1992

H. Shin

A brief survey of zero-knowledge proofs

Computer Science/Department of Algorithmics and Architecture Report CS-R9232 August

CWI is the research institute of the Stichting Mathematisch Centrum, which was founded on February 11, 1946, as a non-profit institution aiming at the promotion of mathematics, computer science, and their applications. It is sponsored by the Dutch Government through the Netherlands organization for scientific research (NWO).

A Brief Survey of Zero-Knowledge Proofs

Hyunyong Shin
CWI
P.O. BOX 4079, 1009 AB
Amsterdam, The Netherlands
AND
Department of Mathematics Education The 3rd College Korea National University of Education 363-791, Korea

Abstract. In cryptography, the notion of zero-knowledge is important. It is also related to complexity theory. In this paper we briefly survey the zero-knowledge proofs in the literature.

1980 Mathematics Subject Classification: 68Q05, 68Q15.
Keywords and Phrases: interactive proofs, zero-knowledge, cryptography, complexity theory.
Note: This work was partially supported by NWO project ALADDIN and Korea Science and Engineering Foundation, and will appear elsewhere.

1 Interactive Proof Systems For Languages

In the 17th Annual ACM Symposium on Theory of Computing (1985), two related papers were presented. One was 'The Knowledge Complexity of Interactive Proof Systems' by S. Goldwasser, S. Micali, and C. Rackoff [GMR1] and the other was 'Trading Group Theory for Randomness' by L. Babai [B].

In [GMR1], the authors formulated 'interactive proof systems' as a tool for developing cryptographic protocols. An interactive proof system involves two parties known as the prover and the verifier, and a language L. The prover is allowed unlimited computing power, whereas the verifier is restricted to feasible computations (such as probabilistic polynomial time). The purpose of the interactive proof system is for the prover to convince the verifier about the membership of strings in the language L. To reach this goal, the two parties are allowed to exchange messages and toss private coins. At the end of the interaction, the verifier will either accept or reject the prover's claim. Two properties are required of the interactive proof system: it must be complete, meaning that if $x \in L$ and if both parties follow their prescribed protocols then the verifier will accept with overwhelming probability, and it must be sound, meaning that if $x \notin L$, and if the verifier follows his protocol, then he will reject with overwhelming probability even if the prover deviates arbitrarily from her protocol. We will denote the class of languages having the interactive proof systems by IP.

Note that in [GMS], Goldreich, Mansour, and Sipser considered the 'perfect completeness'. They showed that any language that has an $f(n)$-round interactive proof system has a $(f(n)+1)$-round interactive proof system such that if $x \in L$ then the verifier always accepts. They also considered the 'perfect soundness'. It was shown that only NP languages have interactive proof system such that the verifier always rejects if $x \notin L$.

In [GMR1], they introduced the interesting notions of zero-knowledge[1] and knowledge complexity[2].

[1]The original formulation of zero-knowledge turned out not to be closed under sequential composition. More stronger formulations of zero-knowledge (e.g. black-box simulation) were introduced. See [GK] or [O].

[2]The formalization of the 'amount of knowledge' (in case it is not zero) that appeared in [GMR1] was omitted

Report CS-R9232
ISSN 0169-118X
CWI
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

They also gave examples of zero-knowledge proof systems for the languages, Quadratic Residuosity[3] and Quadratic Non-Residuosity. These are the first examples of zero-knowledge proofs for languages not known to be efficiently recognizable.

In [B], trying to get a complexity class just above NP, Babai introduced the 'Arthur - Merlin games'[4]. These games constitute a class of languages that we will denote by AM.

These two models are probabilistic extensions of the complexity class NP. The key difference between them is in the way of coin tossing of the verifier. Babai required that coins flipped by the verifier be public. In other words, they are known to the prover. So the verifier is only to supply random bits to the prover. At the end of the interaction, the verifier decides whether he is convinced that a particular string is in the language. On the other hand, in the model of Goldwasser, Micali, and Rackoff, the verifier's coins are private[5].

These pioneering works stimulated many exciting cryptographic and complexity theoretic results.

Important subsequent work was done by O. Goldreich, S. Micali, and A. Wigderson in [GMW]. They demonstrated zero-knowledge interactive proofs for the languages of Graph Isomorphism[6], Graph Non-Isomorphism[7], and Graph 3-Colourability. By that time, zero-knowledge proofs were known only for some number theoretic languages in $NP \cap co-NP$. The existence of an interactive proof for Graph Non-Isomorphism is interesting, since Graph Non-Isomorphism is not known to be in NP. Using the NP-completeness of Graph 3-Colourability, they proved that every NP language has a zero-knowledge interactive proof system[8] under the assumption of existence of secure encryptions. In that paper, they claimed that if there exists a secure encryption, then every language which has an interactive proof system, has a zero-knowledge one. In [BGGHKRM], this was formally proved.

In 1987, R. Boppana, J. Hastad, and S. Zachos [BHZ] showed that if $co-NP$ is contained in AM, then the polynomial-time hierarchy is contained in $AM \subseteq \Pi_2^P$[9]. Also in 1987, L. Fortnow [F] observed that if a language L has a perfect or statistically zero-knowledge interactive proof system, then its complement $\bar{L}$ has a single round interactive proof system[10]. As easy consequences of above two results, we can prove that if the Graph Isomorphism problem is NP-complete, then the polynomial-time hierarchy collapses, and the same conclusion holds if Graph 3-Colourability had a perfect or statistically zero-knowledge proof system.

From a structural complexity point of view, one of the most natural questions about IP was: Characterize exactly the class of problems that can be recognized by an interactive proof system. It is clear that $NP \subseteq IP$. As mentioned before, Goldreich, Micali, and Wigderson gave an example of a problem in IP not known to be in NP: Graph Non-Isomorphism. But the final solution to this question was provided by Lund, Fortnow, Karloff, and Nisan [LFKN] and Shamir [S] in December in

---

from the later version of this paper [GMR2]. In [GP], the authors present several alternative definitions of knowledge complexity.

[3]This proof system is perfect zero-knowledge of unbounded rounds of message exchanges.

[4]Papadimitriou [Pa] introduced the term 'games against nature' to describe complexity classes arising from polynomially bounded games against an indifferent, randomizing adversary. Arthur-Merlin games are particular games against nature, the crucial restriction being the condition that the winning chances are always bounded away from 1/2.

[5]Goldwasser and Sipser [GS] proved that for language recognition the two models are equivalent. Thus from a language recognition viewpoint, the public coin model suffices, even though interactive proofs are simpler to construct using hidden coins.

[6]The Graph Isomorphism problem, trivially in NP, is not known to be in $co-NP$, and is believed not to be NP-complete. This proof system for Graph Isomorphism is perfect zero-knowledge.

[7]Note that the existence of an interactive proof system for the language L does not imply its existence for the complement of L. This proof system for Graph Non-Isomorphism is constant-round and perfect zero-knowledge.

[8]This is a computationally zero-knowledge proof system.

[9]In [FoSi], Fortnow and Sipser conjectured that $co-NP$-complete problems do not have interactive proof systems. In other words, they believed that the class IP of languages accepted by interactive proofs is not much larger than NP. But later it was proved that the interactive proof systems have far greater power than originally believed.

[10]A perfect zero-knowledge proof of Graph Isomorphism was presented in [GMW]. Fortnow's construction converts this perfect zero-knowledge protocol to an interactive protocol for Graph Non-Isomorphism which is identical to the protocol described in [GMW]. Also note that Aiello and Hastad [AH] proved a complementary result of this fact. That is, they proved that if L admits a perfect or statistically zero-knowledge proof then L can also be recognized by a single round interactive proof.

1989. In fact, Lund, Fortnow, Karloff, and Nisan proved that the entire polynomial-time hierarchy is included in IP[11]. They achieved this result by giving an interactive protocol for the permanent, a well-known $\#P$-complete problem [V]. Right after this result, Shamir settled the question of characterizing IP. Using techniques similar to those of Lund, Fortnow, Karloff, and Nisan, he proved that $IP = PSPACE$ [S]. This fact demonstrated the unexpectedly immense power of randomization and interaction in efficient provability.

It was an intriguing question that the parallel versions of the protocols in [GMR1] and [GMW] are still zero-knowledge. Trying to answer this question, Goldreich and Krawczyk [GK] proved that only BPP languages have 3-move interactive proofs which are black-box simulation[12] zero-knowledge. Since the parallel versions of the above examples are 3-move interactive proofs it follows that these interactive proofs cannot be proven zero-knowledge using black-box simulation zero-knowledge, unless the corresponding languages are in BPP. The proof in [GK] uses the infinite computing power of the prover. But in [FS3], Feige and Shamir showed that zero-knowledge is not preserved under parallel composition even if the provers are only polynomially bounded.

It is not plausible that the result in [GK] could be extended to 4-move interactive proofs since such proofs are known for languages believed to be outside BPP[13].

On the other hand, for Quadratic Residuosity and Graph Isomorphism, Bellare, Micali, and Ostrovsky exhibited perfect[14] zero-knowledge proofs that require 5 moves[15] and no unproven assumptions [BMO]. In fact, more generally, they showed that any random self-reducible language [AL, TW] has a 5-move perfect zero-knowledge interactive proof.

2 Interactive Proofs For Decision Problems

Extending the notion of the interactive proof system for a language, Galil, Haber, and Yung introduced 'interactive proofs for decision problems' [GHY1, GHY2]. In fact, they extended the ability of interactive proof system from confirming that a given string x is in a language L to deciding whether $x \in L$ or $x \notin L$. Even though they use 'minimum-knowledge'[16] instead of 'zero-knowledge', they are essentially the same.

They gave a nontrivial example of a language L[17] so that both L and its complement $\overline{L}$ have minimum-knowledge interactive proof systems for confirming membership. In other words, they use the same protocol for both the proof of membership in L and the proof of nonmembership of L which releases no more knowledge than the value of the membership bit[18]. Furthermore, by following the protocol, the prover demonstrates to the verifier either that $x \in L$ or that $x \notin L$ in such a way that the two cases are indistinguishable to an eavesdropping third party that is limited to feasible computations. They call this property 'result-indistinguishability'[19]. Also they proved that the concatenation of two minimum-knowledge protocols is minimum-knowledge.

---

[11] In fact, they showed that every language in $BPP^{\#P}$ has an interactive proof system. Together with Toda's result that $P^{\#P}$ contains all the languages of the polynomial-time hierarchy [T], the above theorem implies that $PH \subseteq IP$. So, unless PH collapses, there are interactive proof systems that can not be converted into bounded-round protocols.

[12] All known zero-knowledge protocols are also black-box simulation zero-knowledge. For details, see [GK].

[13] The protocols for Quadratic Non-Residuosity [GMR1] and Graph Non-Isomorphism [GMW] are examples of this.

[14] Because of Fortnow's result, their protocol can not be extended to NP-complete problems unless the polynomial-time hierarchy collapses.

[15] By that time the known proofs for both languages required an unbounded number of rounds.

[16] They also defined 'perfect minimum-knowledge'.

[17] This language is in $NP \cap co - NP$. In [IY], Impagliazzo and Yung provide a minimum-knowledge interactive proof for any language in IP.

[18] Their protocol is perfect minimum-knowledge and perfect result-indistinguishable and can be converted into a constant round protocol. Also note that the proof that their protocol is minimum-knowledge with respect to the verifier and result-indistinguishable with respect to the eavesdropper does not rely on unproven assumptions about the complexity of a number-theoretic problem.

[19] All messages are sent in the clear. This property with minimum-knowledgeness enables one to define a cryptosystem in which each user receives exactly the knowledge he is supposed to receive, and nothing else.

3 Interactive Proofs Of Knowledge

In [C], Chaum obtained a result similar to those of [GMW], but under a very different model which emphasizes the unconditional privacy of the prover's secret information even if the verifier has unlimited computing power. Independently, Brassard and Crépeau [BC] considered a model in which all parties involved are assumed to have reasonable computing power, and they also obtained a protocol unconditionally secure for the prover. In these models, the prover is not allowed to be infinitely powerful. Therefore, these protocols are not proof systems in the terminology of [GMR1]. This model is often called an 'argument'. Recently, Chaum proposed to call the GMR-model as 'statistically convincing' protocol and the latter model as 'computationally convincing' protocol [B2]. In [BCC], the authors presented perfect zero-knowledge, computationally convincing protocols for all NP-problems under the Certified Discrete Log Assumption.

Eventually Tompa and Woll [TW] and Feige, Fiat, and Shamir [FFS] independently proposed some formalizations of 'interactive proofs of knowledge'. The two definitions differ in some technical ways, but the concepts are the same. In particular, Feige, Fiat, and Shamir observed that in the GMR-model the prover reveals one bit of knowledge to the verifier (namely that a string is in a language). But in their model the prover's goal is not to prove that x belongs to L, but to prove that he knows the status of x with respect to L[20]. They demonstrated the advantage of their model by proposing an efficient identification scheme.

Even though the FFS-scheme is very efficient, their scheme lacks in generality. Their scheme is for the purpose of identification, and is not designed to handle NP-complete problems. On the other hand, the more general protocols of [BC, BCC] require an unbounded number of rounds. So one natural question was: To what extend can we combine generality and efficiency? For this question, Brassard, Crépeau, and Yung [BCY] proved that any NP statement can be handled by a 3-round perfect zero-knowledge, computationally convincing protocol.

Shortly after this, Feige and Shamir introduced a different solution to the same problem [FS1]. They constructed 2-round zero-knowledge proofs of knowledge for any NP language under the assumption that one way functions exist. They also remarked that under the stronger Certified Discrete Log Assumption, their protocol is perfect zero-knowledge.

4 Proofs Of Computational Power

In [Y], Yung tried to extend 'proof of knowledge' to a proof which demonstrates more than just possession of a witness to some computation, but rather possession of algorithmic power. And he gave a perfect zero-knowledge proof of the computational power to factor. He also remarked that if we allow the protocols to be computationally zero-knowledge, we can prove more problems. In a subsequent work by Okamoto, Chaum, and Ohta, a more efficient and constant round zero-knowledge proof[21] of computational power for some problems was given assuming the existence of a one way function [OCO]. They also introduced a formal definition of interactive proofs of computational power.

5 Multi-Prover Interactive Proofs

Many cryptographic systems have been developed based on some assumptions, like the existence of one way functions. Trying to remove such assumptions, Ben-Or, Goldwasser, Kilian, and Wigderson [BGKW] introduced a new model of generalized interactive proofs[22]. They call this new model the multi-prover interactive proofs. Then they proved that all NP languages have perfect zero-knowledge proof systems in their model[23], without making any intractability assumption.

[20] This model restricts the prover's proofs of knowledge to problems in NP.

[21] The perfectness, statisticalness, or computationalness depends on the assumptions.

[22] In [FST], Feige, Shamir, and Tennenholtz modeled a model similar to this, called a 'multi-oracle model'. Based on the assumption that one of the oracles is trusted, they showed that $PSPACE$ languages can be recognized in a 2-oracle model.

[23] They exhibited a sequential two-prover protocol and remarked that the parallel execution of their protocol is also a perfect zero-knowledge proof system with a single round under a weak definition which requires only a constant

This generalized interactive proof model consists of two computationally unbounded and untrusted provers who jointly agree on a strategy to convince the verifier of the truth of an assertion and then engage in a polynomial number of message exchanges with the verifier. To believe the validity of the assertion, the prover must make sure that the two provers can not communicate with each other during the course of the proof process. Thus the complexity assumptions made in previous work have been traded for a physical separation between the two provers.

The main feature of their model is that the verifier can check its interactions with the provers against each other. They also showed that any language which can be recognized in their extended model can be recognized in perfect zero-knowledge making no intractability assumptions. Furthermore, it was shown that adding more provers than two adds no more power to the model. Along the same lines of Goldreich, Mansour, and Sipser [GMS], they showed any two-prover system has an equivalent system that accepts with probability one for strings in the language.

Using this model, Ben-Or, Goldwasser, and Kilian [BGK] presented two efficient identification schemes, where the verifier (e.g. the bank) interacts with two untrusted provers (e.g. two bank identification cards) who have jointly agreed on a strategy to convince the verifier of their identity.

As mentioned before, it is now known that $IP = PSPACE$. A natural question is how powerful the multi-prover system is. This question was answered by Babai, Fortnow, and Lund [BFL] in 1990. They showed that $MIP = NEXP$, where MIP is the class of languages that have multi-prover interactive proof systems. From this fact, it follows that polynomial-time intractable languages may admit efficient proof systems since $NEXP \neq P$ [SFM].

Since Ben-Or, Goldwasser, Kilian, and Wigderson showed that all languages that have multi-prover proof systems have perfect zero-knowledge ones with no cryptographic assumption, all languages of $NEXP$ have perfect zero-knowledge multi-prover proof systems.

6 Instance-Hiding Proof Systems

In [AFK], Abadi, Feigenbaum, and Kilian considered the instance-hiding schemes for a function f[24]. The protocol allows the verifier V to obtain the value of $f(x)$ without revealing to the prover any information about x (other than its length). But in this protocol, V does not necessarily obtain any evidence of the correctness of this value. That is why the provers are called 'oracles'. Even though V does not entrust any information about x to the provers, but he must trust the provers to behave correctly.

Later, Beaver, Feigenbaum, and Shoup [BFS] introduced the notion of an instance-hiding proof system for a function f. Note that in this model, there are multiple provers. Roughly speaking, an instance-hiding proof system for a function f is a protocol in which a polynomial-time verifier is convinced of the value of $f(x)$ but does not reveal the input to the provers. Thus the verifier need not entrust any information about x to the provers, nor need he trust the provers to behave correctly.

In an instance-hiding proof system for a function f, the provers do not know the input x (except its length). Thus they can not hope to prevent a verifier from learning $f(x')$ instead of $f(x)$, where $|x'| = |x|$. So, it is natural to define the notion of zero-knowledge for instance-hiding proof system which captures the intuitive idea that the verifier, even a misbehaving one, learns the value of f at exactly one input of length n and nothing else. In other words, the provers learn nothing about x, and the verifier learns nothing but the value of $f(x)$.

In [BFS], it was shown that any instance-hiding proof system can be made zero-knowledge[25]. In

probability of cheating. Later, Lapidot and Shamir [LS2] showed that under the stronger definition which requires a negligible probability of cheating every problem in NP has a one-round two-prover protocol which is perfectly zero-knowledge under no cryptographic assumption. This fact was extended to $PSPACE$ and $NEXP$ in [CCL] and [LS3], respectively.

[24]They showed that no NP-hard function has a one-oracle instance-hiding scheme that leaks at most $|x|$, unless the polynomial-time hierarchy collapses. In [BF], Beaver and Feigenbaum proved that all functions allow multi-oracle instance-hiding schemes.

[25]The constant-roundness is not considered.

fact, it was proved that if a Boolean function f is the characteristic function of a language in $NEXP \cap co-NEXP$[26], f has a perfect zero-knowledge instance-hiding proof system[27]. A main open problem in this model is concerned with the number of provers[28].

For a more detailed discussion on this scheme, the reader is referred to [B1].

7 Interactive Proofs With Space Bounded Verifiers

In sections 4 and 6, we considered some variations of the GMR-model in which the nature of the provers is altered. We may also consider the variations in which the nature of the verifiers is altered. Such a model was first considered by Condon [Co]. In that paper, Condon described 'probabilistic game automata' that are the natural space bounded analogues of Arthur-Merlin games and interactive proof systems[29]. It was also shown that if the protocols are allowed to run for arbitrarily many rounds, exponential-time languages may be proven to a log-space verifier. Eventually a more realistic model was considered.

In [K], Kilian considered a model in which protocols are polynomially bounded, both in the number of rounds of communication, and in the number of computational steps allowed for the verifier. He also defined the zero-knowledgeness[30] for his model (called 'language-recognition zero-knowledge') and showed that anything provable in his model can be proved in language-recognition zero-knowledge. In [FS2], Feige and Shamir investigated the power of space bounded verifiers in models with many provers[31].

8 Non-Interactive Proof Systems

The main ingredients of zero-knowledge proof systems are interaction, hidden coins, and computational difficulty. One may ask if all of them are really essential for the zero-knowledge proofs. In [BFM], Blum, Feldman, and Micali considered this question and introduced the interesting concept of non-interactive zero-knowledge proofs. Roughly speaking, they showed that only computational difficulty is essential. To be more precise, they proved that if the prover and the verifier share a common random string, the prover can non-interactively and yet in zero-knowledge convince the verifier of the validity of any theorem under the assumption that it is hard to distinguish products of 2 primes from products of 3 primes[32].

Using Graph 3-Colourability, an NP-complete language, they proved the existence of bounded[33] non-interactive zero-knowledge proof systems for all NP-languages. They used their result to construct a public key cryptosystem secure against chosen ciphertext attack[34].

Two natural problems were proposed; whether many provers could share the same random string, and whether it is possible to implement non-interactive zero-knowledge with a general complexity assumption[35].

---

[26] Note that if a Boolean function f has an instance-hiding proof system, then f is the characteristic function of a language in $NEXP \cap co-NEXP$.

[27] It is claimed that Feigenbaum and Ostrovsky have characterized the functions which have one-oracle instance-hiding proof systems. They also claimed that the existence of a one way function implies that one-oracle instance-hiding systems can be made computational zero-knowledge.

[28] The best known upper bound for number of provers is $n/logn$, where n is the input length.

[29] One of the interesting results in [Co] is that the private coin of the verifier adds power to space bounded probabilistic games. This must be contrasted with the fact that Arthur-Merlin games and interactive proof systems recognize the same class of languages [GS].

[30] In [DS], they defined a reasonable notion of zero-knowledge, which models the GMR-notion of computational zero-knowledge.

[31] For further results on the power of space bounded interactive proofs, see [CL] and [DS].

[32] This computational assumption is weakened in [DMP1] where the assumption is that Quadratic Residuosity is hard. See also [BDMP].

[33] Using a random string, the prover can prove in zero-knowledge only a single theorem.

[34] Rabin's scheme, whose breaking for a passive adversary is as hard as factoring, is easily vulnerable to this attack.

[35] To try to solve this problem, De Santis, Micali, and Persiano [DMP2] proposed a modified model called non-interactive zero-knowledge with preprocessing. They proved that the existence of any secure probabilistic encryption

Important progress for these questions was made by Lapidot and Shamir. In [LS1], they constructed publicly verifiable[36] non-interactive zero-knowledge proof for any NP-statement under the general assumption that one way permutations exist. If the prover is polynomially bounded then their scheme is based on the stronger assumption that trapdoor permutations exist[37]. However, their scheme is a bounded non-interactive zero-knowledge proof system.

In [FLS], Feige, Lapidot, and Shamir have shown how to transform any bounded non-interactive zero-knowledge proof system with polynomial-time provers into a general non-interactive zero-knowledge proof system in which polynomially many independent provers can share the same random string and use it to prove polynomially many statements of polynomial length. The transformation is based on the general assumption that one way functions exist.

On the other hand, in [D] Damgård proved an arbitrary NP-statement non-interactively without using Karp-reductions to 3-SAT or Graph Hamiltonicity. Also he presented a statistical[38] zero-knowledge non-interactive computationally convincing protocol with preprocessing for any NP-statement under the existence assumption of collision intractable hash functions. It is still open to construct a perfect (or statistical) zero-knowledge computationally convincing protocol in the shared string model for an NP-complete problem.

The non-interactive zero-knowledge proof systems have become an important primitive for cryptographic protocols, with applications such as signature schemes and encryption schemes secure against chosen ciphertext attack. Using non-interactive zero-knowledge proof systems, Bellare and Goldwasser provided a simple new paradigm for digital signing[39] and message authentication secure against chosen message attack [BG]. In [RS], Rackoff and Simon proposed a non-interactive public key cryptosystem based on non-interactive zero-knowledge proof of knowledge and showed that it is secure against chosen ciphertext attack[40].

In [DP], it was shown that after a constant-round preprocessing stage, it is possible to give any polynomial number of non-interactive proofs of knowledge for any NP-language. Their proof system is based on the existence of one way functions and non-interactive zero-knowledge proof system for language membership[41].

9 Remarks

Besides the proofs mentioned in this article, there might be other types of zero-knowledge proofs (e.g. interactive proofs for promise problems [GKu]). Also it is quite possible that the author is ignorant of some significant work concerned with zero-knowledge proofs.

Acknowledgements

This work was carried out while the author was visiting CWI, Amsterdam, the Netherlands.The author greatly thanks CWI for the hospitality and the perfect academic atmosphere. Thanks also to Paul

scheme is enough for their modified model.

[36] The non-interactive proofs previously presented are not publicly verifiable and all of them are directed to a particular verifier.

[37] In [NY], Naor and Yung showed how to construct a public key cryptosystem which is provably secure against chosen ciphertext attack, given a public key cryptosystem which is secure against passive eavesdropping and a non-interactive zero-knowledge proof system in the shared string model. Using their result with those of Lapidot and Shamir implies that under the general assumption that trapdoor permutations exist, there exists a public key cryptosystem which is provably secure against chosen ciphertext attack.

[38] This can be perfect under the Certified Discrete Log Assumption.

[39] For digital signatures the non-interactive zero-knowledge proofs are required to be publicly verifiable; that is, they should be checkable by anyone rather than a particular verifier.

[40] Galil, Haber and Yung [GHY3] showed zero-knowledge interactive proofs of knowledge, first defined by Fiat, Feige, and Shamir, could be used to make a public key cryptosystem secure against chosen ciphertext attack.

[41] As an application of their protocol, they presented a protocol for electronic cash which is provably secure under general complexity assumptions.

Vitányi, Evangelos Kranakis, Eugene van Heijst, John Tromp, and Stefan Brands for their significant help on this work.

REFERENCES

[AFK] Abadi, M., Feigenbaum, J., and Kilian, J., 'On hiding information from an oracle', J. Comput. System Sci., 39, 1989, pp. 21-59.

[AH] Aiello, W. and Hastad, J., 'Perfect zero-knowledge languages can be recognized in two rounds', Proc. 28th IEEE Symposium on Foundation of Computer Science, 1987, pp. 439-448.

[AL] Angluin, D. and Lichtenstein, D., 'Provably security of cryptosystems: a survey', YALEU, DCS, TR-288, Yale University, 1983.

[B] Babai, L., 'Trading group theory for randomness', Proc. 17th Annual ACM Symposium on the Theory of Computing, 1985, pp. 421-429.

[BFL] Babai, L., Fortnow, L., and Lund, C., 'Non-deterministic exponential time has two-prover interactive protocols', Proc. 31st IEEE Symposium on Foundation of Computer Science, 1990, pp. 16-25.

[BF] Beaver, D. and Feigenbaum, J., 'Hiding information from several oracles', Harvard University, TR-10-89, 1989.

[BFS] Beaver, D., Feigenbaum, J., and Shoup, V., 'Hiding instances in zero-knowledge proof systems', Proc. CRYPTO 90, 1990, pp. 326-338.

[BG] Bellare, M. and Goldwasser, S., 'New paradigms for digital signatures and message authentication based on non-interactive zero-knowledge', Proc. CRYPTO 89, 1989, pp. 194-211.

[BMO] Bellare, M., Micali, M., and Ostrovsky,R., 'Perfect zero-knowledge in constant round', Proc. 22nd ACM Symposium on Theory of Computing, 1990, pp. 482-493.

[BGGHKRM] Ben-Or, M., Goldreich, O., Goldwasser, S., Hastad, J., Kilian, J., Rogaway, P., and Micali, S., 'Everything provable is provable in Zero-knowledge', Proc. CRYPTO 88, 1988, pp. 37-56.

[BGK] Ben-Or, M., Goldwasser, S., and Kilian, J., 'Efficient identification schemes using two prover interactive proofs', Proc. CRYPTO 89, 1989, pp. 498-506.

[BGKW] Ben-Or, M., Goldwasser, S., Kilian, J., and Wigderson, A., 'Multi-prover interactive proofs: How to remove intractability assumptions', Proc. 20th Annual ACM Symposium on the Theory of Computing, 1988, pp. 113-131.

[BDMP] Blum, M., De Santis, A., Micali, S., and Persiano, G., 'Non-interactive zero-knowledge', SIAM Journal on Computing, 20, 6, 1991, pp. 1084-1118.

[BFM] Blum, M., Feldman, P., and Micali, S., 'Non-interactive zero-knowledge and its applications', Proc. 20th Annual ACM Symposium on the Theory of Computing, 1988, pp. 103-112.

[BHZ] Boppana, R., Hastad, J., and Zachos, S., 'Does $co - NP$ have short interactive proofs?', Information Processing Letters, 25, 1987, pp. 127-132.

[BLP] Boyar, J., Lund, C., and Peralta, R., 'On the communication complexity of zero-knowledge', to appear.

[B1] Brassard, G., Cryptology column: Hiding information from oracles, Sigact News, 21, 1990, pp. 5-11.

[B2] Brassard, G., Cryptology column: How convincing is your protocols?, Sigact News, 22, 1991, pp. 5-12.

[BCC] Brassard, G., Chaum, D., and Crépeau, C., 'Minimum disclosure proofs of knowledge', J. Comput. System Sci., Vol.37, No.2, 1988, pp. 156-189.

[BC] Brassard, G. and Crépeau, C., 'Non-transitive transfer of confidence: a perfect zero-knowledge interactive protocol for SAT and beyond', Proc. 27th IEEE Symposium on Foundation of Computer Science, 1986, pp. 188-195.

[BCLL] Brassard, G., Crépeau, C., Laplante, S., and Légar, C., 'Computationally convincing proofs of knowledge', Proc. 8th Symposium on Theoretical Aspects of Computer Science, 1991, pp. 251-262.

[BCY] Brassard, G., Crépeau, C., and Yung. M., 'Constant-round perfect zero-knowledge computationally convincing protocols', Theoretical Computer Science, 84, 1991, pp. 23-52.

[CCL] Cai, J., Condon, A., and Lipton, R., '$PSPACE$ is provable by two provers in one round', Proc. 6th Structure in Complexity Theory, 1991, pp. 110-115.

[C] Chaum, D., 'Demonstrating that a public predicate can be satisfied without revealing any information about how', Proc. CRYPTO 86, 1986, pp. 195-199.

[Co] Condon, A., 'Bounded space probabilistic games', Proc. 3rd Structure in Complexity Theory, 1988, pp. 162-174.

[CL] Condon, A. and Lipton, R., 'On the complexity of space bounded interactive proofs', Proc. 30th IEEE Symposium on Foundation of Computer Science, 1989, pp. 462-467.

[D] Damgård, I., 'Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing', Extended Abstracts, EUROCRYPT 92, 1992, pp. 313-326.

[DMP1] De Santis, A., Micali, S., and Persiano, G., 'Non-interactive zero-knowledge proof systems', Proc. CRYPTO 87, 1987, pp. 52-72.

[DMP2] De Santis, A., Micali, S., and Persiano, G., 'Non-interactive zero-knowledge with preprocessing', Proc. CRYPTO 88, 1988, pp. 269-282.

[DP] De Santis, A. and Persiano, G., 'Communication efficient zero-knowledge proofs of knowledge (With applications to electronic cash)', Proc. 9th Symposium on Theoretical Aspects of Computer Science, 1992, pp. 449-460.

[DS] Dwork, C. and Stockmeyer, L., 'On the power of 2-way probabilistic finite state automata', Tech. Report RJ 6262, IBM Research Division, Almaden Research Center, San Jose, CA, 1988.

[FFS] Feige, U., Fiat, A., and Shamir, A., 'Zero-knowledge proofs of identity', J. Cryptology, Vol.1, 1988, pp. 77-94.

[FLS] Feige, U., Lapidot, D. and Shamir, A., 'Multiple non-interactive zero-knowledge proofs based on a single random string', Proc. 31st IEEE Symposium on Foundation of Computer Science, 1990, pp. 308-317.

[FS1] Feige, U. and Shamir, A., 'Zero-knowledge proofs of knowledge in two rounds', Proc. CRYPTO 89, 1989, pp. 526-544.

[FS2] Feige, U. and Shamir, A., 'Multi-oracle interactive protocols with space bounded verifiers', Proc. 30th IEEE Symposium on Foundation of Computer Science, 1989, pp. 158-164.

[FS3] Feige, U. and Shamir, A., 'Witness indistinguishable and witness hiding protocols', Proc. 22nd Annual ACM Symposium on the Theory of Computing, 1990, pp. 416-426.

[FST] Feige, U., Shamir, A., and Tennenholtz, M., 'The noisy oracle problem', Proc. CRYPTO 88, 1988, pp. 284-296.

[F] Fortnow, L., 'The complexity of perfect zero-knowledge', Proc. 19th Annual ACM Symposium on the Theory of Computing, 1987, pp. 204-209.

[FRS] Fortnow, L., Rompel, J., and Sipser, M., 'On the power multi-prover interactive protocols', Proc. 3rd Structure in Complexity Theory, 1988, pp. 156-161.

[FoSi] Fortnow, L. and Sipser, M.,'Are there interactive protocols for $co-NP$ languages?', Information Processing Letters, 28, 1988, pp. 249-251.

[GHY1] Galil, Z., Haber, S., and Yung, M., 'A private interactive test of a Boolean predicate and minimum-knowledge public key cryptosystem', Proc. 26th IEEE Symposium on Foundation of Computer Science, 1985, pp. 360-371.

[GHY2] Galil, Z., Haber, S., and Yung, M., 'Minimum-knowledge interactive proofs for decision problems', SIAM Journal on Computing, Vol.18, No .4, 1989, pp. 711-739.

[GHY3] Galil, Z., Haber, S., and Yung, M., 'Symmetric public key cryptosystems', to appear.

[GK] Goldreich, O. and Krawczyk, H., 'On the composition of zero-knowledge proof system', Proc. 17th Internat. Coll. on Automata, Languages and Programming, 1990, pp. 268-282.

[GKu] Goldreich, O. and Kushilevitz, E., 'A perfect zero knowledge proof for a problem equivalent to discrete logarithm', Proc. CRYPTO 88, 1988, pp. 57-70.

[GMS] Goldreich, O., Mansour, Y., and Sipser, M., 'Interactive proof systems: Provers that never fail and random selection', Proc. 28th IEEE Symposium on Foundation of Computer Science, 1987, pp. 449-462.

[GMW] Goldreich, O., Micali, M., and Wigderson, A., 'Proofs that yield nothing but their validity and a methodology of cryptographic protocol design', Proc. 27th Annual IEEE Symposium on Foundations of Computer Science, 1986, pp. 174-187.

[GP] Goldreich, O. and Petrank, E., 'Quantifying knowledge complexity', Proc. 32nd Annual IEEE Symposium on Foundations of Computer Science, 1991, pp. 59-68.

[GMR1] Goldwasser, S., Micali, S., and Rackoff, C., 'The knowledge complexity of interactive proof system', Proc. 17th Annual ACM Symposium on the Theory of Computing, 1985, pp. 291-304.

[GMR2] Goldwasser, S., Micali, S., and Rackoff, C., 'The knowledge complexity of interactive proof system', SIAM Journal on Computing, Vol.18, no.1, 1989, pp. 186-208.

[GS] Goldwasser, S and Sipser, M, 'Private coins versus public coins in interactive proof system', Proc. 18th Annual ACM Symposium on Theory of Computing, 1986, pp. 59-68.

[IY] Impagliazzo, R. and Yung, M., 'Direct minimum-knowledge computations', Proc. CRYPTO 87, 1987, pp. 40-51.

[K] Kilian, J., 'Zero-knowledge with log-space verifier', Proc. 29th IEEE Symposium on Foundation of Computer Science, 1988, pp. 25-35.

[LS1] Lapidot, D. and Shamir, A., 'Publicly verifiable non-interactive zero-knowledge proofs', Proc. CRYPTO 90, 1990, pp. 353-365.

[LS2] Lapidot, D. and Shamir, A., 'A one-round, two-prover, zero-knowledge protocol for NP', Proc. CRYPTO 91, 1991, pp. 213-224.

[LS3] Lapidot, D. and Shamir, A., 'Fully parallelized multi-prover protocols for $NEXP$-time', Proc. 32nd IEEE Symposium on Foundation of Computer Science, 1991, pp. 13-18.

[LFKN] Lund, C., Fortnow, L., Karloff, H., and Nisan, N., 'Algebraic methods for interactive proof system', Proc. 31st IEEE Symposium on Foundation of Computer Science, 1990, pp. 2-10.

[NY] Naor, M. and Yung, M., 'Public key cryptosystems provably secure against chosen ciphertext attacks', Proc. 22nd Annual ACM Symposium on the Theory of Computing, 1990, pp. 427-437.

[OCO] Okamoto, T., Chaum, D., and Ohta, K., 'Direct zero-knowledge proofs of computational power in five rounds', Proc. EUROCRYPT 91, 1991, pp. 96-105.

[O] Oren, Y., 'On the cunning power of cheating verifiers: Some observations about zero-knowledge proofs', Proc. 28th IEEE Symposium on Foundation of Computer Science, 1987, pp. 462-471.

[RS] Rackoff, C. and Simon, D., 'Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack', Proc. CRYPTO 91, 1991, pp. 433-444.

[SFM] Seiferas, J., Fischer, M., and Meyer, A., 'Separating non-deterministic time complexity classes', J. ACM, 25, 1, 1978, pp. 146-167.

[S] Shamir, A., '$IP = PSPACE$', Proc. 31st IEEE Symposium on Foundation of Computer Science, 1990, pp. 11-15.

[T] Toda, S., 'On the computational power of PP and $\bigoplus P$', Proc. 30th IEEE Symposium on Foundation of Computer Science, 1989, pp. 514-519.

[TW] Tompa, M. and Woll, H., 'Random self-reducibility and zero-knowledge interactive proofs of possession of information', Proc. 28th IEEE Symposium on Foundation of Computer Science, 1987, Annual ACM Symposium on the Theory of Computing, pp. 472-482.

[V] Valiant, L. G., 'The complexity of computing the permanent', Theoretical Computer Science, 8, 1979, pp. 189-201.

[Y] Yung, M., 'Zero-knowledge proofs of computational power', Proc. EUROCRYPT 89, 1989, pp. 196-207.