Simultaneous Resettable WI from One-way Functions

Kai-Min Chung* Rafael Pass*

February 5, 2013

Abstract

In this short note, we demonstrate that the existence of one-way functions implies the existence of an $\omega(1)$-round simultaneously resettable witness indistinguishable argument of knowledge.

1 Introduction

In this short note we consider constructions of *simultaneously* resettable witness indistinguishable ($\mathsf{sr}\mathcal{WI}$) argument for NP; that is, interactive argument systems that both remains *sound* and *witness indistinguishable* under resetting attacks (see [BGGL01] for formal definition). Barak, Goldreich, Goldwasser and Lindell [BGGL01] note that the two-round witness indistinguishable arguments (called "zaps") of Dwork and Naor [DN00] directly are $\mathsf{sr}\mathcal{WI}$. More recently, Cho, Ostrovsky, Scafuro, and Visconti [COSV12] provide a construction of $\mathsf{sr}\mathcal{WI}$ *argument of knowledge* based on the existence of zaps and collision-resistant hash functions.

But constructions of zaps are only known under stronger assumptions than just one-way functions (e.g., trapdoor permutations). A very recent elegant work by Ostrovsky and Visconti [OV12] presents a construction of $poly(n)$-round $\mathsf{sr}\mathcal{WI}$ arguments of knowledge based on collision-resistant hash functions. They exploit a connection between lower bounds for black-box zero-knowledge and resettable soundness first made in [PTW11]:[1] black-box zero-knowledge lower bounds typically demonstrate certain classes of protocols (e.g., constant-round public-coin protocols), or *compositions* (e.g., concurrent or parallel) of certain classes of underlying protocols (e.g., protocols with "few" rounds, or public-coin protocols), satisfy a weaker notion of *fixed-input* resettable soundness (where soundness only needs to hold as long as the resetting prover does not get to change the statement; see [PTW11] for a formal definition) if the verifier is slightly modified to appropriately generate its randomness using a pseudorandom function (PRF): For instance, as noted in [PTW11],

*Cornell University. {chung,rafael}@cs.cornell.edu

Chung is supported in part by a Simon's Foundation postdoctoral fellowship.

Pass is supported in part by a Alfred P. Sloan Fellowship, Microsoft New Faculty Fellowship, NSF Award CNS-1217821, NSF CAREER Award CCF-0746990, NSF Award CCF-1214844, AFOSR YIP Award FA9550-10-1-0093, and DARPA and AFRL under contract FA8750-11-2- 0211. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the US Government.

[1] Although this connection was made in [PTW11], no new corollaries of this connection were provided there.

the original black-box zero-knowledge lower bound of [GK96] for constant-round public-coin protocols implicitly shows that any constant-round public-coin argument is fixed-input resettably-sound if the verifier generates its randomness by applying a PRF to the transcript. On the other hand, the black-box zero-knowledge lower-bound for parallel composition of public-coin protocols of [PTW11] shows that repeating any (not necessarily constant-round) public-coin protocol sufficiently many times in parallel and generating the verifier's randomness in each session by applying a PRF to the transcript, yields a fixed-input resettably-sound protocol. [PTW11] also note that, following the technique used in [BGGL01], if the underlying protocol also is an *argument of knowledge*, then the resulting protocol actually satisfies the standard (unbounded) notion of resettable soundness. Ostrovsky and Visconti [OV12] rely on a similar paradigm but instead rely on the black-box zero-knowledge lower bound for *concurrent* composition of 7-round protocols of Rosen [Ros00] to show that any 7-round argument of knowledge protocol can be transformed into a $poly(n)$-round resettably-sound argument of knowledge, by scheduling sufficiently many concurrent sessions of the underlying protocol in a particular pattern (described in [Ros00]) and generating the verifier's randomness in each session by applying a PRF to the transcript. Ostrovksy and Visconti [OV12] next provide a construction of a 7-round resettable-witness indistinguishable protocol ($\mathsf{r}\mathcal{WI}$) argument of knowledge based on collision-resistant hash functions by modifying a construction due to [BGGL01] to make it fit into 7 rounds; the key observation (made in [OV12]) is that (resettable) witness indistinguishability is preserved under such schedulings.

In this note, we observe that by instead relying on the recent black-box zero-knowledge lower-bound for concurrent composition of Chung, Pass and Tseng [CPT12] (which provides a sharper variant of the lower bound of Canetti, Kilian, Petrank and Rosen [CKPR01] for the case of constant-round protocols)[2], that any constant-round argument of knowledge can be transformed into an $\omega(1)$-round resettably-sound argument by appropriately scheduling concurrent sessions of the underlying protocol, and letting the verifier generate its randomness using a PRF. Since, as in [OV12], such concurrent schedulings preserve $\mathsf{r}\mathcal{WI}$ and completeness, we have the following theorem.

Theorem 1. *Assume the existence of a constant-round $\mathsf{r}\mathcal{WI}$ argument of knowledge for $\mathcal{NP}$. Then there exists an $\omega(1)$-round $\mathsf{sr}\mathcal{WI}$ argument of knowledge for $\mathcal{NP}$.*[3]

Combined with the constant-round $\mathsf{r}\mathcal{WI}$ argument of knowledge construction of [BGGL01], this yields an $\omega(1)$-round $\mathsf{sr}\mathcal{WI}$ based on collision-resistant hash functions (improving the round-complexity of the construction of Ostrovksy and Visconti [OV12]). If we instead rely on the recent constant-round $\mathsf{r}\mathcal{WI}$ argument of knowledge construction of Chung, Pass and Seth [CPS12] based on one-way functions, we get an $\omega(1)$-round $\mathsf{sr}\mathcal{WI}$ based on the minimal assumption of one-way functions.

Applications to Simulatnously Resettable Zero-knowledge Recently Deng, Goyal and Sahai [DGS09] provided a construction of a polynomial-round *simultanously resettable zero-knowledge* argument (again, see [BGGL01] for formal definition) based on the existence of 1) zaps, 2) collision-resistant hash functions, and 3) a non-interactive commitment with unique decommitments. Ostrovksy and Visconti [OV12] note that the use of zaps in the construction of [DGS09] can be replaced

[2] We could also have relied on the result of [CKPR01] but the scheduling imposed by their result would lead to a protocol with a polynomial number of rounds; the scheduling in [CPT12] is more round efficient.

[3] More generally, the existence of a $o(\frac{\log n}{\log \log n})$-round $\mathsf{r}\mathcal{WI}$ argument of knowledge for $\mathcal{NP}$ implies the existence of a $\mathrm{poly}(n)$-round $\mathsf{sr}\mathcal{WI}$ argument of knowledge for $\mathcal{NP}$.

by a sr$\mathcal{WI}$ arguments of knowledge. On the other hand, [CPS12] shows how to replace the need for collision-resistant hash-functions using one-way functions. Both these modifications are orthogonal, and can be done one after the other. As a corollary of Theorem 1, we thus get that the existence of non-interactive commitments with unique decommitments (which e.g., are implied by the existence of 1-1 one-way functions) implies the existence of a polynomial-round simultanously resettable zero-knowledge argument.

In personal communication, the authors of [DGS09] note that the need for a non-interactive commitment with a unique decommitment can be replaced with a standard commitment scheme (which can be based on any one-way functions); a revision of of [CPS12] provides an alternative variant of the [DGS09] without the need for the non-interactive commitment with a unique decommitment. A corollary of Theorem 1 and this modified DGS protocol thus yields a polynomial-round simultaneously resettable zero-knowledge argument based on one-way functions.

2 Proof of the Theorem

The proof of the Theorem 1 is a direct combination of results proven in [CPT12, PTW11, BGGL01]. Let us elaborate. We first briefly recall the construction of [CPT12] (CPT), which modularizes (and improves in terms of round-complexity) the construction of [CKPR01]. The construction proceeds in two steps:

Step 1: Parallel Repetition With Random-Terminating Verifiers Take any constant-round protocol (P, V). Repeat the protocol sufficiently many times in parallel with the follow exception: following [CKPR01, Hai09], at each round, let each of the parallel verifier terminate, *accepting*, at random with some appropriately set probability; each parallel verifier generates the randomness needed to decide whether to terminate or not, by applying a PRF to the current transcript. CPT (see "Lemma 7, generalized" in [CPT12]) shows that by appropriately fixing the number of parallel repetitions and the termination probability, the resulting protocol $(\hat{P}, \hat{V})$ is n-query fixed-input resettable sound, where n is the security parameter; q-query resettable soundness (defined in [PTW11]) means that resettable soundness holds as long as the resetting prover resets the verifier at most q times.[4]

Step 2: Amplification Through Nesting The second steps shows how to amplify fixed-input bounded-query resettable soundness by "nesting" protocol executions. More precisely, given an underlying m-round protocol $(\hat{P}, \hat{V})$ with fixed-input q-query resettable soundness, recursively define a k-level protocol (P^k, V^k) by executing $(\hat{P}, \hat{V})$ once, and in-between any two messages in $(\hat{P}, \hat{V})$ running an instance of (P^{k-1}, V^{k-1}) where V^{k-1}'s randomness is generated by applying a PRF to the transcript, and letting (P^0, V^0) be the "empty" protocol. The resulting protocol (P^k, V^k) has $O(m^k)$ rounds and CPT shows that (P^k, V^k) has fixed-input q^k-query resettable soundness; see Lemma 9 in [CPT12].

[4] CPT actually provide a more general bound that applies also to protocols with slightly sub-logarithmic number of rounds: if the protocol has m rounds, we get $O(n^{1/m})$-query fixed-input resettable soundness.

So, by combining the above two steps, if we let $k = \omega(1)$, we turn any constant-round argument (P, V) into an $\omega(1)$-round single-instance (unbounded query) resettably sound argument.[5] [6]

Finally, following the observation in [PTW11] (relying on the technique from [BGGL01]), both of the above steps actually yield a standard (as opposed to a fixed-input) resettably-sound protocol if the underlying protocol (P, V) actually is an argument of knowledge. (Technically, the reason we need the protocol to be an argument of knowledge is the following. All black-box lower-bounds consider an idealized scenario where the verifier actually generates its randomness using a truly random oracle, and then replace the random oracle with a PRF. If we consider a scenario where the resetting prover may pick statements to prove on the fly, violating the pseudoranomness property becomes tricky, since checking whether the prover actually proves a false statement cannot be done efficiently. However, as observed in [BGGL01], if the protocol is an argument of knowledge, then we can runs the "witness-extractor" algorithm to determine whether an instance is true or false, and switching from the random oracle to the PRF can be done as usual.)

References

[BGGL01] Boaz Barak, Oded Goldreich, Shafi Goldwasser, and Yehuda Lindell. Resettably-sound zero-knowledge and its applications. In *FOCS '02*, pages 116–125, 2001. 1, 2, 3, 4

[CKPR01] Ran Canetti, Joe Kilian, Erez Petrank, and Alon Rosen. Black-box concurrent zero-knowledge requires $\tilde{\omega}(\log n)$ rounds. In *STOC '01*, pages 570–579, 2001. 2, 3

[COSV12] Chongwon Cho, Rafail Ostrovsky, Alessandra Scafuro, and Ivan Visconti. Simultaneously resettable arguments of knowledge. In *TCC*, pages 530–547, 2012. 1

[CPS12] Kai-Min Chung, Rafael Pass, and Karn Seth. Non-black-box simulation from one-way functions and applications to resettable security. Manuscript in submission to STOC 2013, 2012. 2, 3

[CPT12] Kai-Min Chung, Rafael Pass, and Wei-Lung Dustin Tseng. The knowledge tightness of parallel zero-knowledge. In *TCC*, pages 512–529, 2012. 2, 3

[DGS09] Yi Deng, Vipul Goyal, and Amit Sahai. Resolving the simultaneous resettability conjecture and a new non-black-box simulation strategy. In *FOCS*, pages 251–260, 2009. 2, 3

[DN00] Cynthia Dwork and Moni Naor. Zaps and their applications. In *In 41st FOCS*, pages 283–293. IEEE, 2000. 1

[GK96] Oded Goldreich and Hugo Krawczyk. On the composition of zero-knowledge proof systems. *SIAM Journal on Computing*, 25(1):169–192, 1996. 2

[5] Technically, CPT has the verifier generate its randomness using a q^k-wise independent hash function. However, as is well-known (and made explicitly in [PTW11], see e.g., Theorem 17), the verifier used in black-box lower bounds can be made computationally efficient by using a PRF.

[6] More generally, as long as the original protocol has $m = o(\frac{\log n}{\log \log n})$ rounds, the parallel protocol obtained in Step 1 is q-query resettably sound for $q = O(n^{1/m}) = m^{\omega(1)}$. A poly$(n)$-round single-instance (unbounded query) resettably sound argument can be obtained by properly choosing k so that $q^k = n^{\omega(1)}$ while $O(m^k) = \text{poly}(n)$.

[Hai09] Iftach Haitner. A parallel repetition theorem for any interactive argument. In *FOCS*, pages 241–250, 2009. 3

[OV12] Rafail Ostrovsky and Ivan Visconti. Simultaneous resettability from collision resistance. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:164, 2012. 1, 2

[PTW11] Rafael Pass, Wei-Lung Dustin Tseng, and Douglas Wikström. On the composition of public-coin zero-knowledge protocols. *SIAM J. Comput.*, 40(6):1529–1553, 2011. 1, 2, 3, 4

[Ros00] Alon Rosen. A note on the round-complexity of concurrent zero-knowledge. In *CRYPTO*, pages 451–468, 2000. 2