On Round-Efficient Argument Systems

Hoeteck Wee[*]

Computer Science Division
UC Berkeley

Abstract. We consider the problem of constructing round-efficient public-coin argument systems, that is, interactive proof systems that are only computationally sound with a constant number of rounds. We focus on argument systems for $\mathsf{NTime}(T(n))$ where either the communication complexity or the verifier's running time is subpolynomial in $T(n)$, such as Kilian's argument system for NP [Kil92] and universal arguments [BG02,Mic00]. We begin with the observation that under standard complexity assumptions, such argument systems require at least 2 rounds. Next, we relate the existence of non-trivial 2-round argument systems to that of hard-on-average search problems in NP and that of efficient public-coin zero-knowledge arguments for NP. Finally, we show that the Fiat-Shamir paradigm [FS86] and Babai-Moran round reduction [BM88] fails to preserve computational soundness for some 3-round and 4-round argument systems.

1 Introduction

1.1 Background and Motivation

Argument systems are like interactive proof systems, except we only require computational soundness, namely that it is *computationally infeasible* (and not impossible) for a prover to convince the verifier to accept inputs not in the language. The relaxation in the soundness requirement was used to obtain protocols for NP that are perfect zero-knowledge [BCC88], or constant-round with low communication complexity [Kil92], and in both cases, seems to also be necessary [For89,GH98].

In this paper, we focus on the study of round-efficient argument systems for $\mathsf{NTime}(T(n))$ that do not necessarily satisfy any notion of secrecy, such as witness indistinguishability (WI), or zero-knowledge (although we do indulge in the occasional digression). We will however require that either the communication complexity or the verifier's running time be subpolynomial in $T(n)$ which is necessary in some applications, and to rule out the trivial one-round proof system. Argument systems of the latter type with bounded verifier's running time are a crucial component in the use of non-black-box techniques in cryptography [CGH98,Bar01,Bar04,GK03].

[*] `hoeteck@cs.berkeley.edu`. Work supported by US-Israel BSF Grant 2002246.

The study of round-efficient argument systems was initiated by Kilian [Kil92], who constructed a 4-round public-coin argument system for NP with polylogarithmic communication complexity based on a probabilistically checkable proof (PCP) system for NP. Micali [Mic00] introduced *CS Proofs*, an argument system for NEXP satisfying a relatively efficient prover condition and wherein the verifier runs in polynomial time (much less than the time needed to verify an NEXP relation). In addition, he provided a non-interactive construction in the random oracle model, which is essentially derived from scaling up and then applying the Fiat-Shamir transformation to Kilian's argument system. Barak and Goldreich [BG02] adapted Kilian's construction to obtain *universal arguments (of knowledge)*, which is a single argument system for any language in NP, and in addition, satisfies a weak proof-of-knowledge property. We stress that in a universal argument, the communication complexity and the verifier's running time is bounded by an a-priori fixed polynomial in the input length, whereas the length of the witness may be any arbitrary polynomial in the length of the input. Both of the constructions in [Kil92] and in [BG02] rely on the existence of collision-resistant function ensembles.

In this work, we initiate a systematic study of round-efficient argument systems.

- What is the minimal round complexity of argument systems with bounded communication complexity or verifier's running time?
- What are the minimal assumptions and cryptographic primitives needed for the existence of such argument systems? Are collision-resistant function ensembles really necessary? What kind of security parameters do we require from these primitives (possibly as a function of communication complexity)?
- How useful is improving the round efficiency of argument systems for the construction of round-efficient cryptographic protocols?
- Is there an efficient function ensemble with which we could securely realize the Fiat-Shamir transformation for the 4-round argument systems in [Kil92] and [BG02] (as conjectured by Micali in [Mic00])? More generally, is there some generic round reduction technique that preserves computational soundness?

We provide partial answers for all of these questions in this paper.

1.2 Our Results

We begin with the observations (possibly known in "folklore") that under standard complexity assumptions, the argument systems we are interested in require at least 2 rounds, and anything provable with such an argument system can be proven in 4 rounds. Refer to Sec 3 for the precise statements.

Necessity of hardness assumptions. We show that under standard complexity assumptions, the existence of 2-round argument systems for NP with subpolynomial communication complexity implies the existence of hard-on-average search problems in NP, that is, there is samplable distribution over CSAT instances (circuit satisfiability, namely given a circuit, decide whether the circuit has a satisfying assignment) with the property that most instances (say a constant fraction) are satisfiable, but any nonuniform polynomial-time algorithm on input a random instance from the distribution succeeds in finding a satisfying assignment for that instance with only negligible probability. Note that the existence of hard-on-average search problems in NP is possibly weaker than that of one-way functions and collision-resistant function ensembles.

Zero-knowledge and 2-round argument systems. We note that the existence of a 2-round public-coin universal argument of knowledge secure against subexponential-sized circuits yields a 4-round public-coin zero-knowledge argument for NP with negligible soundness error; this follows readily from the work of Barak et al. [Bar01,BLV04]. Such an argument system is almost round-optimal, as there is no 2-round zero-knowledge argument system for languages outside of BPP [GO94]. We also relate the existence of non-interactive zero-knowledge arguments to that 2-round witness-indistinguishable arguments for NP where the length of the common reference string, messages and proofs are subpolynomial in the input length. This follows readily from a similar characterization in [DN00].

Insecurity of the Fiat-Shamir transformation. We observe that the constructions of Goldwasser and Kalai [GK03] demonstrating the insecurity of the Fiat-Shamir transformation as applied to identification schemes also yield a 4-round argument system such that the instantiation of the Fiat-Shamir transformation with any efficiently computable function results in a 2-round protocol that is no longer computationally sound. Note that Barak's zero-knowledge argument system [Bar01] already yields a 6-round argument system for which the Fiat-Shamir transformation is insecure [DNRS03]. We also prove that there exists a 4-round universal argument of knowledge for which the Fiat-Shamir transformation fails to preserve the weak proof-of-knowledge property.

Insecurity of Babai-Moran round reduction. Babai and Moran [BM88] used a round reduction procedure to prove that any language having a constant-round public-coin interactive proof system also has a 2-round public-coin proof system. In particular, the round reduction procedure preserves soundness of proof systems. Here, we construct 3-round and 4-round argument systems for which the round reduction procedure fails to preserve computational soundness.

A note on presentation: We state our results for argument systems with either bounded communication complexity or bounded verifier's running time, depending on which of the two leads to a cleaner statement. In most cases, an analogous statement can be deduced for the other set-up. Note that a subpolynomial bound on verifier's running time must necessarily imply a subpolynomial bound on the communication complexity.

1.3 Additional Related Work

Dwork et al. [DLN$^+$04] investigated the possibility of constructing 2-round argument systems for NP with poly-logarithmic communication complexity based on a suggestion of Aiello, Bhatt, Ostrovsky and Rajagopalan, namely, to compose a PCP system for NP with computational private information retrieval scheme; their results are mostly negative. Goldreich and Håstad [GH98] proved that NP does not have constant-round public-coin proof systems with subpolynomial communication complexity, unless NP has probabilistic subexponential time algorithms. Barak et al. [BLV04] proved that the Fiat-Shamir transformation is in fact secure for proof systems under a non-standard but very plausible and concrete assumption.

2 Definitions and Setup

Due to space limitations, we refer the reader to [Gol01] to definitions of interactive protocols, zero-knowledge and witness-indistinguishability.

2.1 Interactive proofs and argument systems

For a relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$, the *language associated with* R is $L_R = \{x : \exists y \ (x,y) \in R\}$.

Definition 1 (interactive proof system). *An interactive protocol* (P, V) *is an* interactive proof system *for a language* L *if there is a relation* R *such that* $L = L_R$*, and functions* $c, s : \mathbb{N} \to [0,1]$ *such that* $1 - c(n) > s(n) + 1/poly(n)$ *and the following holds:*

- *(efficiency): the length of all the messages are polynomially-bounded, and* V *is computable in probabilistic polynomial time.*
- *(completeness): If* $(x,w) \in R$*, then* V *accepts in* $(P(w), V)(x)$ *with probability at least* $1 - c(|x|)$*,*
- *(soundness): If* $x \notin L$*, then for every* P^**,* V *accepts in* $(P^*, V)(x)$ *with probability at most* $s(|x|)$*.*

We call $c(\cdot)$ the *completeness error* and $s(\cdot)$ the *soundness error*. We say that (P, V) has *negligible error* if both c and s are negligible. We say that it has *perfect completeness* if $c = 0$. P is an *efficient prover* if $P(w)$ is computable by a probabilistic polynomial-time algorithm when $w \in R_x$. The *communication complexity* of the proof system is the total length of all the messages exchanged by both parties. For a public-coin protocol (P, V), $\mathsf{view}(V(x))$ is the set of accepting transcripts on common input x. We also use $\mathsf{AM}_{c,s}(m(n))$ to denote constant-round public-coin interactive proof systems with completeness error c, soundness s and communication complexity bounded by $m(n)$.

Definition 2 (argument system). *An* argument system (P, V) *is defined in the same way as an interactive proof system, with the following modification:*

- *The soundness condition is replaced with* computational soundness*: For every nonuniform PPT P^* and for all sufficiently long $x \notin L$, the verifier V accepts in $(P^*, V)(x)$ with probability at most $s(|x|)$.*

2.2 Universal arguments

We begin with the universal language L_U: the tuple (M, x, t) (where t is specified in binary) is in L_U is M is a non-deterministic Turing machine that accepts x within t steps. We use R_U to denote the associated relation.

Definition 3 (universal argument). *A* universal argument for $\mathsf{NTime}(T(n))$ *is an argument system (P, V) for $L_U \cap \mathsf{NTime}(T(n))$ that satisfies the following properties:*

- *(completeness by a relatively-efficient prover) For every $((M, x, t), w) \in R_u$ with $(M, x, t) \in \mathsf{NTime}(T(n))$,*
$$\Pr[V \textit{ accepts } (P(w), V)(M, x, t)] = 1$$
Furthermore, there exists a polynomial p such that the total time spent by $P(w)$, on common input (M, x, t), is at most $p(T_M(x, w)) \leq p(t)$.
- *(computational soundness) For every nonuniform PPT P^*, there exists a negligible function $\epsilon(n)$ such that for every n and every $(M, x, t) \in \{0, 1\}^n \setminus L_U$, the verifier V accepts in $(P^*, V)(M, x, t)$ with probability at most $\epsilon(n)$.*

In addition, we call (P, V) a *universal argument of knowledge* if it satisfies the weak proof-of-knowledge property [BG02]. Informally, this means that there is an efficient oracle machine (the knowledge extractor) that given oracle access to a cheating prover that convinces the verifier with inverse polynomial probability, outputs an implicit description of a witness. Both the running time and the success probability of the knowledge extractor are allowed to depend on the success probability of the cheating verifier.

Theorem 1 ([BG02]). *The existence of (standard) collision-resistant function ensembles implies the existence of a 4-round public-coin universal argument of knowledge $(P_{\mathsf{ua}}, V_{\mathsf{ua}})$ for $\mathsf{NTime}(n^{\log n})$. In addition, if the collision-resistant function ensemble is secure against circuits of size 2^{n^ϵ} for some $\epsilon > 0$, then $(P_{\mathsf{ua}}, V_{\mathsf{ua}})$ is a universal argument of knowledge against circuits of size $2^{O(n^\epsilon)}$.*

3 Simple bounds on round complexity

The results in this section are probably known in “folklore”. As pointed out in [BP04], non-interactive (one-round) arguments are equivalent to non-interactive (one-round) proof systems, since if there exists a prover message that can convince the verifier of a false statement, the non-uniform prover that has this message “hard-wired into it”. This essentially rules out non-interactive argument systems for NP with subpolynomial communication complexity.

Proposition 1. *Unless* $\mathsf{NP} \subseteq \mathsf{BPTime}(2^{n^{o(1)}})$*, non-interactive argument systems with subpolynomial communication complexity for* NP *do not exist.*

In the context of efficient-prover argument systems, we have a collapse to 4 rounds (as pointed out to us by Salil Vadhan).

Proposition 2. *Suppose there exists collision-resistant function ensembles secure against* $2^{n^{\epsilon}}$*-sized circuits for some* $\epsilon > 0$ *and a language in* E *with* $2^{\Omega(n)}$ *circuit complexity. Then, any language* L *with an efficient-prover argument system has a 4-round, public-coin, efficient-prover argument system with subpolynomial (in fact, poly-logarithmic) communication complexity.*

This follows from the observation in [BLV04] that any language with an efficient-prover argument system is contained in MA, which collapses to NP under the given derandomization assumption. The proposition then follows from Kilian's protocol [Kil92].

4 Necessity of hardness assumptions

We present hardness assumptions that are necessary for 2-round argument systems for NP with subpolynomial communication complexity. Under complexity assumptions, such a protocol cannot be a proof system [GH98]. Hence, there exists infinitely many NO instances that are merely "computationally sound", from which we may construct hard-on-average search problems in NP.

Note that we may assume the 2-round argument system has negligible soundness error, which can be achieved with $\omega(\log n)$ parallel repetitions [BIN97]. Parallel repetition blows up the communication complexity by a $\omega(\log n)$ multiplicative factor, but preserves prover's complexity, perfect completeness and public-coin property.

Lemma 1. *Suppose a promise problem* $\Pi = (\Pi_Y, \Pi_N)$ *has a 2-round public-coin argument system* (P, V) *with communication complexity* $m(n)$*, perfect completeness and negligible soundness error. Then, there exists a subset* $I \subset \Pi_N$ *such that:*

- *Ignoring inputs in* I*,* Π *has a* $\mathsf{AM}_{1,1/2}(m(n))$ *proof system. Formally,* $(\Pi_Y, \Pi_N \setminus I) \in \mathsf{AM}_{1,1/2}(m(n))$*.*
- *When* $x \in I$*, the predicate* $V(x, \cdot, \cdot)$ *induces a hard-on-average search instances in* NP*. That is, for every* $x \in I$*:*

$$\Pr_r[\exists\, y : V(x, r, y) = 1] \geq 1/2,$$

but for every n*, every* $x \in I \cap \{0,1\}^n$ *and every nonuniform PPT* A*, there exists a negligible function* $\epsilon(n)$ *such that ,*

$$\Pr_r[V(x, r, A(r)) = 1] < \epsilon(n)$$

Remark 1. Note that we may boost the probability of generating a satisfying assignment for the hard-on-average search instance to $1 - 1/\operatorname{poly}(n)$ while maintaining the same hardness parameters by taking the OR of $O(\log n)$ independent copies of $V(x, \cdot, \cdot)$.

Theorem 2. *Suppose* NP *has a 2-round public-coin argument system* (P, V) *with communication complexity* $n^{o(1)}$*, perfect completeness and negligible soundness error. Then, at least one of the following is true:*

- $\mathsf{NP} \subseteq \mathsf{AM}_{1,1/2}(n^{o(1)})$
- *There exists an infinite set* I *such that for all* $x \in I$*, the predicate* $V(x, \cdot, \cdot)$ *induces a hard-on-average search instance in* NP *(as formalized in Lemma 1). This yields an auxiliary-input samplable distribution over search instances in* NP *that is infinitely-often hard on average.*

Remark 2. The first statement is unlikely to be true as it would imply that $\mathsf{NP} \subseteq \mathsf{BPTime}(2^{n^{o(1)}})$ [GH98]. On the other hand, the latter is possibly weaker than the existence of (auxiliary input, i.o.) one-way functions. However, it does imply that there is no probabilistic polynomial-time algorithm for the circuit satisfiability problem where the number of variables is bounded by $n^{o(1)}$.

Remark 3. Salil Vadhan pointed out that if there exists a hard-on-average decision problem in NP where the instances and witnesses have length bounded by $m(n)$, then every language has a 2-round argument system with communication complexity $m(n)$. However, the argument system does not satisfy the efficient prover constraint, though the constraint is (trivially) satisfied if we consider the empty language. This shows that the conclusion in Theorem 2 is essentially the strongest we can hope for without making additional assumptions about the argument system, for instance, that it has an efficient prover, that it is WI, or that it is an argument of knowledge.

5 Zero-knowledge and 2-round argument systems

Barak et. al [BLV04] constructed a 2-round argument for NP that is zero-knowledge against cheating verifiers of bounded non-uniformity assuming the existence of a 2-round universal argument secure against $2^{n^{\epsilon}}$-sized circuits. We observe that if we strengthen the soundness requirement on the universal argument to an argument of knowledge, it follows readily from [Bar01,BLV04] that there exists a 4-round zero-knowledge argument for NP. The idea is to convert the universal argument of knowledge into a WI universal argument of knowledge (with a subexponential-time knowledge extractor) without any overhead in the number of rounds. To accomplish this, we encrypt the messages of the universal argument using a weak commitment scheme and prove correctness using a WI proof for NP [DN00].

Theorem 3 ([Bar01,BLV04]). *Suppose there exist 2-round public-coin universal argument of knowledge for* $\mathsf{NTime}(f(n))$ *for some super-polynomial*

$f : \mathbb{N} \rightarrow \mathbb{N}$, enhanced trapdoor permutations and collision-resistant function ensembles secure against 2^{n^ϵ}-sized circuits for some constant $\epsilon > 0$. Then, there exists a 4-round public-coin (auxiliary-input) zero-knowledge argument system for NP*, with perfect completeness, negligible soundness error, an efficient prover and a simulator that runs in strict polynomial time.*

Another open problem is whether there exists non-interactive zero-knowledge (NIZK) arguments or 2-round WI arguments for NP with subpolynomial communication complexity and randomness [FLS99,KP98,DLN$^+$04]. We do not know how to construct either primitive starting from an argument system for NP with subpolynomial communication complexity, but it follows from the characterization of zaps (a 2-round public-coin WI proof system for NP) in [DN00] that they are almost equivalent:

Theorem 4 ([FLS99,DN00]). *Suppose there exist one-way functions secure against 2^{n^ϵ}-sized circuits for some constant $\epsilon > 0$. Then, the following statements are equivalent:*

- *There exists a 2-round public-coin efficient-prover honest-verifier WI argument for* NP *with subpolynomial communication complexity.*
- *There exists an efficient-prover NIZK argument for* NP *where the length of the common reference string and the proof are subpolynomial in the length of the input.*

Theorem 4 is weaker than the characterization of zaps in [DN00] in that we can only deduce the existence the existence of honest-verifier WI (but not cheating-verifier WI) arguments for NP from NIZK. This is because the construction of zaps from NIZK protocols requires that the underlying NIZK protocol be a proof system in order to preserve soundness. On the other hand, we observe that honest-verifier WI is sufficient for the construction of a NIZK argument for NP.

6 Insecurity of the Fiat-Shamir transformation

Goldwasser and Kalai [GK03] proved the existence of a (secure) 3-round public-coin identification scheme for which any instantiation of the Fiat-Shamir transformation with an efficiently computable function ensemble yields an insecure signature scheme. As both the identification scheme and the signature scheme are defined in the public-key model, there is a fairly natural interpretation of the construction as obtaining a 2-round argument system from a 4-round argument system via the Fiat-Shamir transformation. The main (albeit minor) technical difference is in handling auxiliary inputs inherent to argument systems, as the set-up in [GK03] is inherently uniform (there, the variable is the security parameter, and messages to be signed are thought of as having constant size[1]).

[1] Alternatively, we may consider the forger as forging a family of uniformly computable messages of length polynomial in the security parameter, infinitely often.

We also feel that viewing the constructions of [GK03] in the context of argument systems yields a clearer and simpler presentation of their constructions and results. The following result has been independently observed by the authors of [GK03] (but was not explicitly mentioned in [GK03]):

Theorem 5 ([GK03]). *Suppose there exists (standard) collision-resistant function ensembles. Then, there exists a 4-round public-coin argument system with negligible soundness error, but for which the instantiation of the Fiat-Shamir transformation with any efficiently function ensemble yields a 2-round protocol that is not computationally sound (that is, it has a polynomial-sized cheating prover that succeeds with non-negligible probability).*

Remark 4. The cheating prover in the proof of Theorem 5 succeeds with only a non-negligible probability. It is therefore conceivable while the Fiat-Shamir paradigm does not in general preserve soundness of 4-round argument systems, the Fiat-Shamir paradigm along with parallel repetition does preserve soundness of 4-round argument systems (since parallel repetition does reduce the soundness error for 2-round argument systems to a negligible quantity [BIN97]).

We also observe that the Fiat-Shamir transformation fails to preserve the weak proof-of-knowledge property. The proof goes via a case analysis similar to that in [GK03] (except a lot simpler). Suppose the statement holds for $(P_{\mathsf{ua}}, V_{\mathsf{ua}})$; then we are done. Otherwise, we have a 2-round public-coin universal argument of knowledge which combined with Barak's non-uniform generation protocol [Bar01] yields the desired argument system.

Theorem 6. *Suppose there exists (standard) collision-resistant function ensembles. Then, there exists a 4-round public-coin universal argument of knowledge, but for which the instantiation of the Fiat-Shamir transformation with any efficiently function ensemble yields a 2-round protocol that does not satisfy the weak proof-of-knowledge property.*

7 Insecurity of Babai-Moran round reduction

We start by describing Babai-Moran round reduction. For a public-coin proof system $\Pi = (P, V)$ of at most 4 rounds, this procedure has a simple description and comprises two steps, for some parameter $k = poly(n)$. First, the residual protocol after the prover's first message is repeated k times in parallel and the new verifier accepts if all k repetitions are accepting. Next, second, the order of the prover's first message and the verifier's next message are reversed. We denote the new protocol by $\Pi^{\mathsf{rr}(k)}$. For protocols with 3 or 4 rounds, the resulting protocol has 2 rounds.

Intuitively, Babai-Moran round reduction fails to preserve computational soundness for the following reasons:

- Parallel repetition fails to reduce soundness error at an exponential rate beyond $1/\operatorname{poly}(n)$ if we require a black-box proof of security [BIN97].

– A cheating prover can gain significant advantage upon round-switching, wherein the verifier reveals his coin tosses before the prover sends his next message.

We exploit the former reasoning in our construction of the 3-round argument system, as the latter does not seem to apply in this case (made precise in Prop 3) as the first message of a 3-round argument system is "unconditionally sound". For the 4-round argument system, we exploit the latter reasoning in an essential manner so as to obtain a result that holds even with a non-black-box proof of security.

Theorem 7 (Babai-Moran round reduction).

(i) Suppose there exists collision-resistant function ensembles secure against $n^{\log n}$-sized circuits. Then, there exists a 4-round public-coin argument system with negligible soundness error for which Babai-Moran round reduction yields a 2-round argument system that is not computationally sound.

(ii) There exists a 3-round (relativized) public-coin argument system with negligible soundness error for which Babai-Moran round reduction yields a 2-round argument system that is not computationally sound if limited to a black-box proof of security.

In both constructions, the cheating prover succeeds with probability $1 - \mathrm{neg}(n)$*. This means that even upon applying parallel repetition to the resulting 2-round argument systems, we would not obtain a computationally sound protocol.*

Both constructions are for the empty language $L_\emptyset$. The 4-round protocol, specified in Fig 1, is a straight-forward simplification of the argument system in [Kil92]. For 3-round argument systems, we only rule out the case with a black-box proof of security. In this setting, it suffices to construct a relativized protocol, wherein all parties (provers, cheating provers, verifier) have oracle access to a permutation π, as shown in Fig 2. It helps to think of π as a one-way permutation, although we will require a stronger property that we only know how to prove in a relativized setting:

Lemma 2 ([GT00]). *For all sufficiently large n, there exists a permutation π on $\{0,1\}^n$ such that for all oracle circuits A of size $n^{\log n}$,*

$$\Pr[\sigma \leftarrow \{0,1\}^n;\ A^{\pi, I_\sigma}(\sigma) = y;\ \pi(y) = \sigma] < \frac{1}{n^{\log n}}$$

where I_σ is an oracle that on input $\sigma' \neq \sigma$ returns $\pi^{-1}(\sigma')$, and $\perp$ otherwise.

We note that overcoming the limitation to black-box proof of security for 3-round argument systems will require resolving a well-known open problem:

Proposition 3. *Suppose parallel repetition on 2-round argument systems can reduce the computational soundness error exponentially fast to $2^{-\mathrm{poly}(n)}$, then Babai-Moran round reduction yields a collapse of 3-round argument systems to 2-round argument systems.*

Common input: 1^n

1. (V1) verifier sends a random h from $\mathcal{H}$ (collision-resistant function ensemble).
2. (P1) prover sends a Merkle-tree commitment to B, where B is an array of $n^{\log n}$ blocks of 0^n.
3. (V2) verifier sends β at random from 1 to $n^{\log n}$ and γ at random from $\{0,1\}^n$.
4. (P2) prover decommits to $B[\beta]$.

Verification: verifier accepts if $B[\beta]$ decommits to γ.

---

1. (V1) verifier sends a random h from $\mathcal{H}$, and $\beta_1, \ldots, \beta_k$ at random from 1 to $n^{\log n}$ and $\gamma_1, \ldots, \gamma_k$ at random from $\{0,1\}^n$.
2. (P1) prover sends a Merkle-tree commitment to B, which is an array of $n^{\log n}$ blocks of 0^n, and decommits to $B[\beta_1], \ldots, B[\beta_k]$.

Verification: verifier accepts if $B[\beta_i]$ decommits to γ_i for all $i = 1, \ldots, k$.

Fig. 1. 4-round protocol $\mathit{\Pi}_1$ and 2-round protocol $\mathit{\Pi}_1^{\mathsf{rr}(k)}$ for the empty language $L_\emptyset$

Common input: 1^n, oracle access to π (a permutation on $\{0,1\}^n$)

1. (P1) prover sends $z \in \{0,1\}^n$.
2. (V1) verifier sends a random σ in $\{0,1\}^n$.
3. (P2) prover sends $y \in \{0,1\}^n$.

Verification: verifier accepts iff $\pi(y) = z \oplus \sigma$.

---

1. (V1) verifier sends random $\sigma_1, \ldots, \sigma_k$ in $\{0,1\}^n$.
2. (P1) prover sends $z, y_1, \ldots, y_k \in \{0,1\}^n$.

Verification: verifier accepts iff $\pi(y_i) = z \oplus \sigma_i$, for all $i = 1, \ldots, k$.

Fig. 2. 3-round relativized protocol $\mathit{\Pi}_2$ and 2-round protocol $\mathit{\Pi}_1^{\mathsf{rr}(k)}$ for $L_\emptyset$

8 Conclusion

We hope that the collection of observations, connections and results presented in this paper (one that is perhaps better regarded as a survey) clarifies our understanding of round-efficient argument systems and motivates further work in this area, and perhaps a resolution of the main open problem – determining the exact round complexity of non-trivial argument systems.

9 Acknowledgments

I am very grateful to Yael Tauman Kalai, Luca Trevisan and Salil Vadhan for their encouragement and insightful discussions on the subject; Salil also gave me very valuable feedback on earlier versions of this paper. I thank Kobbi Nissim for bringing [DLN$^+$04] to my attention, and the anonymous referees for helpful suggestions on the write-up.

References

[Bar01] Boaz Barak. How to go beyond the black-box simulation barrier. In *Proc. 42nd FOCS*, 2001.

[Bar04] Boaz Barak. *Non-Black-Box Techniques in Cryptography.* Ph.D., Weizmann Institute of Science, January 2004.

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 37(2):156–189, 1988.

[BG02] Boaz Barak and Oded Goldreich. Universal arguments and their applications. In *Proc. CCC '02*, 2002.

[BIN97] Mihir Bellare, Russell Impagliazzo, and Moni Naor. Does parallel repetition lower the error in computationally sound protocols? In *Proc. 38th FOCS*, 1997.

[BLV04] Boaz Barak, Yehuda Lindell, and Salil Vadhan. Lower bounds for non-black-box zero knowledge. Cryptology ePrint Archive, Report 2004/226, 2004. Extended abstract in *Proc. 44th FOCS*, 2003.

[BM88] László Babai and Shlomo Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity class. *JCSS*, 36(2):254–276, 1988.

[BP04] Boaz Barak and Rafael Pass. On the possibility of one-message weak zero-knowledge. In *Proc. 1st TCC*, 2004.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *Proc. 30th STOC*, 1998.

[DLN$^+$04] Cynthia Dwork, Michael Langberg, Moni Naor, Kobbi Nissim, and Omer Reingold. Succint proofs for NP and spooky interactions. manuscript, 2004.

[DN00] Cynthia Dwork and Moni Naor. Zaps and their applications. In *Proc. 41st FOCS*, 2000.

[DNRS03] Cynthia Dwork, Moni Naor, Omer Reingold, and Larry Stockmeyer. Magic functions. *JACM*, 50(6):852–921, 2003.

[FLS99] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. *SICOMP*, 29(1):1–28, 1999.

[For89] Lance Fortnow. The complexity of perfect zero-knowledge. *Advances in Computing Research*, 5:429–442, 1989.

[FS86] Amos Fiat and Adi Shamir. How to prove to yourself: practical solutions to identification and signature problems. In *Proc. Crypto '86*, 1986.

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

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *Proc. 44th FOCS*, 2003.

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

[Gol01] Oded Goldreich. *Foundations of Cryptography: Basic Tools.* Cambridge University Press, 2001.

[GT00] Rosario Gennaro and Luca Trevisan. Lower bounds on efficiency of generic cryptographic constructions. In *Proc. 41st FOCS*, 2000.

[Kil92] Joe Kilian. A note on efficient zero-knowledge proofs and arguments. In *Proc. 24th STOC*, 1992.

[KP98] Joe Kilian and Erez Petrank. An efficient noninteractive zero-knowledge proof system for NP with general assumptions. *J. Cryptology*, 11(1):1–27, 1998.

[Mic00] Silvio Micali. Computationally sound proofs. *SICOMP*, 30(4):1253–1298, 2000.