \boldsymbol{w}) \in \mathcal{C}_n$, where $\langle \mathsf{P}_{\mathsf{ZK}}(\boldsymbol{w}) \to \mathsf{V}_{\mathsf{ZK}} \rangle(C)$ denotes V_{ZK}'s view (in statistically-hiding mode), we proceed in two steps.

In the first step, we switch to an intermediate distribution H_{ZK}, described in Fig. 4.4, where all views (crs_g, π_g) of the underlying $\mathsf{NIDSZKA}$ Π are simulated but using *actual* commitments to $\boldsymbol{w}$. We claim that

For $n \in \mathbb{N}$, let $(C, \boldsymbol{w}) \in \mathcal{C}_n$. Let $\Pi = (\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}, \mathsf{V})$, $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ and S be as defined in Fig. 4.3. The hybrid distribution H_{ZK} for proof of Theorem 4.5 is described below.

$\underline{(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}}) \leftarrow H_{\mathsf{ZK}}(C, \boldsymbol{w})}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. Use Δ to commit to value of each wire: for $i \in [n]$, $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, w_i)$.
3. Simulate underlying views for all gates using S. That is, for each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$ generate a simulated view that $(crs_\Delta, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g)$:
$$(crs_g, \pi_g) \leftarrow \mathsf{S}(crs_\Delta, c_i, c_j, c_k).$$
4. Set $crs_{\mathsf{ZK}} := (crs_\Delta, (crs_1, \ldots, crs_n))$ and $\pi_{\mathsf{ZK}} := ((c_1, \cdots, c_n), (\pi_1, \cdots, \pi_{|C|}), d_n)$
5. Output $(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}})$

Figure 4.4: H_{ZK}, the intermediate hybrid distribution in proof of Theorem 4.5.

Π being distributionally SZK for $\mathcal{D}_g$ with error ε implies for all $(C, \boldsymbol{w})$ as above,
$$\mathsf{SD}(\langle \mathsf{P}_{\mathsf{ZK}}(\boldsymbol{w}) \to \mathsf{V}_{\mathsf{ZK}} \rangle(C), H_{\mathsf{ZK}}(C, \boldsymbol{w})) \leqslant 4|C|\varepsilon. \tag{7}$$
To argue this, we proceed via a hybrid argument consisting of $|C|$ steps, where in the ℓ-th hybrid $H_{\mathsf{ZK},\ell} = H_{\mathsf{ZK},\ell}(C, \boldsymbol{w})$, $\ell \in [0, |C|]$, the views corresponding to the first ℓ gates (say, according to topological order) are simulated using S. Hence $H_{\mathsf{ZK},0}$ corresponds to $\langle \mathsf{P}_{\mathsf{ZK}}(\boldsymbol{w}) \to \mathsf{V}_{\mathsf{ZK}} \rangle(C)$ and $H_{\mathsf{ZK},|C|}$ corresponds to the intermediate distribution H_{ZK}. We aim to prove that for every $\ell \in [1, |C|]$
$$\mathsf{SD}(H_{\mathsf{ZK},\ell-1}, H_{\mathsf{ZK},\ell}) \leqslant 4\varepsilon. \tag{8}$$
To this end, for the gate g that is switched from real to simulated in the ℓ-th hybrid, let us consider the "local distributions" R_g and S_g for g formally defined in Fig. 4.5.

In the following claim, we prove statistical indistinguishability of R_g and S_g assuming Π is ε-DSZK for $\mathcal{D}_g$. Note that the R_g and S_g are worst-case with respect to consistent assignments, and the crucial observation is that a worst-case to average-case reduction is possible since the number of consistent assignments for a Boolean gate is bounded.

Claim 4.6. *Fix a gate g. For any assignment $\boldsymbol{w} = (w_1, w_2, w_3) \in \{0,1\}^3$ consistent with g,*
$$\mathsf{SD}(R_g(1^n, \boldsymbol{w}), S_g(1^n, \boldsymbol{w})) \leqslant 4\varepsilon \ .$$

Proof. Since there are at most four consistent assignments, and $\mathcal{D}_g$ samples a uniformly random one, we have that for any consistent assignment $\boldsymbol{w}$,
$$\begin{aligned}
\frac{1}{4} \cdot \mathsf{SD}(R_g(1^n, \boldsymbol{w}), S_g(1^n, \boldsymbol{w})) &= \frac{1}{4} \cdot \mathop{\mathbb{E}}_{crs_\Delta, (\boldsymbol{c}, \boldsymbol{d})} [\mathsf{SD}((crs_g, \pi_g), \mathsf{S}(crs_\Delta, \boldsymbol{c}))] \\
&\leqslant \mathop{\mathbb{E}}_{\boldsymbol{w}'} \left[\mathop{\mathbb{E}}_{crs_\Delta, (\boldsymbol{c}', \boldsymbol{d}')} [\mathsf{SD}((crs_g, \pi'_g), \mathsf{S}(crs_\Delta, \boldsymbol{c}'))] \right] \qquad (9) \\
&= \mathop{\mathbb{E}}_{((crs_\Delta, \boldsymbol{c}'), (\boldsymbol{w}', \boldsymbol{d}')) \leftarrow \mathcal{D}_g(1^n)} [\mathsf{SD}((crs_g, \pi'_g), \mathsf{S}(crs_\Delta, \boldsymbol{c}'))] \\
&\leqslant \varepsilon, \qquad (10)
\end{aligned}$$
where

Let g denote the gate that is switched from real to simulated in hybrid ℓ, and let (w_i, w_j, w_k) denote its wire values. The distributions *local* to g in the $\ell-1$-th and ℓ-th hybrids are described below.

Real local distribution $R_g(1^n, w_i, w_j, w_k)$

1. Sample a random hiding CRS: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$
2. For $l \in \{i, j, k\}$, generate $(c_l, d_l) \leftarrow \mathsf{Com}(crs_\Delta, w_l)$
3. Sample $crs_g \leftarrow \mathsf{SHGen}(1^n)$ and $\pi_g \leftarrow \mathsf{P}\left(crs_g, (crs_\Delta, c_i, c_j, c_k), ((w_i, w_j, w_k), (d_i, d_j, d_k))\right)$
4. Output $(crs_\Delta, crs_g, \pi_g, (c_i, c_j, c_k), (d_i, d_j, d_k))$

Simulated local distribution $S_g(1^n, w_i, w_j, w_k)$

1. Sample a random hiding CRS: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$
2. For $l \in \{i, j, k\}$, generate $(c_l, d_l) \leftarrow \mathsf{Com}(crs_\Delta, w_l)$
3. Sample $(crs_g, \pi_g) \leftarrow \mathsf{S}\left(crs_\Delta, c_i, c_j, c_k\right)$
4. Output $(crs_\Delta, crs_g, \pi_g, (c_i, c_j, c_k), (d_i, d_j, d_k))$

Figure 4.5: R_g and S_g, the local distributions in the $\ell-1$-th and ℓ-th hybrids, respectively, in Claim 4.6.

- $crs_g \leftarrow \mathsf{SHGen}(1^n)$, $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, w_i)$ for $i \in [3]$, $\pi_g \leftarrow \mathsf{P}(crs_g, (crs_\Delta, \boldsymbol{c}), (\boldsymbol{w}, \boldsymbol{d}))$;
- the expectation in Eq. (9) is over random consistent wire values $\boldsymbol{w}' \in \{0,1\}^3$, and $(c'_i, d'_i) \leftarrow \mathsf{Com}(crs_\Delta, w'_i)$ for $i \in [3]$, $\pi'_g \leftarrow \mathsf{P}(crs_g, (crs_\Delta, \boldsymbol{c}'), (\boldsymbol{w}', \boldsymbol{d}'))$; and
- Eq. (10) follows from our assumption that Π is ε-DSZK for $\mathcal{D}_g$. $\square$

Since the views for the rest of the gates in $H_{\mathsf{ZK},\ell-1}$ and $H_{\mathsf{ZK},\ell}$ can be generated from the output $(crs_\Delta, crs_g, \pi_g, (c_i, c_j, c_k), (d_i, d_j, d_k))$ using the same random process, Claim 4.6 implies Eq. (8). By applying the triangle inequality to Eq. (8) with every $\ell \in [0, |C|]$, we get $\mathsf{SD}(H_{\mathsf{ZK},0}, H_{\mathsf{ZK},|C|}) \leqslant 4|C|\varepsilon$, completing the first step.

In the second step, all commitments (except that of the output wire) in H_{ZK} are switched to *dummy* commitments. The resulting distribution is the same as the output distribution of S_{ZK} (Fig. 4.3). Since Δ is used in hiding mode, this switch is $((n-1)\delta)$-statistically-indistinguishable by Δ's δ statistical hiding, i.e.:

$$\mathsf{SD}(H_{\mathsf{ZK}}(C, \boldsymbol{w}), \mathsf{S}_{\mathsf{ZK}}(C)) \leqslant (n-1)\delta. \tag{11}$$

Using the fact that $|C| \leqslant n$, Eq. (6) follows by applying the triangle inequality to Eqs. (7) and (11). $\square$

4.3 Privacy Amplification Using DMC and MPC

Finally, given a dual-mode NISZKA for any NP relation $\mathcal{R}$ with a sufficiently-small inverse-polynomial ZK error, we use DMC and semi-honest MPC to obtain a dual-mode NISWIA for $\mathcal{R}$ with *negligible* WI error. By Corollary 3.21, this (together with the fact that DMC implies OWF) implies dual-mode NISZKA for $\mathcal{R}$ with negligible ZK error.

We start with the definition of semi-honest MPC, following the convention from [IKOS07].

Definition 4.7 (Multi-Party Computation (MPC) [IKOS07]). *For $n \in \mathbb{N}$, an* MPC *protocol is a protocol involving n parties $P_1, \ldots, P_n$ that takes place in $\rho = \rho(n)$ rounds of communication. The public input is denoted by x, while the private input and random coins of P_i are denoted by $w_i \in \{0,1\}^{\mathsf{poly}(|x|)}$ and $r_i \in \{0,1\}^{\mathsf{poly}(|x|)}$, respectively. The protocol is specified by its next-message function*

$$(m_{i,j,k})_{j\in[n]} := M(i, x, w_i, r_i, ((m_{j,i,1})_{j\in[n]}, \ldots, (m_{j,i,k-1})_{j\in[n]})),$$

where, for $i \neq j \in [n]$ and $k \in [\rho]$, $m_{i,j,k}$ denotes the returns the message sent by P_i to P_j in round k. The view *of party P_i, denoted by $v_i = v_i(x, w_1, \ldots, w_n; r_1, \ldots r_n)$, consists of the private input and randomness, and the messages it receives over all rounds: i.e.,*

$$v_i := \left(w_i, r_i, (m_{j,i,k})_{j\in[n],k\in[\rho]}\right). \tag{12}$$

Two views v_i and v_j are said to be consistent *if the outgoing messages implicit in v_i are identical to the incoming messages in v_j and vice versa.*

Definition 4.8 (t-Perfectly-Secure MPC in the Semi-Honest Model [IKOS07]). *For $t \leqslant n \in \mathbb{N}$, an* MPC *protocol* M *realises an n-party functionality $f = f(x, w_1, \ldots, w_n)$ with* t-perfect-security in the semi-honest model *if the following properties hold:*

1. M realises f with perfect correctness. *That is, for any input $(x, w_1, \ldots, w_n)$, the probability (over the choice of $r_1, \ldots, r_n$) that the output of some player is different from the value of f is* 0.
2. M realises f with perfect t-privacy. *That is, there is a PPT simulator S_{M} such that for any inputs $x, w_1, \ldots, w_n$ and any set of corrupted players $\mathcal{C} \subseteq [n]$ with $|\mathcal{C}| < t$, the distribution of joint views of players in $\mathcal{C}$, denoted $V_{\mathcal{C}} = V_{\mathcal{C}}(x, w_1, \ldots, w_n)$, is* identical *to $\mathsf{S}_{\mathrm{M}}(\mathcal{C}, x, (w_i)_{i\in\mathcal{C}}, f_{\mathcal{C}}(x, w_1, \ldots, w_n))$. Here $f_{\mathcal{C}}(x, w_1, \ldots, w_n) := (f_i(x, w_1, \ldots, w_n))_{i\in\mathcal{C}}$ and f_i denotes the i-th output of f.*

In our constructions, we will need an MPC protocol to compute the following (Boolean) functionality based on an NP relation $\mathcal{R}$:

$$f_{\mathcal{R}}(x, w_1, \ldots, w_n) := \mathcal{R}(x, \oplus_{i=1}^{n} w_i). \tag{13}$$

Lemma 4.9 ([BGW88, AL17]). *Let $\mathcal{R}$ be any* NP *relation, and consider $f_{\mathcal{R}}(x, w_1, \ldots, w_n)$ defined in Eq. (13). There exists an $n/2$-perfectly-secure semi-honest* MPC *protocol for computing $f_{\mathcal{R}}$.*

Amplification Theorem. Our amplification protocol Π_{WI} is described formally in Fig. 4.6, followed by the amplification theorem in Theorem 4.10. The approach is similar in spirit to that in [GJS19] in the sense that the prover executes an MPC protocol "in its head" [IKOS07], commits to the view of each party in the execution and then proves consistency of each pair of views using the underlying proof system.

There are some key differences though:

1. We use DMC instead of a (plain) commitment scheme. DMC has two (indistinguishable) modes of operation: in the binding mode it act as a perfectly-binding commitment with overwhelming probability, whereas in the hiding mode it acts as a statistically-hiding commitment. Since we set it up in our protocol in hiding mode (see Fig. 4.6, Line 1), we are able to show amplification of privacy using statistical tools. In particular, we build on the approach from [LM20] based on statistical coupling [Ald83]. On the other hand, when arguing soundness we first switch the commitment to binding mode and exploit the fact that it acts as a perfectly-binding commitment. Thus, we are able to avoid the argument based on (computational) hardcore lemmas [Imp95, Hol05], which [GJS19] rely on.
2. We commit to the views as a whole (as in [IKOS07]) instead of the fine-grained way of committing in [GJS19]. In more detail, [GJS19] commit to the private inputs of parties, their private coins and each message in the transcript using separate commitments; we only commit to the view of each party as a whole.

3. Since we start from a dual-mode NISWIA with a negligible soundness error, MPC correctness in our protocol is guaranteed and therefore semi-honest privacy suffices. This is in contrast to [GJS19] who rely on malicious security to deal also with a soundness error of the underlying proof system.

Before stating and proving the theorem that Π_{WI} amplifies hiding, we define in Fig. 4.7 an NP relation $\mathcal{V}$, that captures *local consistency* of commitments to views.

Theorem 4.10 (Amplification Theorem)**.** *Let $\mathcal{R}$ be any* NP *relation. Consider the dual-mode non-interactive protocol Π_{WI} for $\mathcal{R}_n$ described in Fig. 4.6, and instantiate:*

1. M *using an $n/2$-perfectly-secure semi-honest* MPC *protocol for $f_{\mathcal{R}}$ (Eq. (13)).*

2. Π_{ZK} *using a dual-mode* NISZKA *for $\mathcal{V}$ with ZK error $\varepsilon = 1/100n$.*

3. Δ *using an* DMC *that is δ-statistically-indistinguishable.*

Then Π_{WI} is a dual-mode NISWIA *for $\mathcal{R}$ with following properties:*

- *If Π_{ZK} has negligible (resp., 0) completeness error then so does Π_{WI}.*
- *The soundness error is negligible in Δ's (computational) security parameter.*
- *The WI error is $2^{-n+1} + 2^{n+2}\delta n$. In particular, taking $\delta \leqslant 2^{-2n}/n$, the WI error is at most $O(2^{-n})$.*

As a corollary of Theorems 3.17, 4.5 and 4.10 and Corollaries 3.21 and 3.22, we get the main result of this section.

Corollary 4.11. *Let $\mathcal{R}$ be any* NP*-complete relation. Assuming* DMC*, a sufficiently-compressing somewhere-sound* NIBARG *for $\mathcal{R}$ implies a dual-mode* NISZKA *for $\mathcal{R}$.*

Proof Sketch. Completeness, mode indistinguishability and soundness follow readily. We focus on zero knowledge. Suppose that the NIBARG we start off with has a sufficiently small compression rate $\rho(\lambda) = O(1/\lambda^4)$, where λ is the security parameter. Recall the local consistency relation $\mathcal{G}_g$ and the corresponding distribution $\mathcal{D}_g$ (Fig. 4.1). By Theorem 3.17 and Corollary 3.22, NIBARG and OWF (which is implied by DMC) implies a dual-mode NIDSZKA for $\mathcal{D}_g$ with error $O(1/\lambda^2)$, as explained below.

1. By Theorem 3.17, the NIBARG implies a dual-mode NIDSWIA for any efficiently-sampleable distribution $\mathcal{D}' = (D'_\lambda)_{\lambda\in\mathbb{N}}$ with error $O(1/\lambda^2)$, where D'_λ is supported over triples (x, w_0, w_1) such that $(x, w_0), (x, w_1) \in \mathcal{R}_\lambda$.

2. Consider the "OR" relation $\mathcal{G}_{\mathrm{OR}}$ and distribution $\mathcal{D}_{g,\mathrm{OR}}$ defined analogous to Eq. (5) and Corollary 3.22. Thanks to the Karp reduction from $\mathcal{G}_g$ to $\mathcal{R}$, Line 1 also implies a dual-mode NIDSWIA for $\mathcal{D}_{g,\mathrm{OR}}$ with error $O(1/\lambda^2)$.

3. Finally, by Corollary 3.22, we get the claimed dual-mode NIDSZKA for $\mathcal{D}_g$ with error $O(1/\lambda^2)$.

Assuming that DMC is δ-statistically-indistinguishable for a negligible δ (see Remark 4.3), Theorem 4.5 now yields a dual-mode NISZKA for $\mathcal{R}$ with ZK error $O(1/\lambda)$ (where we invoke the Karp reduction from $\mathcal{R}$ to $\mathcal{C}$). Moreover, if δ is exponentially-small, say $2^{-2\lambda}/\lambda$, applying the amplification theorem in Theorem 4.10 to this dual-mode NISZKA, we get a dual-mode NISWIA for $\mathcal{R}$ with exponentially-small WI error. Finally, an application of Corollary 3.21 yields a dual-mode NISZKA for $\mathcal{R}$ with exponentially-small ZK error. By Remark 2.20.1, the ZK of this NISZKA in statistically-hiding mode can be made adaptive. □

Proof of Theorem 4.10. The fact that Π_{WI} is uniform if Π_{ZK} is follows by construction. Mode indistinguishability follows from mode indistinguishability of Δ and Π_{ZK}. We prove the rest of the properties in Propositions 4.12, 4.13 and 4.16.

Proposition 4.12 (Completeness)**.** *If Π_{ZK} has completeness error ε_c in statistically-hiding (resp., adaptively-sound) mode, then Π_{WI} has completeness error $n^2 \cdot \varepsilon_c$ in statistically-hiding (resp., adaptively-sound) mode.*

Let $\mathcal{R}$ be any NP relation and, for $n \in \mathbb{N}$, let $(x, w) \in \mathcal{R}_n$. Let

- $\Pi_{\mathsf{ZK}} = (\mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{ASGen}_{\mathsf{ZK}}, \mathsf{P}_{\mathsf{ZK}}, \mathsf{V}_{\mathsf{ZK}})$ be a base dual-mode ε-NISZKA for $\mathcal{V}$ (Fig. 4.7),
- $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ be an DMC; and
- M be an MPC protocol for $f_{\mathcal{R}}$.

The amplified dual-mode NISWIA $\Pi_{\mathsf{WI}} = (\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}_{\mathsf{WI}}, \mathsf{V}_{\mathsf{WI}})$ for $\mathcal{R}_n$ is described below.

$\underline{crs_{\mathsf{WI}} \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^n)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. For each pair of parties, set up Π_{ZK} in *statistically-hiding* mode: for $(i,j) \in \binom{[n]}{2}$, $crs_{i,j} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^n)$.
3. Output $crs_{\mathsf{WI}} := (crs_\Delta, crs_{1,2}, \ldots, crs_{n-1,n})$ as the CRS.

$\underline{crs_{\mathsf{WI}} \leftarrow \mathsf{ASGen}_{\mathsf{WI}}(1^n)}$

1. Set up Δ in *binding* mode: $crs_\Delta \leftarrow \mathsf{BGen}(1^n)$.
2. For each pair of parties, set up Π_{ZK} in *adaptively-sound* mode: for $(i,j) \in \binom{[n]}{2}$, $crs_{i,j} \leftarrow \mathsf{ASGen}_{\mathsf{ZK}}(1^n)$
3. Output $crs_{\mathsf{WI}} := (crs_\Delta, crs_{1,2}, \ldots, crs_{n-1,n})$ as the CRS.

$\underline{\pi_{\mathsf{WI}} \leftarrow \mathsf{P}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, w)}$

1. Execute M "in the head" for $f_{\mathcal{R}}$ (Eq. (13)) and use crs_Δ to *commit* to the views:
   (a) Generate shares $w_1, \ldots, w_n$ of the witness w: sample $w_1, \ldots, w_{n-1} \leftarrow \{0,1\}^{|w|}$ and then set $w_n := w \oplus w_1 \oplus \ldots \oplus w_{n-1}$.
   (b) Sample random coins $r_1, \ldots, r_n$ for the n parties $P_1, \ldots, P_n$.
   (c) Set x as the public input, w_i and r_i, respectively, as P_i's private input and random coins, and run M for $f_{\mathcal{R}}(x, w_1, \ldots, w_n)$. Let v_i denote P_i's view in the above execution.
   (d) Commit to the view of each party: for $i \in [n]$, set $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, v_i)$.
2. Prove pairwise local consistency: for all $(i,j) \in \binom{[n]}{2}$, use (v_i, d_i, v_j, d_j) as witness to generate a proof $\pi_{i,j}$ that $(c_i, c_j) \in \mathcal{L}(\mathcal{V}_{i,j})$
$$\pi_{i,j} \leftarrow \mathsf{P}_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), (v_i, d_i, v_j, d_j)).$$
3. Output $\pi_{\mathsf{WI}} := ((c_1, \ldots, c_n), (\pi_{1,2}, \ldots, \pi_{n-1,n}))$.

$\underline{b := \mathsf{V}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, \pi_{\mathsf{WI}})}$

1. Output $b := 1$ (accept π_{WI}) if and only if for each pair of parties $(i,j) \in \binom{[n]}{2}$, $\pi_{i,j}$ is a valid proof for $(c_i, c_j) \in \mathcal{L}(\mathcal{V}_{i,j})$, i.e., $\mathsf{V}_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), \pi_{i,j}) = 1$.

Figure 4.6: Π_{WI}, a dual mode NISWIA for any NP relation $\mathcal{R}$.

Local consistency relation $\mathcal{V}_{i,j}$ (for index $n \in \mathbb{N}$)

- *Hardwired.*
  1. Descriptions of a DMC scheme $\Delta = (\mathsf{BGen}, \mathsf{HGen}, \mathsf{Com}, \mathsf{VOpen})$ and MPC protocol M
  2. A CRS crs_Δ of Δ
  3. Indices $i, j \in [n]$ of parties.
- *Instance.* A pair of commitments (c_i, c_j)
- *Witness.* (v_i, d_i, v_j, d_j), where v_i and v_j are views, and d_i and d_j are decommitments.
- The relation holds if following conditions hold.
  1. *Commitments are valid*: $\mathsf{VOpen}(crs_\Delta, c_i, d_i, v_i) = 1$ and $\mathsf{VOpen}(crs_\Delta, c_j, d_j, v_j) = 1$
  2. Views v_i and v_j are consistent with respect to public input x and protocol M, and locally accepting (i.e., the local outputs are 1).

Figure 4.7: $\mathcal{V} := (\mathcal{V}_{i,j})_{(i,j)\in\binom{n}{2}}$, the relation capturing local consistency of views.

Proof Sketch. Let us focus on statistically-hiding mode – the proof for adaptively-sound mode is similar. Completeness of Π_{WI} in statistically-hiding mode reduces to completeness of Π_{ZK} in statistically-hiding mode thanks to the perfect correctness of M as we argue next. If $(x, w) \in \mathcal{R}$, then by correctness of M all pairs of views (v_i, v_j) are consistent and locally accepting. This implies that $((c_i, c_i), (v_i, d_i, v_j, d_j)) \in \mathcal{V}_{i,j}$ for every execution (i, j).[14] Since V_{WI} accepts if V_{ZK} accepts all the underlying proofs, and since the CRSs of Π_{ZK} are sampled independently, the correctness error is at most $(1 - (1 - \varepsilon_c)^{\binom{n}{2}}) \leqslant \varepsilon_c \cdot \binom{n}{2} \leqslant n^2 \cdot \varepsilon_c$. □

Proposition 4.13 (Adaptive Soundness Preserved)**.** *In adaptively-sound mode, Π_{WI} is adaptively sound with a negligible soundness error.*

Proof Sketch. We reduce from adaptive soundness of Π_{ZK}, the underlying NISZKA. Let $\mathsf{P}^* = (\mathsf{P}^*_n)_{n\in\mathbb{N}}$ be any polynomial-sized family of malicious provers that breaks Π_{WI}'s adaptive soundness with a non-negligible probability. Given a challenge CRS crs^*, the reduction generates

$$crs^*_{\mathsf{WI}} := (crs_\Delta, (crs_{1,2}, \ldots, crs_{n-1,n})),$$

where crs_Δ is a binding CRS of Δ sampled using BGen, $crs_{i^*,j^*} := crs^*$ for $(i^*, j^*) \leftarrow \binom{[n]}{2}$, and the remaining CRSs of Π_{ZK} are sampled independently using $\mathsf{ASGen}_{\mathsf{ZK}}$. The reduction runs P^* on crs^*_{WI}, which outputs $(x^*, \pi^*_{\mathsf{WI}})$ such that $x^* \notin \mathcal{L}(\mathcal{R})$ but $\pi^*_{\mathsf{WI}} =: ((c^*_1, \cdots, c^*_n), (\pi^*_{1,2}, \cdots, \pi^*_{n-1,n}))$ is accepted by V_{WI}. Recall that in binding mode, Δ act as perfectly-binding commitments with overwhelming probability. Therefore, the commitments $(c^*_1, \cdots, c^*_n)$ open to some views $(v^*_1, \cdots, v^*_n)$. Since $x^* \notin \mathcal{L}(\mathcal{R})$, there must exist at least one pair of views (v^*_i, v^*_j) such that $(c^*_i, c^*_j) \notin \mathcal{V}_{i,j}$, i.e., the views are *inconsistent* with respect to the public input, which is the instance x^*, or do not lead to output 1. Otherwise, if all pairs of views are consistent with respect to x^*, then by perfect correctness of M it can be argued that $x^* \in \mathcal{L}(\mathcal{R})$ (see [IKOS07, Lemma 2.3] about local vs. global consistency). Since V_{WI} accepts π^*_{WI} if and only if all the underlying proofs accept, and

[14]Note that we don't rely on correctness of decryption of Δ here and only use the fact that the encryption algorithm is a map once the random coins are fixed.

$(i,j) = (i^*, j^*)$ with probability at least $1/n^2$, the reduction can output $((c^*_{i^*}, c^*_{j^*}), \pi^*_{i^*,j^*})$ to break Π_{ZK}'s soundness with a $1/n^2$ loss, which is still non-negligible.[15]

$\square$

Before proving WI in Proposition 4.16, we establish some useful notation.

Notation 4.14 (Non-Standard String Notation)**.**

- *For a string or vector s of length n and a set $\mathcal{S} \subseteq [n]$, we use $s_{\mathcal{S}}$ to denote $(s_i)_{i \in \mathcal{S}}$.*
- *We let N denote $\binom{n}{2}$, and interpret a string $s \in \{0,1\}^N$ as $(s_{i,j})_{(i,j)\in\binom{[n]}{2}}$.*
- *By $\{0,1\}^N_{\geqslant T}$, we denote subset of strings in $\{0,1\}^N$ with Hamming weight* at least *T: i.e. $\{0,1\}^N_{\geqslant T} := \left\{s \in \{0,1\}^N : \|s\|_0 \geqslant T\right\}$.*

Notation 4.15 (Hybrid Distributions)**.**

- *We use $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle(x)$ to denote the random variable corresponding to V_{WI}'s view when the protocol in Fig. 4.6 is executed in* statistically-hiding *mode on $(x,w) \in \mathcal{R}$, i.e., $(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi})$, where $(crs_\Delta, \boldsymbol{crs}) \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^n)$ and $(\boldsymbol{c}, \boldsymbol{\pi}) \leftarrow \mathsf{P}_{\mathsf{WI}}((crs_\Delta, \boldsymbol{crs}), x, w)$.*
- *Similarly, $\langle \mathsf{P}_{\mathsf{ZK}}((v_i, d_i, v_j, d_j)) \to \mathsf{V}_{\mathsf{ZK}} \rangle(c_i, c_j)$ denotes the random variable corresponding to V_{ZK}'s views when the protocol Π_{ZK} is executed in statistically-hiding mode on $((c_i, c_j), (v_i, d_i, v_j, d_j)) \in \mathcal{V}_{i,j}$, i.e., $(crs_{i,j}, \pi_{i,j})$, where $crs_{i,j} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^n)$ and $\pi_{i,j} \leftarrow \mathsf{P}_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), (v_i, d_i, v_j, d_j))$.*
- *For $s \in \{0,1\}^N$, we use $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)$ to denote the hybrid distribution described in Fig. 4.8, where the views of V_{ZK} in executions (i,j) such that $s_{i,j} = 1$ are simulated using S_{ZK} (thus $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_{0^N}(x)$ corresponds to the real view). For a distribution S over $\{0,1\}^N$, $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_S(x)$ is defined as in Fig. 4.8, with s first sampled according to S.*

Proposition 4.16 (Privacy Amplified)**.** *Π_{WI} is HVSWI with an error $2^{-n+1} + 2^{n+2}\delta n$.*

Proof. The proof proceeds in two steps. We first prove in Claim 4.17 that, when set up in statistically-hiding mode, Π_{WI} is a combiner: if a large enough fraction of the NISZKA proofs are perfect ZK, then the resulting protocol is WI (with a negligible WI error). Then, taking a common approach in the literature, we prove in Claim 4.18 that any such combiner is also a good amplifier: provided that every NISZK has a small enough ZK error ε, the resulting protocol is WI (with a negligible WI error related to that of the corresponding combiner). Specifically, the proof of the latter claim follows the ideas developed in [LM20].

Claim 4.17 (Π_{WI} is a Threshold Combiner)**.** *For any $n \in \mathbb{N}$, $T := N - n/4 + 1$ and any $s \in \{0,1\}^N_{\geqslant T}$, $(x,w), (x,w') \in \mathcal{R}$,*

$$\mathsf{SD}(\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)), \langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)) \leqslant 2\delta n.$$

Claim 4.18 (Amplification from Threshold Combiners)**.** *For $T := N - n/4 + 1$ and any $(x,w), (x,w') \in \mathcal{R}$,*

$$\begin{aligned}&\mathsf{SD}(\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle(x), \langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle(x)) \leqslant \\ &2^{-n+1} + 2^{n+1} \cdot \max_{s \in \{0,1\}^N_{\geqslant T}} \mathsf{SD}(\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x), \langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)) \ .\end{aligned}$$

Proof of Claim 4.17. We proceed via a hybrid argument, and let $H_1 = H_{1,s}$ denote the distribution $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)$ from Fig. 4.8. Since $\|s\|_0 \geqslant T = N - n/4 + 1$ and as each proof depends on at most two parties, there exists a set $\mathcal{H} \subset [n]$ determined by s of size at least $n/2$ such that $s_{i,j} = 1$ holds for every $i \in \mathcal{H}$ and $j \in [n] \backslash \{i\}$. We think of these as the *honest* parties of the MPC protocol.

[15] This explains why we require Π_{ZK} to be adaptively sound (in the adaptively-sound mode) to start off with: the instance (c^*_i, c^*_j) and the associated proof $\pi^*_{i,j}$ that breaks Π_{ZK}'s soundness are determined by the output of the cheating prover P^*.

Let $n := |x|$ and $N := \binom{[n]}{2}$. For $s \in \{0,1\}^N$, the distribution $H_1 = H_{1,s}$ is defined below. For a distribution S over $\{0,1\}^N$, the hybrid distribution $\langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_S(x)$ is defined as $H_{1,s}$ with s first sampled according to S.

$\underline{(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi}) \leftarrow H_{1,s}(x,w)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. Generate the commitments $\boldsymbol{c}$ as specified in Fig. 4.6, Line 1. That is:
   (a) Run MPC as in Fig. 4.6, Lines 1a to 1c to generate views $(v_1, \ldots, v_n)$.
   (b) Compute the n-tuple of commitments $\boldsymbol{c}$, where $(c_i, d_i) \leftarrow \mathsf{Com}(crs_\Delta, v_i)$, as in Fig. 4.6, Line 1d.
3. Generate V_{ZK}'s views in Fig. 4.6, Line 2 depending on s. That is, sample $(\boldsymbol{crs}, \boldsymbol{\pi})$, where for $(i,j) \in \binom{[n]}{2}$
$$(crs_{i,j}, \pi_{i,j}) \leftarrow \begin{cases} \langle \mathsf{P}_{\mathsf{ZK}}((v_i, d_i, v_j, d_j)) \to \mathsf{V}_{\mathsf{ZK}} \rangle(c_i, c_j) & \text{if } s_{i,j} = 0 \\ \mathsf{S}_{\mathsf{ZK}}(c_i, c_j) & \text{otherwise.} \end{cases}$$
4. Output $(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi})$.

Figure 4.8: $H_1 = H_{1,s}$, a hybrid distribution used in proof of Proposition 4.16.

- In hybrid $H_2 = H_{2,s}$, we switch the messages underlying the commitments $c_{\mathcal{H}}$ from honestly-generated views $v_{\mathcal{H}}$ to a dummy message independent of the witness w: see Fig. 4.9. To see why $\mathsf{SD}(H_1, H_2) \leqslant \delta n$ (for any s), fix any $i \in \mathcal{H}$. Since the view $\langle \mathsf{P}_{\mathsf{ZK}}((v_i, d_i, v_j, d_j)) \to \mathsf{V}_{\mathsf{ZK}} \rangle(c_i, c_j)$ in every execution (i,j), $j \in [n] \backslash \{i\}$, is simulated, it follows that the decommitments d_i corresponding to the commitment c_i (which serve as part of witness for Π_{ZK}) are no longer required for generating proofs. Therefore, it is possible to use δ-statistical-indistinguishability of Δ to switch all commitments in $\mathcal{H}$ (of which there are at most n of).
- In the next hybrid $H_3 = H_{3,s}$, we simulate the joint views $v_{\overline{\mathcal{H}}}$ of the remaining parties using the MPC simulator $\mathsf{S}_{\mathsf{MPC}}$: see Fig. 4.10. The commitments and proofs that depend on $v_{\overline{\mathcal{H}}}$ are generated accordingly. Note that H_3 is distributed identically to H_2 thanks to $n/2$-privacy of M.

We get that $\mathsf{SD}(H_1, H_3) \leqslant \delta n$. By a symmetric argument to above it is possible to show that $\mathsf{SD}(H_3, \langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)) \leqslant \delta n$. The claim now follows by an application of the triangle inequality. □

Proof of Claim 4.18. For $s \in \{0,1\}^N$ and distribution S over $\{0,1\}^N$, recall the distributions $H_{1,s} = \langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)$ and $H_{1,S} = \langle \mathsf{P}_{\mathsf{WI}}(w) \to \mathsf{V}_{\mathsf{WI}} \rangle_S(x)$ defined in Fig. 4.8. Similarly, let $H'_{1,s}$ and $H'_{1,S}$ denote $\langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle_s(x)$ and $\langle \mathsf{P}_{\mathsf{WI}}(w') \to \mathsf{V}_{\mathsf{WI}} \rangle_S(x)$, respectively. Recall that our goal is to show that

$$\mathsf{SD}(H_{1,0^N}, H'_{1,0^N}) \leqslant 2^{-n+1} + 2^{n+1} \cdot \max_{s \in \{0,1\}^N_{\geqslant T}} \mathsf{SD}(H_{1,s}, H'_{1,s}) \ .$$

Let $n := |x|$ and $N := \binom{[n]}{2}$. For $s \in \{0,1\}^N$, the distribution $H_2 = H_{2,s}$ is defined below.

$\underline{(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi}) \leftarrow H_{2,s}(x, w)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. Generate the commitment $\boldsymbol{c}$ with dummy messages for the parties in $\mathcal{H}$. That is:
   (a) Run MPC as in Fig. 4.6, Lines 1a to 1c to generate views $(v_1, \ldots, v_n)$.
   (b) Compute the n-tuple of commitments $\boldsymbol{c}$ depending on h, where $h \in \{0,1\}^n$ denotes the indicator string for $\mathcal{H}$ determined by s:

$$(c_i, d_i) \leftarrow \begin{cases} \mathsf{Com}(crs_\Delta, v_i) & \text{if } h_i = 0 \\ \mathsf{Com}(crs_\Delta, 0^{|v_i|}) & \text{otherwise} \end{cases}$$

3. Generate $\mathsf{V_{ZK}}$'s views in Fig. 4.6, Line 2 depending on s. That is, sample $(\boldsymbol{crs}, \boldsymbol{\pi})$, where for $(i,j) \in \binom{[n]}{2}$

$$(crs_{i,j}, \pi_{i,j}) \leftarrow \begin{cases} \langle \mathsf{P_{ZK}}((v_i, d_i, v_j, d_j)) \to \mathsf{V_{ZK}} \rangle (c_i, c_j) & \text{if } s_{i,j} = 0 \\ \mathsf{S_{ZK}}(c_i, c_j) & \text{otherwise} \end{cases}$$

4. Output $(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi})$

Figure 4.9: $H_2 = H_{2,s}$, a hybrid distribution used in proof of Claim 4.17.

Let $n := |x|$ and $N := \binom{[n]}{2}$. For $s \in \{0,1\}^N$, the distribution $H_2 = H_{2,s}$ is defined below.

$\underline{(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi}) \leftarrow H_{3,s}(x, w)}$

1. Set up Δ in *hiding* mode: $crs_\Delta \leftarrow \mathsf{HGen}(1^n)$.
2. Generate the commitment $\boldsymbol{c}$ with dummy messages for the parties in $\mathcal{H}$ and simulated views for parties in $\overline{\mathcal{H}}$. That is:
   (a) Generate shares $w_1, \ldots, w_n$ of the witness w and use it to simulate the MPC (joint) views $v_{\overline{\mathcal{H}}} := \mathsf{S_{MPC}}(\overline{\mathcal{H}}, x, (w_i)_{i \in \overline{\mathcal{H}}}, (1, \ldots, 1))$
   (b) Compute the n-tuple of commitments $\boldsymbol{c}$ depending on h, where $h \in \{0,1\}^n$ denotes the indicator string for $\mathcal{H}$ determined by s:

$$(c_i, d_i) \leftarrow \begin{cases} \mathsf{Com}(crs_\Delta, v_i) & \text{if } h_i = 0 \\ \mathsf{Com}(crs_\Delta, 0^{|v_i|}) & \text{otherwise} \end{cases}$$

3. Generate $\mathsf{V_{ZK}}$'s views in Fig. 4.6, Line 2 depending on s. That is, sample $(\boldsymbol{crs}, \boldsymbol{\pi})$, where for $(i,j) \in \binom{[n]}{2}$

$$(crs_{i,j}, \pi_{i,j}) \leftarrow \begin{cases} \langle \mathsf{P_{ZK}}((v_i, d_i, v_j, d_j)) \to \mathsf{V_{ZK}} \rangle (c_i, c_j) & \text{if } s_{i,j} = 0 \\ \mathsf{S_{ZK}}(c_i, c_j) & \text{otherwise} \end{cases}$$

4. Output $(crs_\Delta, \boldsymbol{crs}, \boldsymbol{c}, \boldsymbol{\pi})$

Figure 4.10: $H_3 = H_{3,s}$, a hybrid distribution used in proof of Claim 4.17.

First, for any distributions Z over $\{0,1\}^N_{\geqslant T} \cup \{0^N\}$, we have

$$
\begin{aligned}
\mathsf{SD}(H_{1,Z}, H'_{1,Z}) &= \frac{1}{2}\sum_h \left|H_{1,Z}(h) - H'_{1,Z}(h)\right| \\
&= \frac{1}{2}\sum_h \left| \sum_{z\in\{0,1\}^N_{\geqslant T}\cup\{0^N\}} Z(z)(H_{1,z}(h) - H'_{1,z}(h)) \right| \\
&\geqslant \frac{1}{2}\sum_h \left(Z(0^N)\left|H_{1,0^N}(h) - H'_{1,0^N}(h)\right| - \sum_{z\in\{0,1\}^N_{\geqslant T}} Z(z)\left|H_{1,z}(h) - H'_{1,z}(h)\right| \right) \\
&= Z(0^N)\cdot \mathsf{SD}(H_{1,0^N}, H'_{1,0^N}) - \sum_{z\in\{0,1\}^N_{\geqslant T}} Z(z)\cdot \mathsf{SD}(H_{1,z}, H'_{1,z}) \\
&\geqslant Z(0^N)\cdot \mathsf{SD}(H_{1,0^N}, H'_{1,0^N}) - \max_{z\in\{0,1\}^N_{\geqslant T}} \mathsf{SD}(H_{1,z}, H'_{1,z}).
\end{aligned}
$$

Thus, for any distribution Z over $\{0,1\}^N_{\geqslant T} \cup \{0^N\}$ with $Z(0^N) > 0$, and distribution S over $\{0,1\}^N_{\geqslant T}$,

$$
\begin{aligned}
\mathsf{SD}(H_{1,0^N}, H'_{1,0^N}) &\leqslant Z(0^N)^{-1}\cdot(\mathsf{SD}(H_{1,Z}, H'_{1,Z}) + \max_{z\in\{0,1\}^N_{\geqslant T}} \mathsf{SD}(H_{1,z}, H'_{1,z})) \\
&\leqslant Z(0^N)^{-1}\cdot(\mathsf{SD}(H_{1,Z}, H_{1,S}) + \mathsf{SD}(H_{1,S}, H'_{1,S}) + \mathsf{SD}(H'_{1,S}, H'_{1,Z}) + \max_{z\in\{0,1\}^N_{\geqslant T}} \mathsf{SD}(H_{1,z}, H'_{1,z})) \\
&\leqslant Z(0^N)^{-1}\cdot(\mathsf{SD}(H_{1,Z}, H_{1,S}) + \mathsf{SD}(H'_{1,Z}, H'_{1,S})) + 2Z(0^N)^{-1}\cdot \max_{z\in\{0,1\}^N_{\geqslant T}} \mathsf{SD}(H_{1,z}, H'_{1,z})\ .
\end{aligned}
$$

To complete the proof, we use the following Lemma.

Lemma 4.19. *There exist two distributions Z and S, where Z is over $\{0,1\}^N_{\geqslant T} \cup \{0^N\}$, with $Z(0^N) > 2^{-n}$, and S is over $\{0,1\}^N_{\geqslant T}$, such that*

$$
Z(0^N)^{-1}\cdot \max\left\{\mathsf{SD}(H_{1,Z}, H_{1,S}), \mathsf{SD}(H'_{1,Z}, H'_{1,S})\right\} \leqslant \left(\frac{4eN}{n}\varepsilon\right)^{n/4}. \tag{14}
$$

Indeed, for our setting of parameters, i.e., $N = \binom{n}{2}$ and $\varepsilon = 1/100n$, the value of Eq. (14) is at most $1/2^n$.

The proof of Lemma 4.19 is based on a coupling argument and roughly follows [LM20]. The proof can be found in Appendix A. This concludes the proof of Claim 4.18. □

This concludes the proof of Proposition 4.16 □

This concludes the proof of Theorem 4.10. □

5 NICWIA from NIBARG and OWF

Recall that the main result in Section 4 was a construction of dual-mode NISZKA from NIBARG and dual-mode commitment (DMC) (Corollary 4.11). In this section, we show that we can replace the DMC in this construction with one-way functions (OWF) at the cost of relaxing statistical zero knowledge to *computational*. Toward this we follow a similar template to that in Section 4, with the main difference being that we use *computational instance-dependent commitments*, which are implied by OWFs, instead of DMC.

5.1 Instance-Dependent Primitives

We now define the notion of computational instance-dependent commitments, as well as corresponding notions of instance-dependent proofs.

Computational Instance-Dependent Commitment (CIDC). A CIDC scheme [FS90b] is associated with an NP relation $\mathcal{I}$. Its corresponding algorithms are parametrized by an instance z, which determines the security properties according to whether or not z is a member of $\mathcal{I}$. When $z \notin \mathcal{L}(\mathcal{I})$, a commitment c is statistically binding. In contrast, when $z \in \mathcal{L}(\mathcal{I})$, then given a witness y for z, there is a way to generate fake commitments $\widetilde{c}$ that are perfectly hiding. For any given message m, a real commitment c along with its decommitment information d are computationally indistinguishable from a fake commitment and decommitment $(\widetilde{c}, \widetilde{d})$ for m.[16] Our formal definition is in the common random string model and is given below.

Notation 5.1 (Instance-dependent schemes). *For an instance dependent scheme, we will use Π^z to denote both cases where the instance has been set to z and where the instance is unspecified (as a placeholder). The same applies to Π's constituent algorithms.*

Definition 5.2 (CIDC: Computational Instance-Dependent Commitment). *Let $\mathcal{I}$ be an* NP *relation. An* computational instance-dependent commitment *(CIDC) scheme for $\mathcal{I}$ is a five-tuple of polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Com}^z, \mathsf{VOpen}^z, \mathsf{SHCom}^{z,y})$, with the following syntax:*

- $crs \leftarrow \mathsf{Gen}(1^n)$. *The randomised set-up algorithm takes as input a security parameter $n \in \mathbb{N}$ and outputs a common random string $crs \in \{0,1\}^{\mathsf{poly}(n)}$.*

  The rest of the algorithms below take as input crs, and are parameterized by an instance $z \in \{0,1\}^n$ of $\mathcal{I}$, which is indicated in the superscript. The last algorithm is also parameterized by $y \in \{0,1\}^*$.

- $(c, d) \leftarrow \mathsf{Com}^z(crs, m)$. *The randomised (honest)* commitment *generation algorithm takes as input a message $m \in \{0,1\}^{\mathsf{poly}(n)}$. It outputs a commitment $c \in \{0,1\}^{\mathsf{poly}(n)}$ to m, along with decommitment information $d \in \{0,1\}^{\mathsf{poly}(n)}$.*

- $b := \mathsf{VOpen}^z(crs, c, d, m)$. *The deterministic* verify opening *algorithm takes as input a commitment $c \in \{0,1\}^{\mathsf{poly}(n)}$, decommitment $d \in \{0,1\}^{\mathsf{poly}(n)}$ and a message $m \in \{0,1\}^{\mathsf{poly}(n)}$. It outputs a bit b indicating accept or reject.*

- $(c, d) \leftarrow \mathsf{SHCom}^{z,y}(crs, m)$. *The randomised (fake)* commitment *generation algorithm takes as input a message $m \in \{0,1\}^{\mathsf{poly}(n)}$. It outputs a commitment $c \in \{0,1\}^{\mathsf{poly}(n)}$ to m, along with decommitment information $d \in \{0,1\}^{\mathsf{poly}(n)}$.*

We require the following properties:

1. Correctness of honestly-generated commitments. *For every $n \in \mathbb{N}$, $z \in \{0,1\}^n$ and $m \in \{0,1\}^{\mathsf{poly}(n)}$,*
$$\Pr_{\substack{crs \leftarrow \mathsf{Gen}(1^n) \\ (c,d) \leftarrow \mathsf{Com}^z(crs, m)}} \left[\mathsf{VOpen}^z(crs, c, d, m) = 1\right] = 1.$$

2. Almost-everywhere perfect binding depending on $z \notin \mathcal{L}(\mathcal{I})$. *With overwhelming probability over the choice of CRS, we require that for all $z \notin \mathcal{L}(\mathcal{I})$, every possible commitment c opens to at most one message. More formally, there exists a negligible function μ such that for all $n \in \mathbb{N}$*
$$\Pr_{crs \leftarrow \mathsf{Gen}(1^n)} \left[\begin{array}{l} \exists c \in \{0,1\}^{\mathsf{poly}(n)}\ \exists z \notin \mathcal{L}(\mathcal{I}_n)\ \exists d, d', m \neq m' \in \{0,1\}^{\mathsf{poly}(n)} \\ \quad \text{s.t. } \mathsf{VOpen}^z(crs, c, d, m) = \mathsf{VOpen}^z(crs, c, d', m') = 1 \end{array} \right] \leqslant \mu(n).$$

3. Perfect hiding of fake commitments with respect to $(z, y) \in \mathcal{I}$. *Formally,*
$$\left(crs, \mathsf{Com}^z(crs, m_0)\right)_{\substack{n \in \mathbb{N}, (z,y) \in \mathcal{I}_n \\ m_0, m_1 \in \{0,1\}^{\mathsf{poly}(n)}}} \equiv \left(crs, \mathsf{SHCom}^{z,y}(crs, m_1)\right)_{\substack{n \in \mathbb{N}, (z,y) \in \mathcal{I}_n \\ m_0, m_1 \in \{0,1\}^{\mathsf{poly}(n)}}},$$
   where $crs \leftarrow \mathsf{Gen}(1^n)$.

[16] We note that this notion of computational instance-dependent commitments should not be confused with the notion of (statistical) instance-dependent commitments of Ong and Vadhan [OV08], where when $z \in \mathcal{L}(\mathcal{I})$, real commitments (rather than fake ones) are statistically hiding. Indeed, this notion only exists for languages in SZK.

4. Indistinguishability of real and fake commitments with respect to $(z, y) \in \mathcal{I}$. *Formally,*

$$(crs, \mathsf{Com}^z(crs, m))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{I}_n\\ m\in\{0,1\}^{\mathsf{poly}(n)}}} \overset{c}{\approx} (crs, \mathsf{SHCom}^{z,y}(crs, m))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{I}_n\\ m\in\{0,1\}^{\mathsf{poly}(n)}}},$$

where $crs \leftarrow \mathsf{Gen}(1^n)$.

A construction of CIDC based on non-interactive commitments is described in [FS90b]. In the CRS model, where non-interactive commitments follow from one-way functions [Nao91], it too can be based on one-way functions.

Theorem 5.3 ([FS90b, Nao91])**.** *Assuming* OWF*s exist, there exists* CIDC *for any* NP *relation* $\mathcal{I}$.

Instance-Dependent ZK and WI. We next define the notions of instance-dependent (ID) NISZKA and NISWIA. An instance-dependent proof system for proving membership in $\mathcal{L}$ is associated with an additional NP relation $\mathcal{I}$. The system is parametrized by an instance z, which determines the security properties according to whether or not z is a member of $\mathcal{I}$, analogously to instance-dependent commitments. When $z \notin \mathcal{L}(\mathcal{I})$, the system is adaptively-sound. In contrast, when $z \in \mathcal{L}(\mathcal{I})$, then given a witness for z, there is a way to efficiently generate fake CRS and proof $\widetilde{crs}, \tilde{\pi}$ that are computationally indistinguishable from a real CRS and proof (crs, π). Moreover, the fake CRS and proof are statistically private (SZK or SWI), as a proof system for the language $\mathcal{L}$. This guarantee will allow us, in the analysis, to (computationally) switch to a world where we'll be able to invoke the statistical guarantees required for the amplification theorems from the previous section.

Definition 5.4 (ID-NISZKA and ID-NISWIA)**.** *Let* $\mathcal{R}$ *and* $\mathcal{I}$ *be* NP *relations. A non-interactive protocol* $\Pi := (\mathsf{ASGen}, \mathsf{P}^z, \mathsf{V}^z, \mathsf{SHGen}, \mathsf{SHP}^{z,y})$ *for* $\mathcal{R}$ *is a* ε-ID-NISZKA *(or* NISWIA*) for* $\mathcal{R}$ depending on $\mathcal{I}$ *if the following requirements are satisfied:*

1. *For any* $z \in \{0,1\}^*$*,* $(\mathsf{ASGen}, \mathsf{P}^z, \mathsf{V}^z)$ *has perfect completeness.*
2. *With respect to (adaptively-chosen) instances* $z \notin \mathcal{L}(\mathcal{I})$*,* $(\mathsf{ASGen}, \mathsf{P}^z, \mathsf{V}^z)$ *is* adaptively *computationally sound. Formally, for every polynomial-size circuit family of provers* $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda\in\mathbb{N}}$*, there is a negligible function* μ*, such that for all* $\lambda \in \mathbb{N}$*:*
$$\Pr_{crs\leftarrow\mathsf{ASGen}(1^\lambda)}[z \notin \mathcal{L}(\mathcal{I}) \wedge x \notin \mathcal{L}(\mathcal{R}_\lambda) \wedge \mathsf{V}^z(crs, x, \pi) = 1] \leqslant \mu(\lambda),$$
where $(z, x, \pi) := \mathsf{P}^*_\lambda(crs)$.
3. *With respect to (non-adaptively-chosen) instances* $z \in \mathcal{L}(\mathcal{I})$*,* $(\mathsf{SHGen}, \mathsf{SHP}^{z,y}, \mathsf{V}^z)$ *is* SZK *with error* ε*. Formally, there exists a PPT simulator* $\mathsf{S}^{z,y}$ *such that*
$$(crs, \mathsf{SHP}^{z,y}(crs, x, w))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{L}(\mathcal{I}_n)\\ (x,w)\in\mathcal{R}_n}} \approx_\varepsilon (\mathsf{S}^{z,y}(x))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{L}(\mathcal{I}_n)\\ (x,w)\in\mathcal{R}_n}}, \tag{15}$$
where $crs \leftarrow \mathsf{SHGen}(1^\lambda)$.
4. *With respect to (non-adaptively-chosen)* $(z, y) \in \mathcal{I}$*,* $(\mathsf{ASGen}, \mathsf{P}^z)$ *and* $(\mathsf{SHGen}, \mathsf{SHP}^{z,y})$ *are computationally indistinguishable. Formally,*
$$\left(crs, \mathsf{P}^z(crs, x, w) : crs \leftarrow \mathsf{ASGen}(1^\lambda)\right)_{\substack{n\in\mathbb{N},\\ (z,y)\in\mathcal{L}(\mathcal{I}_n),\\ (x,w)\in\mathcal{R}_n}} \overset{c}{\approx}_\varepsilon \left(crs, \mathsf{SHP}^{z,y}(crs, x, w) : crs \leftarrow \mathsf{SHGen}(1^\lambda)\right)_{\substack{n\in\mathbb{N},\\ (z,y)\in\mathcal{L}(\mathcal{I}_n),\\ (x,w)\in\mathcal{R}_n}}. \tag{16}$$

The definition of ε-ID-NISWIA *is obtained by replacing Condition 3 with following.*

3. *With respect to (non-adaptively-chosen) instances* $z \in \mathcal{L}(\mathcal{I})$*,* $(\mathsf{SHGen}, \mathsf{SHP}^{z,y}, \mathsf{V}^z)$ *is* SWI *with error* ε*. Formally,*
$$(crs, \mathsf{SHP}^{z,y}(crs, x, w_0))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{L}(\mathcal{I}_n)\\ (x,w_0),(x,w_1)\in\mathcal{R}_n}} \approx_\varepsilon (crs, \mathsf{SHP}^{z,y}(crs, x, w_1))_{\substack{n\in\mathbb{N},(z,y)\in\mathcal{L}(\mathcal{I}_n)\\ (x,w_0),(x,w_1)\in\mathcal{R}_n}} \tag{17}$$
where $crs \leftarrow \mathsf{SHGen}(1^\lambda)$.

5.2 ID-NISZKA from Dual-Mode NIDSZKA and CIDC

We construct an ID-NISZKA based on CIDC and dual-mode NIDSZKA that satisfies a natural *distribution-obliviousness* property, satisfied by the system constructed in Section 3. The property essentially says that the NIDSZKA for a given relation $\mathcal{G}$, only depends on the underlying distribution $\mathcal{D}$ on $\mathcal{G}$ as a black-box; namely, it only requires i.i.d. samples from $\mathcal{D}$.

Definition 5.5. *A non-interactive proof system with an oracle-aided prover* $(\mathsf{ASGen}, \mathsf{SHGen}, \mathsf{P}^{(\cdot)}, \mathsf{V})$ *for relation* $\mathcal{G}$ *is a dual-mode distribution-oblivious* ε-NIDSZKA *if for any sampler* $\mathcal{D}$ *supported on* $\mathcal{G}$, $(\mathsf{ASGen}, \mathsf{SHGen}, \mathsf{P}^{\mathcal{D}}, \mathsf{V})$ *is a dual-mode* ε-NIDSZKA *for* $\mathcal{D}$.

Claim 5.6. *The* ε-NIDSZKA *constructed in Section 3 is distribution oblivious.*

Proof Sketch. Recall that in the constructed NIDSWIA proof system, the prover simply plants its input and witness at random among polynomially many i.i.d. samples from the underlying distribution (and applies the BARG prover). The NIDSZKA for distribution $\mathcal{D}$ is constructed from a corresponding NIDSWIA for the corresponding FLS distribution $\mathcal{D}_{OR}$, where samples in $\mathcal{D}_{OR}$ are efficiently generated from samples in $\mathcal{D}$. □

The Construction. Consider the relation $\mathcal{G}_g$ (Fig. 4.1) naturally augmented to $\mathcal{G}_g^z$, described in Fig. 5.1. Let Π be a distribution-oblivious dual-mode ε-NIDSZKA for $\mathcal{G}_g^z$. We show that Π, along with CIDC, implies an $O(\varepsilon n)$-ID-NISZKA for the circuit satisfiability relation $\mathcal{C}$, where n is the circuit size. The protocol, Π_{ZK}, is described formally in Fig. 5.2.

Theorem 5.7 (ID-NISZKA from Distribution-Oblivious Dual-Mode NIDSZKA and CIDC)**.** *Let* $\mathcal{I}$ *be any* NP *relation. Consider the protocol* Π_{ZK} *described in Fig. 5.2, and instantiate:*

- Π *using a distribution-oblivious dual-mode* NIDSZKA *for* $\mathcal{G}_g^z$ *(Fig. 5.1), with SZK error* ε*; and*
- C *using a* CIDC *for* $\mathcal{I}$.

Then Π_{ZK} *is a* $4n\varepsilon$-ID-NISZKA *for* $\mathcal{C}$*, where* n *denotes the number of wires in the circuit. If* Π *has negligible (resp.,* 0*) completeness error then so does* Π_{ZK}.

Proof Sketch. Completeness follows that of the underlying NIDSZKA and the correctness of CIDC. We next prove soundness (for no instances), and zero knowledge and mode indistinguishability (for yes instances).

Adaptive Soundness when $z \notin \mathcal{L}(\mathcal{I})$. The proof is identical to that of adaptive soundness in Theorem 4.5, except that instead of relying on binding of DMC, it relies on CIDC's binding. Indeed, recall that with overwhelming probability over crs, the CRS sampled for CIDC, for any (adaptively chosen) $z \notin \mathcal{L}(\mathcal{I})$, Com^z is a perfectly binding commitment.

SZK with Respect to $z \in \mathcal{L}(\mathcal{I})$. Fix any $(z, y) \in \mathcal{I}$. Here we need to prove that $(\mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{SHP}^{z,y}_{\mathsf{ZK}}, \mathsf{V}^z_{\mathsf{ZK}})$ is $4n\varepsilon$-SZK. The proof is identical to that of $4n(\varepsilon + \delta)$-SZK in Theorem 4.5, except that:

- Instead of relying on the δ-statistical hiding of DMC, we rely on the perfect statistical hiding of $\mathsf{SHCom}^{z,y}$ (corresponding to $\delta = 0$).
- Accordingly, we rely on the ε-SZK of the NIDSZKA $(\mathsf{SHGen}, \mathsf{P}^{\widehat{D}^{z,y}_{g,n}}, \mathsf{V})$ for the distribution $\widehat{D}^{z,y}_{g,n}$ over the relation $\mathcal{G}_g^z$.

Indistinguishability of Real and Fake Proofs. Here we need to prove that for $(z, y) \in \mathcal{I}$, $(x, w) \in \mathcal{R}$, a real CRS and proof $(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}})$ generated by $\mathsf{ASGen}_{\mathsf{ZK}}(1^n)$ and $\mathsf{P}^z(crs_{\mathsf{ZK}}, x, w)$ are computationally indistinguishable from ones generated by $\mathsf{SHGen}_{\mathsf{ZK}}(1^n)$ and $\mathsf{SHP}^{z,y}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, x, w)$. There are two differences between the two distributions:

Local consistency relation $\mathcal{G}_g^z$ (for index $n \in \mathbb{N}$)

- *Hardwired.*
  1. Description of a relation $\mathcal{R}$ and an instance $z \in \{0,1\}^n$
  2. Description of CIDC algorithms $\mathrm{C} = (\mathsf{Gen}, \mathsf{Com}^z, \mathsf{VOpen}^z, \mathsf{SHCom}^{z,y})$.
  3. A Boolean gate g
- *Instance.* (crs, c_1, c_2, c_3), where crs is a CRS of C and c_i, $i \in [1,3]$, are commitments.
- *Witness.* $((w_1, w_2, w_3), (d_1, d_2, d_3))$, where w_i and d_i, $i \in [1,3]$, are wire values and decommitments.
- The relation holds if following conditions hold.
  1. *Commitments are consistent*: $\mathsf{VOpen}^z(crs, c_i, d_i, w_i) = 1$ for all $i \in [1,3]$
  2. *Wire values are consistent*: $g(w_1, w_2) = w_3$

Distribution $\mathcal{D}_g^z = \left(D_{g,n}^z\right)$ over $\mathcal{G}_g^z$, where $D_{g,n}^z$ is defined via following sampling procedure for input 1^n:

1. Sample a CRS: $crs \leftarrow \mathsf{Gen}(1^\lambda)$
2. Sample a random assignment (w_1, w_2, w_3) consistent with g, i.e., such that $g(w_1, w_2) = w_3$.
3. For $i \in [3]$: generate commitment $(c_i, d_i) \leftarrow \mathsf{Com}^z(crs, w_i)$ to w_i.
4. Output (crs, c_1, c_2, c_3) as the instance and $((w_1, w_2, w_3), (d_1, d_2, d_3))$ as the witness.

Distribution $\widehat{\mathcal{D}}_g^{z,y} = \left(\widehat{D}_{g,n}^{z,y}\right)$ over $\mathcal{G}_g^z$, where $\widehat{D}_{g,n}^{z,y}$ is defined similarly to D_g^z except for item 3:

3. For $i \in [3]$: generate fake commitment $(c_i, d_i) \leftarrow \mathsf{SHCom}^{z,y}(crs, w_i)$ to w_i.

Figure 5.1: $\mathcal{G}_g^z$, the relation capturing local consistency of wire values. $\mathcal{D}_g^z$, the distribution supported over $\mathcal{G}_g^z$ used in the real proof. $\mathcal{D}_g^{z,y}$, the distribution supported over $\mathcal{G}_g^z$ used in the analysis.

For $n \in \mathbb{N}$, let $(C, \boldsymbol{w}) \in \mathcal{C}_n$ be an instance-witness pair of circuit satisfiability (see Notation 4.4). Let

- $\mathcal{I}$ be any NP relation, and $z \in \{0,1\}^n$;
- $\Pi = (\mathsf{SHGen}, \mathsf{ASGen}, \mathsf{P}^{(\cdot)}, \mathsf{V})$ be the distribution-oblivious dual-mode NIDSZKA for $\mathcal{G}_g^z$ (Fig. 5.1);
- $\mathrm{C} = (\mathsf{Gen}, \mathsf{Com}^z, \mathsf{VOpen}^z, \mathsf{SHCom}^{z,y})$ be a CIDC for $\mathcal{I}$.

The ID-NISZKA $\Pi_{\mathsf{ZK}} = (\mathsf{ASGen}_{\mathsf{ZK}}, \mathsf{P}^z_{\mathsf{ZK}}, \mathsf{V}^z_{\mathsf{ZK}}, \mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{SHP}^{z,y}_{\mathsf{ZK}})$ for the circuit satisfiability relation $\mathcal{C}_n$ is described below.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{ASGen}_{\mathsf{ZK}}(1^n)}$

1. Run C's set-up algorithm to generate a CRS: $crs \leftarrow \mathsf{Gen}(1^n)$.
2. For each gate, set up Π in *adaptively-sound* mode: for $i \in [n]$, $crs_i \leftarrow \mathsf{ASGen}(1^n)$.
3. Output $crs_{\mathsf{ZK}} := (crs, crs_1, \ldots, crs_n)$.

$\underline{\pi_{\mathsf{ZK}} \leftarrow \mathsf{P}^z_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, C, \boldsymbol{w})}$

1. Use C with instance z to commit to the value of each wire: for $i \in [n]$, $(c_i, d_i) \leftarrow \mathsf{Com}^z(crs, w_i)$.
2. For each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$, use $((w_i, w_j, w_k), (d_i, d_j, d_k)))$ as witness to generate a proof π_g that $(crs, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g^z)$:
$$\pi_g \leftarrow \mathsf{P}^{D^z_{g,n}}\left(crs_g, (crs, c_i, c_j, c_k), ((w_i, w_j, w_k), (d_i, d_j, d_k))\right).$$
3. Output $\pi_{\mathsf{ZK}} := ((c_1, \cdots, c_n), (\pi_1, \cdots, \pi_{|C|}), d_n)$.

$\underline{b := \mathsf{V}^z_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, C, \pi_{\mathsf{ZK}})}$

1. Output $b := 1$ (accept π_{ZK}) if and only if all the checks below pass.
   (a) For each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$, use π_g to verify that $(crs, c_i, c_j, c_k) \in \mathcal{L}(\mathcal{G}_g^z)$: i.e., $\mathsf{V}\left(crs_g, (pk, c_i, c_j, c_k), \pi_g\right) = 1$.
   (b) Verify that C evaluates to 1, by ensuring that c_n opens to 1: $\mathsf{VOpen}^z(crs, c_n, d_n, 1) = 1$.

$\underline{crs_{\mathsf{ZK}} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^n)}$

1. Run C's set-up algorithm to generate a CRS: $crs \leftarrow \mathsf{Gen}(1^n)$.
2. For each gate, set up Π in *statistically-hiding* mode: for $i \in [n]$, $crs_i \leftarrow \mathsf{SHGen}(1^n)$.
3. Output $crs_{\mathsf{ZK}} := (crs, crs_1, \ldots, crs_n)$ as the CRS.

$\underline{\pi_{\mathsf{ZK}} \leftarrow \mathsf{SHP}^{z,y}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, C, \boldsymbol{w})}$

1. For $i \in [n]$, generate a fake commitment $(c_i, d_i) \leftarrow \mathsf{SHCom}^{z,y}(crs, w_i)$.
2. For each gate g in C with input wires $i, j \in [n]$ and output wire $k \in [n]$:
$$\pi_g \leftarrow \mathsf{P}^{\widehat{D}^{z,y}_{g,n}}\left(crs_g, (crs, c_i, c_j, c_k), ((w_i, w_j, w_k), (d_i, d_j, d_k))\right),$$
using the fake distribution oracle $\widehat{D}^{z,y}_{g,n}$.
3. Output $\pi_{\mathsf{ZK}} := ((c_1, \cdots, c_n), (\pi_1, \cdots, \pi_{|C|}), d_n)$.

Figure 5.2: Π_{ZK}, an ID-NISZKA for circuit satisfiability.

Local consistency relation $\mathcal{V}^z_{i,j}$ (for index $n \in \mathbb{N}$)

- *Hardwired.*
  1. Description of an instance $z \in \{0,1\}^n$ of relation $\mathcal{I}$
  2. Descriptions of the CIDC algorithms $\mathrm{C} = (\mathsf{Gen}, \mathsf{Com}^z, \mathsf{VOpen}^z)$ and MPC protocol M.
  3. A CRS *crs* of C
  4. Indices $i, j \in [n]$ of parties.
- *Instance.* A pair of commitments (c_i, c_j)
- *Witness.* (v_i, d_i, v_j, d_j), where v_i and v_j are views, and d_i and d_j are random coins.
- The relation holds if following conditions hold.
  1. *Commitments are consistent*: $\mathsf{VOpen}^z(crs, c_i, d_i, v_i) = 1$ and $\mathsf{VOpen}^z(crs, c_j, d_j, v_j) = 1$
  2. Views v_i and v_j are consistent with respect to public input x and protocol M and locally accepting (i.e., the local outputs are 1).

Figure 5.3: $\mathcal{V}^z := \left(\mathcal{V}^z_{i,j}\right)_{(i,j)\in\binom{n}{2}}$, the relation capturing local consistency of views.

- In the first, the CRS's crs_i for the distribution-oblivious dual-mode NIDSZKA is sampled using ASGen whereas in the second, it is sampled using SHGen.
- All commitments and decommitments in the first are generated using Com^z, whereas in the second, they are sampled using $\mathsf{SHCom}^{z,y}$. This in particular includes the generation of commitments and decommitments by the samplers $D^z_{g,n}$ and $\widehat{D}^{z,y}_{g,n}$, respectively.

To prove indistinguishability, we first switch all crs_i to be sampled using SHGen. This is computationally indistinguishable by the mode-indistinguishability guarantee of the underlying NIDSZKA. We then switch the generation of all commitments and decommitments to be done using $\mathsf{SHCom}^{z,y}$. This is indistinguishable by the fact that in CIDC, real and fake commitments (plus decommitments) are indistinguishable, whenever $(z, y) \in \mathcal{I}$.

□

5.3 Privacy Amplification using CIDC and MPC

We show how to amplify privacy of any ID-NISZKA with small enough statistical error to one with negligible error, assuming CIDC. Specifically, we follow the same construction from Section 4.3, replacing NISZKA with ID-NISZKA and DMC with CIDC. This construction results in ID-NISWIA with negligible error (which can then be made ID-NISZKA using the FLS transformation). The amplified ID-NISWIA $\Pi_{\mathsf{WI}} = (\mathsf{ASGen}_{\mathsf{WI}}, \mathsf{P}^z_{\mathsf{WI}}, \mathsf{V}^z_{\mathsf{WI}}, \mathsf{SHGen}_{\mathsf{WI}}, \mathsf{SHP}^{z,y})$ for $\mathcal{R}_n$, depending on $\mathcal{I}$, is described in Fig. 5.4. The relation $\mathcal{V}$ (Fig. 4.7) is naturally augmented to $\mathcal{V}^z$, described in Fig. 5.3.

Theorem 5.8 (Amplification Theorem)**.** *Let $\mathcal{R}$ and $\mathcal{I}$ be any* NP *relations. Consider the non-interactive protocol Π_{WI} for $\mathcal{R}$ described in Fig. 5.4, and instantiate:*

1. M *using an $n/2$-perfectly-secure semi-honest* MPC *protocol for $f_{\mathcal{R}}$ (Eq. (13)).*
2. Π_{ZK} *using an* ID-NISZKA *for $\mathcal{V}^z$, depending on $\mathcal{I}$, with* SWI *error $\varepsilon = 1/100n$.*

Let $\mathcal{R}$ be any NP relation and $(x, w) \in \mathcal{R}_n$. Let $\mathcal{I}$ be any NP relation and $z \in \{0,1\}^n$. Let

- $\Pi_{\mathsf{ZK}} = (\mathsf{ASGen}_{\mathsf{ZK}}, \mathsf{P}^z_{\mathsf{ZK}}, \mathsf{V}^z_{\mathsf{ZK}}, \mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{SHP}^{z,y})$ an ID-NISZKA depending on $\mathcal{I}$.
- $\mathrm{C} = (\mathsf{Gen}, \mathsf{Com}^z, \mathsf{VOpen}^z, \mathsf{SHCom}^{z,y})$ be a CIDC depending on $\mathcal{I}$; and
- M be an MPC protocol for $f_{\mathcal{R}}$.

$crs_{\mathsf{WI}} \leftarrow \mathsf{ASGen}_{\mathsf{WI}}(1^n)$

1. Run C's set-up algorithm to generate a CRS: $crs \leftarrow \mathsf{Gen}(1^n)$.
2. For each two parties $(i, j) \in \binom{[n]}{2}$, set up Π_{ZK} in *adaptively-sound* mode: $crs_{i,j} \leftarrow \mathsf{ASGen}_{\mathsf{ZK}}(1^n)$.
3. Output $crs_{\mathsf{WI}} := (crs, crs_{1,2}, \ldots, crs_{n-1,n})$ as the CRS.

$\pi_{\mathsf{WI}} \leftarrow \mathsf{P}^z_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, w)$

1. Execute M "in the head" as in Fig. 4.2, and use CIDC with instance z to commit to the views: i.e., for $i \in [n]$, generate $(c_i, d_i) \leftarrow \mathsf{Com}^z(crs, v_i)$.
2. Prove local consistency: for all $(i, j) \in \binom{[n]}{2}$, prove that $((c_i, c_j), ((v_i, d_i, v_j, d_j))) \in \mathcal{V}^z_{i,j}$ (Fig. 5.3)
$$\pi_{i,j} \leftarrow \mathsf{P}^z_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), (v_i, d_i, v_j, d_j)).$$
3. Output $\pi_{\mathsf{WI}} := ((c_1, \ldots, c_n), (\pi_{1,2}, \ldots, \pi_{n-1,n}))$

$b := \mathsf{V}^z_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, \pi_{\mathsf{WI}})$

1. Output $b := 1$ (accept π_{WI}) if and only if for each pair of parties $(i, j) \in \binom{[n]}{2}$, $\pi_{i,j}$ is a valid proof for $(c_i, c_j) \in \mathcal{L}(\mathcal{V}_{i,j})$, i.e., $\mathsf{V}^z_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), \pi_{i,j}) = 1$.

$crs_{\mathsf{WI}} \leftarrow \mathsf{SHGen}_{\mathsf{WI}}(1^n)$

1. Run C's set-up algorithm to generate a CRS: $crs \leftarrow \mathsf{Gen}(1^n)$.
2. For each two parties $(i, j) \in \binom{[n]}{2}$, set up Π_{ZK} in *statistically-hiding* mode: $crs_{i,j} \leftarrow \mathsf{SHGen}_{\mathsf{ZK}}(1^n)$.
3. Output $crs_{\mathsf{WI}} := (crs, crs_{1,2}, \ldots, crs_{n-1,n})$ as the CRS.

$\pi_{\mathsf{WI}} \leftarrow \mathsf{SHP}^{z,y}_{\mathsf{WI}}(crs_{\mathsf{WI}}, x, w)$

1. Execute M "in the head" as in Fig. 4.2, and use CIDC with instance z to generate fake commitments to the views: i.e., for $i \in [n]$, generate $(c_i, d_i) \leftarrow \mathsf{SHCom}^{z,y}(crs, v_i)$.
2. Generate fake proofs of local consistency: for all $(i, j) \in \binom{[n]}{2}$, prove that $((c_i, c_j), ((v_i, d_i, v_j, d_j))) \in \mathcal{V}^z_{i,j}$ using
$$\pi_{i,j} \leftarrow \mathsf{SHP}^{z,y}_{\mathsf{ZK}}(crs_{i,j}, (c_i, c_j), (v_i, d_i, v_j, d_j)).$$
3. Output $\pi_{\mathsf{WI}} := ((c_1, \ldots, c_n), (\pi_{1,2}, \ldots, \pi_{n-1,n}))$

Figure 5.4: Π_{WI}, a ID-NISWIA protocol for any NP relation $\mathcal{R}$.

3. C *using a* CIDC *depending on* $\mathcal{I}$*.*

Then Π_{WI} *is an* ID-NISWIA *for* $\mathcal{R}$ *depending on* $\mathcal{I}$ *with following properties:*

- *If* Π_{ZK} *has negligible (resp.,* 0*) completeness error then so does* Π_{WI}*.*
- *The soundness error is negligible in* C*'s (computational) security parameter.*
- *The SWI error is* 2^{-n+1}*.*

Proof Sketch. Completeness follows that of the underlying NISZKA and the correctness of CIDC. We next prove soundness (for no instances), and zero knowledge and mode indistinguishability (for yes instances).

Adaptive Soundness when $z \notin \mathcal{L}(\mathcal{I})$**.** The proof is identical to that of adaptive soundness in Theorem 4.10, except that instead of relying on binding of DMC, it relies on CIDC's binding. Again, recall that with overwhelming probability over crs, the CRS sampled for CIDC, for any (adaptively chosen) $z \notin \mathcal{L}(\mathcal{I})$, Com^z is a perfectly binding commitment.

SWI with Respect to $z \in \mathcal{L}(\mathcal{I})$**.** Fix any $(z, y) \in \mathcal{I}$. Here we need to prove that $(\mathsf{SHGen}_{\mathsf{WI}}, \mathsf{SHP}^{z,y}_{\mathsf{WI}}, \mathsf{V}^z_{\mathsf{WI}})$ is 2^{-n+1}-SWI. The proof is identical to that of $(2^{-n+1} + 2^{n+2}\delta n)$-SWI in Theorem 4.10, except that:

- Instead of relying on the δ-statistical hiding of DMC, we rely on the perfect statistical hiding of $\mathsf{SHCom}^{z,y}$ (corresponding to $\delta = 0$).
- Instead of relying on ε-SZK of a dual-mode NISZKA, we rely on the ε-SZK of fake proofs in the ID-NISZKA.

Indistinguishability of Real and Fake Proofs. Here we need to prove that for $(z, y) \in \mathcal{I}$, $(x, w) \in \mathcal{R}$, a real CRS and proof $(crs_{\mathsf{ZK}}, \pi_{\mathsf{ZK}})$ generated by $\mathsf{ASGen}_{\mathsf{ZK}}(1^n)$ and $\mathsf{P}^z(crs_{\mathsf{ZK}}, x, w)$ are computationally indistinguishable from ones generated by $\mathsf{SHGen}_{\mathsf{ZK}}(1^n)$ and $\mathsf{SHP}^{z,y}_{\mathsf{ZK}}(crs_{\mathsf{ZK}}, x, w)$. There are two differences between the two distributions:

- In the first, the CRS's $crs_{i,j}$ and proofs $\pi_{i,j}$ of the ID-NISZKA are sampled using $\mathsf{ASGen}_{\mathsf{ZK}}$ and P_{ZK} whereas in the second, it is sampled using $\mathsf{SHGen}_{\mathsf{ZK}}$ and $\mathsf{SHP}^{z,y}_{\mathsf{ZK}}$.
- All commitments and decommitments in the first are generated using Com^z, whereas in the second, they are sampled using $\mathsf{SHCom}^{z,y}$.

To prove indistinguishability, we first switch all $crs_{i,j}, \pi_{i,j}$ to be sampled using $\mathsf{SHGen}_{\mathsf{ZK}}, \mathsf{SHP}^{z,y}_{\mathsf{ZK}}$. This is computationally indistinguishable by the real vs. fake indistinguishability of the underlying NISZKA, whenever $(z, y) \in \mathcal{I}$. We then switch the generation of all commitments and decommitments to be done using $\mathsf{SHCom}^{z,y}$. This is indistinguishable by the fact that in CIDC, real and fake commitments (plus decommitments) are indistinguishable, whenever $(z, y) \in \mathcal{I}$. □

5.4 Corollaries

To conclude the section, we derive several corollaries.

First, we observe that any ID-NISWIA implies a NICZKA; namely, a plain (rather, than instance dependent) computational WI argument. We focus on the case of negligible error (although this holds more generally).

Lemma 5.9 (NICWIA from Dual-Mode ID-NISWIA)**.** *Let* $\mathcal{R}$ *be any* NP *relation. If there exists a* negl-ID-NISWIA *for* $\mathcal{R}$*, depending on* $\mathcal{I} = \mathcal{R}$*, the there exists a* NICWIA *(with a negligible computational error).*

Proof Sketch. Given the $\mathsf{ID\text{-}NISWIA}$ $(\mathsf{ASGen}, \mathsf{P}^z, \mathsf{V}^z, \mathsf{SHGen}, \mathsf{SHP}^{z,y})$, we construct the NICWIA $(\mathsf{Gen}, \mathsf{P}, \mathsf{V})$ as follows. Gen invokes ASGen, $\mathsf{P}(crs, x, w)$ invokes $\mathsf{P}^x(crs, x, w)$, and $\mathsf{V}(crs, x, \pi)$ invokes $\mathsf{V}^x(crs, x, \pi)$. Completeness and adaptive soundness follow directly from completeness and adaptive soundness of the ID scheme (recall that adaptive soundness also holds with respect to the depending instance). CWI follows by a direct hybrid argument. For any $x \in \mathcal{L}(\mathcal{R})$ and two witnesses w_0, w_1, we have that

$$(crs, \mathsf{P}(crs, x, w_0)) \overset{c}{\approx} (\widetilde{crs}, \mathsf{SHP}^{x,w_0}(\widetilde{crs}, x, w_0)) \approx (\widetilde{crs}, \mathsf{SHP}^{x,w_0}(\widetilde{crs}, x, w_1)) \overset{c}{\approx} (crs, \mathsf{P}(crs, x, w_1)) \ ,$$

where $crs \leftarrow \mathsf{ASGen}(1^\lambda)$ and $\widetilde{crs} \leftarrow \mathsf{SHGen}(1^\lambda)$. Here the outer two computational indistinguishabilities follow by real vs. fake indistinguishability of the ID scheme since $(x, w_0) \in \mathcal{R}$, and the inner statistical indistinguishability follows from the SWI of fake proofs. $\square$

As a corollary of Theorems 3.17, 5.7 and 5.8, Lemma 5.9, and Corollaries 3.21 and 3.22, we get the main result of this section.

Corollary 5.10. *Let $\mathcal{R}$ be any* NP*-complete relation. Assuming* OWF*s, a sufficiently-compressing somewhere-sound* NIBARG *for $\mathcal{R}$ implies an adaptively-sound* NICZKA *for $\mathcal{R}$.*

Acknowledgements

We thank Oded Goldreich for valuable comments and discussion. We also thank Chaya Ganesh for pointing us to the results in [CLP15].

Nir Bitansky is a member of the Checkpoint Institute of Information Security and is supported by the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme (grant agreement No. 101042417, acronym SPP).

Chethan Kamath is supported by Azrieli International Postdoctoral Fellowship, by the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme (grant agreement No. 101042417, acronym SPP), and by ISF grant 1789/19.

Omer Paneth is a member of the Checkpoint Institute of Information Security and is supported by an Azrieli Faculty Fellowship, and ISF grant 1789/19.

Ron Rothblum is funded by the European Union (ERC, FASTPROOF, 101041208). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

Prashant Nalini Vasudevan is supported by the National Research Foundation, Singapore, under its NRF Fellowship programme, award no. NRF-NRFF14-2022-0010.

References

[AH91] William Aiello and Johan Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *J. Comput. Syst. Sci.*, 42(3):327–345, 1991. 5

[AL17] Gilad Asharov and Yehuda Lindell. A full proof of the BGW protocol for perfectly secure multiparty computation. *Journal of Cryptology*, 30(1):58–151, January 2017. 41

[Ald83] David Aldous. Random walks on finite groups and rapidly mixing Markov chains. In *Séminaire de Probabilités XVII 1981/82: Proceedings*, pages 243–297. Springer, 1983. 41, 63

[AR21] Gal Arnon and Guy N. Rothblum. On prover-efficient public-coin emulation of interactive proofs. In Stefano Tessaro, editor, *2nd Conference on Information-Theoretic Cryptography, ITC 2021, July 23-26, 2021, Virtual Conference*, volume 199 of *LIPIcs*, pages 3:1–3:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 4

[AR23] Noga Amit and Guy N. Rothblum. Constant-round arguments from one-way functions. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1537–1544. ACM, 2023. 5

[BBD+20] Marshall Ball, Elette Boyle, Akshay Degwekar, Apoorvaa Deshpande, Alon Rosen, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan. Cryptography from information loss. In Thomas Vidick, editor, *ITCS 2020*, volume 151, pages 81:1–81:27. LIPIcs, January 2020. 7

[BDRV18] Itay Berman, Akshay Degwekar, Ron D. Rothblum, and Prashant Nalini Vasudevan. Multi-collision resistant hash functions and their applications. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 133–161. Springer, 2018. 5, 29

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988. 11, 41

[BHK17] Zvika Brakerski, Justin Holmgren, and Yael Tauman Kalai. Non-interactive delegation and batch NP verification from standard computational assumptions. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 474–482. ACM, 2017. 4, 10

[BHKY19] Nir Bitansky, Iftach Haitner, Ilan Komargodski, and Eylon Yogev. Distributional collision resistance beyond one-way functions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 667–695. Springer, 2019. 5, 29

[BKP18] Nir Bitansky, Yael Tauman Kalai, and Omer Paneth. Multi-collision resistance: a paradigm for keyless hash functions. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 671–684. ACM, 2018. 3, 5

[Blu81] Manuel Blum. Coin flipping by telephone. In Allen Gersho, editor, *CRYPTO'81*, volume ECE Report 82-04, pages 11–15. U.C. Santa Barbara, Dept. of Elec. and Computer Eng., 1981. 31

[BMO90] Mihir Bellare, Silvio Micali, and Rafail Ostrovsky. The (true) complexity of statistical zero knowledge. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 494–502. ACM, 1990. 10

[BP19] Nir Bitansky and Omer Paneth. On round optimal statistical zero knowledge arguments. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 128–156. Springer, Heidelberg, August 2019. 12

[CJJ21] Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. Non-interactive batch arguments for NP from standard assumptions. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part IV*, volume 12828 of *LNCS*, pages 394–423, Virtual Event, August 2021. Springer, Heidelberg. 4

[CJJ22] Arka Rai Choudhuri, Abhishek Jain, and Zhengzhong Jin. SNARGs for $\mathcal{P}$ from LWE. In *62nd FOCS*, pages 68–79. IEEE Computer Society Press, February 2022. 4, 5, 17

[CLP15] Kai-Min Chung, Edward Lui, and Rafael Pass. From weak to strong zero-knowledge and applications. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 66–92. Springer, Heidelberg, March 2015. 7, 57

[CW23] Jeffrey Champion and David J. Wu. Non-interactive zero-knowledge from non-interactive batch arguments. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 38–71. Springer, Heidelberg, August 2023. 7

[Del16] Holger Dell. And-compression of NP-complete problems: Streamlined proof and minor observations. *Algorithmica*, 75(2):403–423, 2016. 7, 8, 20

[DMO00] Giovanni Di Crescenzo, Tal Malkin, and Rafail Ostrovsky. Single database private information retrieval implies oblivious transfer. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 122–138. Springer, Heidelberg, May 2000. 7, 8, 20, 66

[DN02] Ivan Damgård and Jesper Buus Nielsen. Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 581–596. Springer, Heidelberg, August 2002. 34

[DNR04] Cynthia Dwork, Moni Naor, and Omer Reingold. Immunizing encryption schemes from decryption errors. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 342–360. Springer, Heidelberg, May 2004. 67

[DNRS99] Cynthia Dwork, Moni Naor, Omer Reingold, and Larry J. Stockmeyer. Magic functions. In *40th FOCS*, pages 523–534. IEEE Computer Society Press, October 1999. 15

[DPP97] Ivan Damgård, Torben P. Pedersen, and Birgit Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *J. Cryptol.*, 10(3):163–194, 1997. 29

[Dru15] Andrew Drucker. New limits to classical and quantum instance compression. *SIAM J. Comput.*, 44(5):1443–1479, 2015. 7, 8, 20

[FLS90] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*, pages 308–317. IEEE Computer Society, 1990. 10, 12, 17, 31, 32

[For89] Lance Fortnow. The complexity of perfect zero-knowledge. *Adv. Comput. Res.*, 5:327–343, 1989. 5

[FS90a] Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 416–426. ACM, 1990. 10, 29, 31

[FS90b] Uriel Feige and Adi Shamir. Zero knowledge proofs of knowledge in two rounds. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 526–544. Springer, Heidelberg, August 1990. 11, 49, 50

[FS08] Lance Fortnow and Rahul Santhanam. Infeasibility of instance compression and succinct PCPs for NP. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 133–142. ACM Press, May 2008. 7

[GH98] Oded Goldreich and Johan Håstad. On the complexity of interactive proofs with bounded communication. *Inf. Process. Lett.*, 67(4):205–214, 1998. 6

[GJS19] Vipul Goyal, Aayush Jain, and Amit Sahai. Simultaneous amplification: The case of non-interactive zero-knowledge. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 608–637. Springer, Heidelberg, August 2019. 11, 41, 42

[GK96] Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *J. Cryptol.*, 9(3):167–190, 1996. 31

[GMW86] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*, pages 174–187. IEEE Computer Society, 1986. 10, 29, 31

[Gol93] Oded Goldreich. A uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology*, 6(1):21–53, March 1993. 15

[Gol01] Oded Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques.* Cambridge University Press, 2001. 10

[Gol18] Oded Goldreich. On doubly-efficient interactive proof systems. *Found. Trends Theor. Comput. Sci.*, 13(3):158–246, 2018. 3, 13

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, Heidelberg, August 2006. 10

[GOS12] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *J. ACM*, 59(3):11:1–11:35, 2012. 16, 36

[GS89] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. *Adv. Comput. Res.*, 5:73–90, 1989. 4

[GSV98] Oded Goldreich, Amit Sahai, and Salil P. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In Jeffrey Scott Vitter, editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 399–408. ACM, 1998. 10

[GVW02] Oded Goldreich, Salil P. Vadhan, and Avi Wigderson. On interactive proofs with a laconic prover. *Comput. Complex.*, 11(1-2):1–53, 2002. 6, 7

[HHRS15] Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. 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. 5

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999. 31

[HJKS22] James Hulett, Ruta Jawale, Dakshita Khurana, and Akshayaram Srinivasan. SNARGs for P from sub-exponential DDH and QR. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 520–549. Springer, Heidelberg, May / June 2022. 4

[HM96] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Neal Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 201–215. Springer, Heidelberg, August 1996. 29

[HN10] Danny Harnik and Moni Naor. On the compressibility of *NP* instances and cryptographic applications. *SIAM J. Comput.*, 39(5):1667–1713, 2010. 7

[HNO+09] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil P. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.*, 39(3):1153–1218, 2009. 29

[Hol05] Thomas Holenstein. Key agreement from weak bit agreement. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 664–673. ACM Press, May 2005. 41

[HRV18] Pavel Hubácek, Alon Rosen, and Margarita Vald. An efficiency-preserving transformation from honest-verifier statistical zero-knowledge to statistical zero-knowledge. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 66–87. Springer, 2018. 10

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In David S. Johnson and Uriel Feige, editors, *39th ACM STOC*, pages 21–30. ACM Press, June 2007. 40, 41, 44

[Imp95] Russell Impagliazzo. Hard-core distributions for somewhat hard problems. In *36th FOCS*, pages 538–545. IEEE Computer Society Press, October 1995. 41

[Kil92] Joe Kilian. A note on efficient zero-knowledge proofs and arguments (extended abstract). In S. Rao Kosaraju, Mike Fellows, Avi Wigderson, and John A. Ellis, editors, *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Victoria, British Columbia, Canada*, pages 723–732. ACM, 1992. 3

[KLVW22] Yael Tauman Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Daniel Wichs. Boosting batch arguments and RAM delegation. *IACR Cryptol. ePrint Arch.*, page 1320, 2022. 4, 6

[KMY20] Fuyuki Kitagawa, Takahiro Matsuda, and Takashi Yamakawa. NIZK from SNARG. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 567–595. Springer, Heidelberg, November 2020. 7

[KMY23] Fuyuki Kitagawa, Takahiro Matsuda, and Takashi Yamakawa. NIZK from snargs. *J. Cryptol.*, 36(2):14, 2023. 17

[KNY18a] Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 162–194. Springer, 2018. 3, 29

[KNY18b] Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 162–194. Springer, 2018. 5

[KO97] Eyal Kushilevitz and Rafail Ostrovsky. Replication is NOT needed: SINGLE database, computationally-private information retrieval. In *38th FOCS*, pages 364–373. IEEE Computer Society Press, October 1997. 68

[KRR$^+$20] Inbar Kaslasi, Guy N. Rothblum, Ron D. Rothblum, Adam Sealfon, and Prashant Nalini Vasudevan. Batch verification for statistical zero knowledge proofs. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II*, volume 12551 of *Lecture Notes in Computer Science*, pages 139–167. Springer, 2020. 7

[KRV21] Inbar Kaslasi, Ron D. Rothblum, and Prashant Nalini Vasudevan. Public-coin statistical zero-knowledge batch verification against malicious verifiers. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part III*, volume 12698 of *Lecture Notes in Computer Science*, pages 219–246. Springer, 2021. 7

[LFKN92] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992. 3

[LM20] David Lanzenberger and Ueli Maurer. Coupling of random systems. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 207–240. Springer, Heidelberg, November 2020. 11, 35, 41, 45, 48, 64, 65, 66

[LS19] Alex Lombardi and Luke Schaeffer. A note on key agreement and non-interactive commitments. Cryptology ePrint Archive, Report 2019/279, 2019. https://eprint.iacr.org/2019/279. 67

[LY94] Richard J. Lipton and Neal E. Young. Simple strategies for large zero-sum games with applications to complexity theory. In *26th ACM STOC*, pages 734–740. ACM Press, May 1994. 9, 21

[Mic94] Silvio Micali. CS proofs (extended abstracts). In *35th FOCS*, pages 436–453. IEEE Computer Society Press, November 1994. 4

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptol.*, 4(2):151–158, 1991. 29, 50

[Oka96] Tatsuaki Okamoto. On relationships between statistical zero-knowledge proofs. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 649–658. ACM, 1996. 10

[OV08] Shien Jin Ong and Salil P. Vadhan. An equivalence between zero knowledge and commitments. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 482–500. Springer, Heidelberg, March 2008. 11, 49

[OVY93] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Interactive hashing simplifies zero-knowledge protocol design. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 267–273. Springer, 1993. 10

[PP22] Omer Paneth and Rafael Pass. Incrementally verifiable computation via rate-1 batch arguments. In *63rd FOCS*, pages 1045–1056. IEEE Computer Society Press, October / November 2022. 4

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 554–571. Springer, Heidelberg, August 2008. 66

[RR20] Guy N. Rothblum and Ron D. Rothblum. Batch verification and proofs of proximity with polylog overhead. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II*, volume 12551 of *Lecture Notes in Computer Science*, pages 108–138. Springer, 2020. 3

[RRR18] Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum. Efficient batch verification for UP. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, volume 102 of *LIPIcs*, pages 22:1–22:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. 3

[RRR21] Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum. Constant-round interactive proofs for delegating computation. *SIAM J. Comput.*, 50(3), 2021. 3, 6

[Sha92] Adi Shamir. IP = PSPACE. *J. ACM*, 39(4):869–877, 1992. 3

[Vad99] Salil Pravin Vadhan. *A study of statistical zero-knowledge proofs.* PhD thesis, Massachusetts Institute of Technology, 1999. 5, 6, 28

[vN28] J v. Neumann. Zur theorie der gesellschaftsspiele. *Mathematische annalen*, 100(1):295–320, 1928. 21

[VZ13] Salil P. Vadhan and Colin Jia Zheng. A uniform min-max theorem with applications in cryptography. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 93–110. Springer, Heidelberg, August 2013. 7, 9, 23

[Wee05] Hoeteck Wee. On round-efficient argument systems. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings*, volume 3580 of *Lecture Notes in Computer Science*, pages 140–152. Springer, 2005. 3

[WW22] Brent Waters and David J. Wu. Batch arguments for NP and more from standard bilinear group assumptions. In *CRYPTO (2)*, volume 13508 of *Lecture Notes in Computer Science*, pages 433–463. Springer, 2022. 4

A Proof of Lemma 4.19

Before stating and (re)proving Lemma 4.19, which completes the proof of Claim 4.18 and therefore Theorem 4.10, we define statistical coupling (Definition A.1) and recall a lemma about statistical coupling (Lemma A.2) that will be key to the proof. We also introduce some notation (Notation A.3) that will help reduce clutter.

Definition A.1 (Statistical Coupling). *Let X and Y be two probability distributions defined on a finite set Ω. A joint probability distribution XY on Ω^2 is a* statistical coupling *of X and Y if its marginal distributions are X and Y, respectively, i.e., for every $x \in \Omega$:*

$$X(x) = \sum_{y \in \Omega} XY(x, y),$$

and for every $y \in \Omega$:

$$Y(y) = \sum_{x \in \Omega} XY(x, y).$$

Lemma A.2 (Coupling Lemma [Ald83]). *Let X and Y be probability distributions over the same set Ω. Then*

1. *For* every *coupling XY of X and Y,*

$$\mathsf{SD}(X, Y) \leqslant \Pr_{(x,y) \leftarrow XY}[x \neq y]$$

2. *There exists an "optimal" coupling XY^* such that*

$$\mathsf{SD}(X, Y) = \Pr_{(x,y) \leftarrow XY^*}[x \neq y]$$

Notation A.3 ([LM20])**.** *For two vectors of objects (e.g., distributions) $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n)$, and a string $s \in \{0,1\}^n$, we use $\langle \boldsymbol{a}/\boldsymbol{b} \rangle_s = \langle a_1/b_1, a_2/b_2, \ldots, a_n/b_n \rangle_s$ to denote the vector $\boldsymbol{c} = (c_1, \ldots, c_n)$ where*

$$c_i := \begin{cases} a_i & \text{if } s_i = 0 \\ b_i & \text{if } s_1 = 1. \end{cases}$$

The following lemma is a restatement of Lemma 4.19 and is based on Lemma 7, Theorem 3 and Corollary 1 from [LM20]. The notation and presentation has been altered for the sake of compatibility with this paper.

Lemma A.4. *There exists two distributions Z and S, where Z is over $\{0,1\}^N_{\geqslant T} \cup \{0^N\}$, with $Z(0^N) > 2^{-n}$, and S is over $\{0,1\}^N_{\geqslant T}$, such that*

$$Z(0^N)^{-1} \cdot \max\left\{\mathsf{SD}(H_{1,Z}, H_{1,S}), \mathsf{SD}(H'_{1,Z}, H'_{1,S})\right\} \leqslant \left(\frac{4eN}{n}\varepsilon\right)^{n/4}, \tag{18}$$

where N, n, T, ε, $H_{1,Z}$, $H_{1,S}$, $H'_{1,Z}$ and $H'_{1,S}$ are as defined in Section 4.3.

Proof. We proceed in two steps. First, we define what it means for a pair of distributions Z and S, as in the statement of the lemma, to be "good". Then, we show that if Z and S are good then the lemma follows (this roughly corresponds to [LM20, Lemma 7]).

Step I. For two strings $s, e \in \{0,1\}^N$, let $\mathrm{blind}(s, e)$ be the function that returns the substring of s at indices i such that $e_i = 1$.

Definition A.5 (Good pair of distributions)**.** *Let $E = (E_{i,j})_{(i,j) \in \binom{[n]}{2}}$ denote a tuple of N independent Bernoulli distributions with bias at most ε, i.e., for every $(i,j) \in \binom{[n]}{2}$, it holds that*

$$\Pr_{e_{i,j} \leftarrow E_{i,j}}[e_{i,j} = 1] \leqslant \varepsilon.$$

A pair of distributions Z and S is good *if*

- *Z is supported over $\{0,1\}^N_{\geqslant T} \cup \{0^N\}$,*
- *$Z(0^N) > 2^{-n}$,*
- *S is supported over $\{0,1\}^N_{\geqslant T}$,*
- *$\mathbb{E}_{e \leftarrow E}[\mathsf{SD}(\mathrm{blind}(Z, e), \mathrm{blind}(S, e))] \leqslant Z(0^N)\left(\frac{4eN}{n}\varepsilon\right)^{n/4}$.*

In [LM20], a pair of such good distributions is constructed explicitly. For the sake of completeness, we include a description of the [LM20] distributions in Appendix A.1.

Step II. We now prove the lemma given that the pair of distributions Z and S described in Stage I is good. To be specific, we show

$$\mathsf{SD}(H_{1,Z}, H_{1,S}) \leqslant \mathop{\mathbb{E}}_{e \leftarrow E}[\mathsf{SD}(\mathrm{blind}(Z, e), \mathrm{blind}(S, e))]. \tag{19}$$

The proof of the corresponding claim for H' is similar and is hence omitted.

$\underline{(\boldsymbol{\zeta}, \boldsymbol{\sigma}) \leftarrow G_{\boldsymbol{RI}^*}}$

1. Sample $((\boldsymbol{crs}_R, \boldsymbol{\pi}_R), (\boldsymbol{crs}_I, \boldsymbol{\pi}_I)) \leftarrow \boldsymbol{RI}^*$
2. Compute $e = \{e_{i,j}\}_{(i,j)\in\binom{[n]}{2}}$, where $e_{i,j}$ is indicator for the event $R^*_{i,j} = I^*_{i,j}$: i.e., $e_{i,j} = 1 \Leftrightarrow R^*_{i,j} = I^*_{i,j}$, where recall that $R^*_{i,j} = (crs_{R,i,j}, \pi_{R,i,j})$ and $I^*_{i,j} = (crs_{I,i,j}, \pi_{I,i,j})$.
3. Consider the random variables $\text{blind}(Z, e)$ and $\text{blind}(S, e)$ induced by Z and S, and let $\text{blind}(Z, e)\text{blind}(Z, e)^*$ denote the optimal coupling between the two.
4. Sample $(z', s') \leftarrow \text{blind}(Z, e)\text{blind}(S, e)^*$.
5. Sample $z \leftarrow Z$ conditioned on $\text{blind}(z, e) = z'$ and $s \leftarrow S$ conditioned on $\text{blind}(s, e) = s'$
6. Set $\boldsymbol{\zeta} := (\langle \boldsymbol{crs}_R/\boldsymbol{crs}_I\rangle_z, \langle \boldsymbol{\pi}_R/\boldsymbol{\pi}_I\rangle_z)$ and $\boldsymbol{\sigma} := (\langle \boldsymbol{crs}_R/\boldsymbol{crs}_I\rangle_s, \langle \boldsymbol{\pi}_R/\boldsymbol{\pi}_I\rangle_s)$
7. Output $(\boldsymbol{\zeta}, \boldsymbol{\sigma})$

Figure A.1: Coupling experiment G.

Recall the distributions $H_{1,Z}$ and $H_{1,S}$ from Fig. 4.8. Next, consider $H_{1,Z}$ and $H_{1,S}$ with the execution of M and Λ fixed, i.e., the hiding CRS crs_Δ, views $\boldsymbol{v}$ and ciphertext-random coin pair $(\boldsymbol{c}, \boldsymbol{d})$ in distribution $H_{1,Z}$ and $H_{1,S}$ are fixed. To prove the lemma, it suffices to show Eq. (19) holds for every $(crs_\Delta, \boldsymbol{v}, \boldsymbol{c}, \boldsymbol{d})$. Hence, from here on, let's consider $H_{1,Z}$ and $H_{1,S}$ with $(crs_\Delta, \boldsymbol{v}, \boldsymbol{c}, \boldsymbol{d})$ fixed.

For $(i, j) \in \binom{[n]}{2}$, let's denote by $R_{i,j}$ and $I_{i,j}$ the random variables corresponding to the real and simulated execution of Π_{ZK}, respectively (see Fig. 4.8, Line 3). Following [LM20], we denote $H_{1,Z}$ by $H_1(\langle \boldsymbol{R}, \boldsymbol{I}\rangle_Z)$ (see Notation A.3). Since Π_{ZK} is ZK with error $\varepsilon = 1/100n$, we have $\mathsf{SD}(R_{i,j}, I_{i,j}) \leqslant \varepsilon$. As a result, by Lemma A.2, there exists an optimal coupling RI^*_{ij} of $R_{i,j}$ and $I_{i,j}$ such that

$$\Pr_{((crs_{R,i,j}, \pi_{R,i,j}), (crs_{I,i,j}, \pi_{I,i,j})) \leftarrow RI^*_{i,j}} [(crs_{R,i,j}, \pi_{R,i,j}) \neq (crs_{I,i,j}, \pi_{I,i,j})] \leqslant \varepsilon. \tag{20}$$

Let's use $R^*_{i,j}$ and $I^*_{i,j}$ to denote the first and second argument of $RI^*_{i,j}$, respectively. Then, we have

$$\begin{aligned} \mathsf{SD}(H_{1,Z}, H_{1,S}) &= \mathsf{SD}(H_1(\langle \boldsymbol{R}, \boldsymbol{I}\rangle_Z), H_1(\langle \boldsymbol{R}, \boldsymbol{I}\rangle_S)) \\ &= \mathsf{SD}(H_1(\langle \boldsymbol{R}^*, \boldsymbol{I}^*\rangle_Z), H_1(\langle \boldsymbol{R}^*, \boldsymbol{I}^*\rangle_S)) \\ &\leqslant \mathsf{SD}(\langle \boldsymbol{R}^*, \boldsymbol{I}^*\rangle_Z, \langle \boldsymbol{R}^*, \boldsymbol{I}^*\rangle_S). \end{aligned} \tag{21}$$

Here, the second equality follows by the definition of coupling (which requires the marginals to match) and the inequality is a consequence of data processing inequality. To upper bound Eq. (21), we set up a coupling experiment G, described in Fig. A.1, involving $\boldsymbol{RI}^*$. To see why G is a valid coupling, we claim that the marginal distributions of z and s sampled as part of G are Z and S respectively, z is independent of $\boldsymbol{R}$, and s is independent of $\boldsymbol{I}$. As a result, the marginal distributions of $\boldsymbol{\zeta}$ and $\boldsymbol{\sigma}$ are the same as $H_{1,Z}$ and $H_{1,S}$ respectively. To see why the (marginal) distribution of z sampled as part of G is Z (the argument for s and S is analogous) and independent of $\boldsymbol{R}$, note that for any e sampled in the first step, z' is distributed as $\text{blind}(Z, e)$, and z is sampled from Z conditioned on z'.

Therefore, by Lemma A.2 ("for every" claim), we have from Eq. (21) that

$$\begin{aligned}
\mathsf{SD}(\langle \boldsymbol{R}^*, \boldsymbol{I}^* \rangle_Z, \langle \boldsymbol{R}^*, \boldsymbol{I}^* \rangle_S) &\leqslant \Pr_G [\boldsymbol{\zeta} \neq \boldsymbol{\sigma}] \\
&= \sum_{e' \in \binom{[n]}{2}} \Pr_G [\boldsymbol{\zeta} \neq \boldsymbol{\sigma}, e = e'] \\
&= \sum_{e' \in \binom{[n]}{2}} \Pr_G \left[\mathrm{blind}(z, e) \neq \mathrm{blind}(s, e), e = e'\right] \\
&= \sum_{e' \in \binom{[n]}{2}} \Pr_{G|_{e=e'}} \left[\mathrm{blind}(z, e') \neq \mathrm{blind}(s, e')\right] \cdot \Pr_G \left[e = e'\right] \\
&= \sum_{e' \in \binom{[n]}{2}} \mathsf{SD}(\mathrm{blind}(Z, e'), \mathrm{blind}(S, e')) \cdot \Pr_G \left[e = e'\right] \qquad (22)
\end{aligned}$$

where $\boldsymbol{\zeta}$, $\boldsymbol{\sigma}$, e and (z, s) above are sampled as part of G, and Eq. (22) follows by optimality of $\mathrm{blind}(Z, e)\mathrm{blind}(S, e)^*$. Since each $e_{i,j}$ in G is distributed as required (because Π_{ZK} is zero-knowledge with error ε and the executions are independent), we get from Eqs. (21) and (22) that

$$Z(0^N)^{-1} \cdot \mathsf{SD}(H_{1,Z}, H_{1,S}) \leqslant Z(0^N)^{-1} \cdot \mathop{\mathbb{E}}_{e' \leftarrow E} \left[\mathsf{SD}(\mathrm{blind}(Z, e'), \mathrm{blind}(S, e))\right] \leqslant \left(\frac{4eN}{n} \varepsilon\right)^{n/4},$$

where the final inequality follows from the fact that Z and S is a pair of good distributions.

□

A.1 Good Distributions

We recall the good pair of distributions Z and S defined in [LM20], described using multisets, $\mathcal{Z}$ and $\mathcal{S}$, respectively:[17]

$$\mathcal{S} := \bigcup_{j \in \{T, T+2, \cdots, N\}} \left\{ \left(b, \binom{j-1}{T-1}\right) : b \in \{0,1\}^N, \|b\|_0 = j \right\}, \text{ and}$$

$$\mathcal{Z} := \{(0^N, 1)\} \cup \bigcup_{j \in \{T+1, T+3, \cdots, N\}} \left\{ \left(b, \binom{j-1}{T-1}\right) : b \in \{0,1\}^N, \|b\|_0 = j \right\}.$$

The proof that Z and S constitute a pair of good distributions can be found in [LM20, Theorem 3 and Corollary 1].

B LPKE via Somewhere Extractable NIBARGs

In this section, we recall the definition of *somewhere extractable* BARGs from the literature, and also define a variant thereof, which we call *honestly somewhere extractable.* We prove that somewhere-extractable BARGs imply (single databased, computationally-) *private information retrieval* (PIR), which in turn is known to imply *statistically sender-private oblivious transfer* and lossy public-key encryption (LPKE) [DMO00, PVW08].

The resulting LPKE suffers from a negligible decryption error, which makes it insufficient for the NISZKA amplification theorem in Section 4.3. We observe that if the BARGs satisfy honest-somewhere extraction then the resulting LPKE has a stronger correctness guarantee, which is also sufficient for our amplification theorem. First, we recall the definition of LPKE.

[17] A multiset $\mathcal{M}$ over a domain Ω is represented as $\{(x, m_x) : x \in \Omega\}$ where $m_x \in \mathbb{N}$ is the multiplicity of the element x. The cardinality of $\mathcal{M}$ is then defined as $|\mathcal{M}| := \sum_{x \in \Omega} m_x$. The probability distribution M induced by $\mathcal{M}$ is defined naturally: the probability of an element $x \in \Omega$ is $m_x / |\mathcal{M}|$.

Definition B.1 (LPKE)**.** *A* lossy public-key encryption *scheme* Λ *with message-space* $\mathcal{M}$ *and ciphertext-space* $\mathcal{C}$ *is a tuple of polynomial-time algorithms* $(\mathsf{KGen}, \mathsf{LGen}, \mathsf{E}, \mathsf{D})$ *with following syntax:*

- $(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$*. The randomised* binding*-key-generation algorithm, on input a security parameter* $\lambda \in \mathbb{N}$*, outputs a public-private key-pair* (pk, sk)*. We refer to a public key generated by* KGen *as a* binding *key.*
- $pk \leftarrow \mathsf{LGen}(1^\lambda)$*. The randomised* lossy*-key-generation algorithm, on input a security parameter* $\lambda \in \mathbb{N}$*, outputs a public key* pk*, which we refer to as a* lossy *key.*
- $c \leftarrow \mathsf{E}(pk, m)$*. The randomised encryption algorithm takes as input a public key* pk *and a message* $m \in \mathcal{M}$*, and outputs a ciphertext* $c \in \mathcal{C}$*.*
- $m := \mathsf{D}(sk, c)$*. The deterministic decryption algorithm takes a secret key* sk *and a ciphertext* $c \in \mathcal{C}$ *as input and outputs a message* $m \in \mathcal{M}$*.*

We require the following properties from Λ*:*

1. Binding public keys are almost-all-keys perfectly correct [DNR04]. *With overwhelming probability over the choice of binding keys, perfect correctness of decryption must hold. More formally, with overwhelming probability over* $(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$*, for every* $m \in \mathcal{M}$

$$\Pr_{c \leftarrow \mathsf{E}(pk,m)} [\mathsf{D}(sk, c) \neq m] = 0.$$

2. Lossy keys are statistically hiding. *For a random* lossy *key, the distribution of ciphertexts of any two messages must be* statistically *close. To be specific, we say that the lossy keys are* δ-statistically-hiding *if for all* $m_0, m_1 \in \mathcal{M}$ *and large enough* $\lambda \in \mathbb{N}$*:*

$$\mathsf{SD}((pk, \mathsf{E}(pk, m_0)), (pk, \mathsf{E}(pk, m_1))) \leqslant \delta(\lambda),$$

where $pk \leftarrow \mathsf{LGen}(1^\lambda)$*.*

3. Mode indistinguishability. *We require that the binding and lossy keys are computationally indistinguishable. More formally, for every polynomial-size circuit family* $\mathsf{A} = (\mathsf{A}_\lambda)_{\lambda \in \mathbb{N}}$*, there is a negligible function* μ*, such that for all* $\lambda \in \mathbb{N}$*:*

$$\left| \Pr_{(pk,sk) \leftarrow \mathsf{KGen}(1^\lambda)} [1 \leftarrow \mathsf{A}_\lambda(pk)] - \Pr_{pk \leftarrow \mathsf{LGen}(1^\lambda)} [1 \leftarrow \mathsf{A}_\lambda(pk)] \right| \leqslant \mu(\lambda).$$

Remark B.2 (Weak LPKE as Dual-Mode Commitments)**.** *We note that with overwhelming probability over the choice of a random* binding *key* pk*, the encryption algorithm* $\mathsf{E}(pk, \cdot)$ *acts as a perfectly-binding (non-interactive) commitment, with the random coins used for encryption serving as opening (see [LS19]). Analogously, over the choice of a random* hiding *key* pk*, the encryption algorithm* $\mathsf{E}(pk, \cdot)$ *acts as a perfectly-hiding (non-interactive) commitment. By mode indistinguishability of* LPKE*, it follows that* LPKE *implies dual-mode commitments. In fact,* LPKE *implies the stronger notion of* DMC *where the binding CRS is extractable via a trapdoor, here, the secret key (see Remark 4.3). Our results in the reverse direction achieving* LPKE *from somewhere extractable* BARG*s (Appendix B) achieve efficient decryption, and therefore implies the stronger notion of* DMC*.*

B.1 PIR from Somewhere Extractability

Definition B.3 (Somewhere Extractability)**.** *A batch protocol* $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *for a relation* $\mathcal{R}$ *is* somewhere extractable *if it satisfies CRS indistinguishability, and if there is a PPT extractor* E *such that, for every* *polynomial* t *and polynomial-size circuit family of provers* $\mathsf{P}^* = (\mathsf{P}^*_\lambda)_{\lambda \in \mathbb{N}}$, *there is a negligible function* μ *such that for every* $\lambda \in \mathbb{N}$, $t = t(\lambda)$, *and* $i^* \in [t]$:

$$\Pr_{crs^*, td, \mathsf{E}}\left[\mathsf{V}(crs^*, (x_1, \ldots, x_t), \pi) \text{ accepts } \wedge\ (x_{i^*}, w) \notin \mathcal{R}\right] \leqslant \mu(\lambda),$$

where $(crs^*, td) \leftarrow \mathsf{TGen}(1^\lambda, 1^t, i^*)$, $((x_1, \ldots, x_t), \pi) \leftarrow \mathsf{P}^*_\lambda(crs^*, i^*)$, *and* $w \leftarrow \mathsf{E}(td, i^*, crs^*, (x_1, \ldots, x_t), \pi)$.

Definition B.4 (Single-Database, Computational PIR [KO97])**.** *A one-round, single-database computational* PIR *is a tuple of polynomial-time algorithms* $(\mathsf{Q}, \mathsf{D}, \mathsf{R})$ *with the following syntax:*

- $(k, Q) \leftarrow \mathsf{Q}(1^\lambda, \ell, i)$. *The randomized* user query *algorithm takes as input a security parameter* $\lambda \in \mathbb{N}$, *a parameter* $\ell \in \mathbb{N}$ *that represents the length of the database, and a target index* $i \in [\ell]$. *It outputs a key* k *and a query* Q.
- $a := \mathsf{D}(D, Q)$. *The deterministic* database answer *algorithm takes as input a database* $D := (D_1, \ldots, D_\ell) \in \{0,1\}^\ell$ *and a query* Q *and outputs an answer* a.
- $d := \mathsf{R}(k, a)$. *The deterministic* user reconstruct *algorithm takes as input the key* k *and answer* a *and outputs a data bit* d.

We require the following properties:

1. Correctness of reconstruction. *There exists a negligible function* μ *such that for every* $\lambda \in \mathbb{N}$, $\ell \in \mathsf{poly}(\lambda)$, *database* $D \in \{0,1\}^\ell$ *and query* $i \in [\ell]$:

$$\Pr_{(k,Q) \leftarrow \mathsf{Q}(1^\lambda, \ell, i)}\left[\mathsf{R}(k, \mathsf{D}(D, Q)) = D_i\right] \geqslant 1 - \mu(\lambda).$$

2. Succinctness. *We say that the* PIR *is succinct if* $|a| \leqslant \ell^\epsilon$ *for some* $\epsilon < 1$. *We say that the* PIR *is* fully *succinct if there exists* poly *such that* $|a| \leqslant \mathsf{poly}(\lambda)$.
3. Computational user privacy. *No efficient adversary can distinguish between user queries on two target indices. That is, for every polynomial-size circuit family of distinguishers* $\mathsf{A} = \{\mathsf{A}_\lambda\}_{\lambda \in \mathbb{N}}$, *there is a negligible function* μ, *such that for all* $\lambda \in \mathbb{N}$, $\ell \in \mathsf{poly}(\lambda)$ *and* $i, j \in [\ell]$

$$\left| \Pr_{(k,Q) \leftarrow \mathsf{Q}(1^\lambda, \ell, i)}\left[1 \leftarrow \mathsf{A}_\lambda(Q)\right] - \Pr_{(k,Q) \leftarrow \mathsf{Q}(1^\lambda, \ell, j)}\left[1 \leftarrow \mathsf{A}_\lambda(Q)\right] \right| \leqslant \mu(\lambda).$$

The PIR scheme constructed from somewhere-extractable NIBARG is described in Fig. B.1. It relies on the fact that somewhere-extractable NIBARG implies one-way functions (OWFs) , and given a OWF f, we can define an NP relation

$$\mathcal{R}_f := \{((y_0, y_1), x) : f(x) = y_0 \vee f(x) = y_1\} \tag{23}$$

that allows sampling an instance along with *two* witnesses. To be precise, the hard sampler for $\mathcal{R}_f$ invokes the OWF on two random preimages x_0 and x_1, and then outputs the instance $(y_0 := f(x_0), y_1 := f(x_1))$.

Theorem B.5 (Somewhere-Extractable NIBARG Implies PIR)**.** *If there exists a somewhere-extractable* NIBARG $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$, *then the scheme in Fig. B.1 is a one-round, single database* PIR. *If the size of* BARG*s is independent of the number of instances, then the* PIR *is fully succinct.*

Proof Sketch. The construction inherits succinctness of the NIBARG. Whereas, user privacy follows from its CRS indistinguishability (Definitions 2.24 and B.3). Correctness follows from somewhere extractability of the NIBARG and one-wayness as argued next. By somewhere extractability, it is guaranteed that with overwhelming probability the extractor returns *some* witness of $(y_{i,0}, y_{i,1})$, i.e., *some* pre-image of $y_{i,0}$ or $y_{i,1}$ under f. One-wayness of f ensures that it returns a witness corresponding to y_{i,D_i} and not $y_{i,\overline{D}_i}$. Indeed, since Q generates the NIBARG proof based only on the witness/pre-image x_{i,D_i}, it is oblivious of the other witnesses $x_{i,\overline{D}_i}$. As a result, the extractor outputting $x_{i,\overline{D}_i}$ is tantamount to breaking f's one-wayness. ☐

PIR scheme $(\mathsf{Q}, \mathsf{D}, \mathsf{R})$, built using a somewhere-extractable NIBARG $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ with extractor E, and hard sampler for the relation $\mathcal{R}_f$ from Eq. (23).

$\underline{(k, Q) \leftarrow \mathsf{Q}(1^\lambda, \ell, i)}$

1. Use the hard sampler for $\mathcal{R}_f$ to generate ℓ instance-witness pairs

$$\boldsymbol{q} := (((y_{1,0}, y_{1,1}), x_{1,0}, x_{1,1}), \ldots, ((y_{\ell,0}, y_{\ell,1}), x_{\ell,0}, x_{\ell,1})).$$

2. Use TGen to sample a CRS with trapdoor set up at index i: $(crs^*, td) \leftarrow \mathsf{TGen}(1^\lambda, 1^\ell, i)$.

3. Output $((i, td, (crs^*, \boldsymbol{q})), (crs^*, \boldsymbol{q}))$.

$\underline{a := \mathsf{D}(D, Q)}$

1. Run the batch prover on witnesses determined by D:

$$\pi \leftarrow \mathsf{P}(crs^*, ((y_{1,0}, y_{1,1}), \ldots, (y_{\ell,0}, y_{\ell,1})), (x_{1,D_1}, \ldots, x_{\ell,D_\ell})).$$

2. Output π.

$\underline{d := \mathsf{R}(k, a)}$

1. Halt without output if the BARG verifier rejects, i.e., $\mathsf{V}(crs^*, ((y_{1,0}, y_{1,1}), \ldots, (y_{\ell,0}, y_{\ell,1}), \pi)) = 0$.

2. Use BARG extractor to extract witness at i: $w \leftarrow \mathsf{E}(td, i, crs^*, ((y_{1,0}, y_{1,1}), \ldots, (y_{\ell,0}, y_{\ell,1})), \pi)$, and set

$$d := \begin{cases} 0 & \text{if } f(w) = y_{i,0} \\ 1 & \text{otherwise.} \end{cases}$$

3. Output d.

Figure B.1: PIR scheme $(\mathsf{Q}, \mathsf{D}, \mathsf{R})$.

B.2 Honest Somewhere Extractability

Definition B.6 (Honest Somewhere Extractability)**.** *A batch protocol* $(\mathsf{Gen}, \mathsf{TGen}, \mathsf{P}, \mathsf{V})$ *for a relation* $\mathcal{R}$ *is* honestly somewhere extractable *if it satisfies CRS indistinguishability, and if there is a PPT extractor* E *such that, for every* $\lambda \in \mathbb{N}$, $t = t(\lambda)$, $(x_1, w_1), \dots, (x_t, w_t) \in \mathcal{R}$ *and* $i^* \in [t]$*:*

$$\Pr_{crs^*, td, \mathsf{E}}[w_{i^*} \neq w] = 0,$$

where $(crs^*, td) \leftarrow \mathsf{TGen}(1^\lambda, 1^t, i^*)$, $\pi \leftarrow \mathsf{P}(crs^*, (x_1, w_1), \dots, (x_t, w_t))$*, and* $w \leftarrow \mathsf{E}(td, i^*, crs^*, (x_1, \dots, x_t), \pi)$.

Remark B.7. *We can in fact further weaken the above requirement, asking for perfect correctness for* almost any CRS*. Namely, that with overwhelming probability over the choice of CRS, extraction is perfect.*

Going back to the construction if Fig. B.1, in case the BARG satisfies *honest* somewhere extractability (Definition B.6), then the construction satisfies perfect correctness of reconstruction. Indeed, the NIBARG proof generated by Q is honest, the extractor is guaranteed to return the actual witness used at position i, which is x_{i,D_i}.