http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (17): 4114-4121, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4114.4121

Latest Research Progress on Non-interactive Zero Knowledge Proof System

[1]Wu Huixin, [2]Wang Feng and [1]Mo Duo
[1]Department of Information Engineering,
[2]School of Software, North China University of Water Resources and Electric Power,
Zhengzhou, 450011, China,

Abstract: Zero knowledge proof system is an important branch of cryptography and computational complexity theory which has received concern since it was first conceived. Among them, non-interactive zero-knowledge proof system containing only one message from the prover to the verifier has been widely used in the construction of cryptographic protocols and cryptographic algorithms, owning to the better confidentiality, certification and lower interaction complexity. In this study we analyze the basic principles of non-interactive zero-knowledge proof system and summarize the research progress achieved in non-interactive zero-knowledge proof systems for NP problems, non-interactive statistical and perfect zero-knowledge, applications of non-interactive zero-knowledge proof system and so on. Finally, we point out the focus of the future research work.

Key words: Public key cryptography, zero knowledge proof, non-interactive, research progress

INTRODUCTION

In Goldwasser *et al*. (1989) first put forward the concept of interactive proof system and analyze the interactive proof system whose knowledge complexity is zero which created an important branch of cryptography and computational complexity theory-zero knowledge proof. The most attractive feature of zero knowledge proof lies in its seemingly contradictory unique nature that a prover can prove the correctness of an assertion to the verifier without leaking any extra information. It can force the malicious participants in cryptographic protocol to executive in accordance with predetermined steps to ensure the safety of the protocol. Thus it has a broad application prospect. To speak vividly, a verifier who receives the zero knowledge proof of a statement is supposed be told by God that it is true. The main features of zero knowledge proof system include completeness, soundness and zero knowledge.

Completeness: If the statement is correct, then the verifier will "always" accept.

Soundness: If the statement is incorrect, then the verifier will "always" reject.

Zero Knowledge: No (malicious) verifier can get any extra information from the proof procedure, except the correctness of the statement.

Blum *et al*. (1988, 1991) first study the non-interactive zero knowledge (hereinafter referred to as NIZK) proof system and present the common reference string model that is generally applied at present. Non-interactive zero knowledge proof system contains only a message sent by a prover to verifier which can be better used in the construction of cryptographic protocols. Thereafter, researches on the theory and applications of NIZK proof system have started successively, including NIZK proof of NP problems, non-interactive statistical (perfect) zero knowledge as well as the application of NIZK proof to CCA security encryption scheme, anonymous authentication and the construction of group and ring signature, etc.

In recent years Groth *et al*. (2006a, b), suggest to turn the research of NIZK to specific problems (Bayer and Groth, 2012; Groth and Sahai, 2008) and construct NIZK proof systems based on different application scenarios. This idea greatly improves the efficiency and practicability of NIZK and created a new line of research on the applications of NIZK. In the subsequent chapters of this study, we will elaborate the relevant concepts of NIZK proof and summarize the main research results of NIZK.

PRELIMINARY KNOWLEDGE

In the following, let $\{0,1\}^n$ denote the set of n-bit strings and $\{0,1\}^*$ denote the set of all strings. Two

Corresponding Author: Wu Huixin, Department of Information Engineering,
North China University of Water Resources and Electric Power, 450011, Zhengzhou, China

probability ensembles are said to be computationally indistinguishable (denoted by $\approx_c$), if no probabilistic polynomial time turing machine can distinguish them with non-negligible probability. Two probability ensembles are said to be statistically indistinguishable or statistically close (denoted by $\approx_c$), if their statistical distance is negligible.

Zero knowledge interactive proof system: Definition 2.1. (zero knowledge interactive proof system):For language $L\subseteq\{0, 1\}^*$ and a pair of interactive turing machines (P, V), in which P possesses unlimited computational power and V is probabilistic polynomial time, (P, V) is said to be zero knowledge interactive proof system of language L if the following three conditions are true:

- **Completeness:** For any common input $x\in L$ and polynomial p(•):

$$\Pr[(P,V)(x)=1]\geq 1-\frac{1}{p(|x|)}$$

- **Soundness:** For any common input $x\notin L$, any interactive Turing machine P' and polynomial p(.):

$$\Pr[(P',V)(x)=1]<1-\frac{1}{p(|x|)}$$

- **Zero knowledge:** For each probabilistic polynomial time Turing machine V^*,there is a probabilistic polynomial time algorithm M* such that for any $x\in L$:

$$(P,V^*)(x)\approx_c M^*(x)$$

P is called the prover and V is called the verifier.

Intuitively speaking, completeness reflects correctness of the system which means for valid input $x\in L$, a prover can always complete the proof successfully such that the verifier accepts. Soundness is defined against the malicious prover which means for invalid input $x\notin L$, no prover P'can construct a valid proof system such that the verifier accepts. While zero knowledge is for the verifier which means no malicious verifier is able to derive extra knowledge from the process of interaction.

In addition, according to different computational capabilities of the prover and verifier, the above properties (2) and (3) can also be modified, respectively. If the indistinguishability of the two probability ensembles in property (3) is enhanced to statistically indistinguishable or identically distributed, zero-knowledge will be correspondingly defined as statistical zero knowledge and perfect zero knowledge. On the other hand, if soundness holds for any probabilistic polynomial time prover, i.e., computational soundness, then the interactive proof system is called the zero knowledge argument system (Brassard *et al*., 1988).

Non-interactive zero knowledge: Since it has been shown that, in the plain model only languages in BPP have NIZK proof systems, therefore the definition for NIZK proof system usually contains an initial set-up assumption. At present it is generally accepted by the researchers to construct NIZK proof system in the common reference string (hereinafter referred to CRS) model.

Definition 2.2. (NIZK proof system): For a pair of probabilistic Turing machines (P,V), in which P is probabilistic polynomial time and V is deterministic polynomial time. (P, V) is called the non-interactive zero knowledge proof system for language L if the following conditions are met:

- **Completeness:** For any common input $x\in L$ and polynomial p(.):

$$\Pr[V(x,R,P(x,R))=1]\geq 1-\frac{1}{p(|x|)}$$

- **Soundness:** For any common input $x\notin L$, any interactive turing machine P' and polynomial p(.):

$$\Pr[V(x,R,P'(x,R))=1]<\frac{1}{P(|x|)}$$

- **Zero knowledge:** For any $x\in L$, there is a probabilistic polynomial time algorithm M such that:

$$V(x)=(x,R\in\{0,1\}^{c(|x|)},P(x,R))\approx cM(x)x\in L$$

Witness indistinguishability: Definition 2.3 (witness indistinguishable (Feige and Shamir, 1990): Let L be an NP language, (P, V) be the interactive proof system of L, R_L be the witness relation of L and $z\in\{0,1\}^*$ be the auxiliary input of V. (P, V) is said to be witness indistinguishable for R_L, if for any probabilistic polynomial time interactive turing machine V* and any ω_1, $\omega_2\in R_L(x)$, the following probability ensembles are computationally indistinguishable:

$$\{(P(\omega_1),V^*(z))(x)\}_{x\in L z\in\{0,1\}^*}$$
$$\approx_c\{(P(\omega_2),V^*(z))(x)\}_{x\in L z\in\{0,1\}^*}$$

Witness indistinguishability is a weaker notion of zero knowledge, but it is sufficient to ensure the security of cryptographic protocol in some applications. It is worth mentioning that witness indistinguishability is closed under concurrent composition.

RESEARCH PROGRESS OF NIZK

Definition and models of NIZK: In view of the important theoretical and applied value of zero knowledge interactive proof system in the fields of computational complexity and cryptography its inherent nature and characteristics have caused much attention, such as interactivity, the randomness of participants and auxiliary input, etc. Oren (1987) first proves that NIZK proof systems only exist for BPP languages in the plain model (without any trusted set-up assumption). In 1988, NIZK proof system based on the CRS model is proposed by Blum *et al.* (1988) . CRS is generated by a trusted party and is accessible to both the prover and verifier. This model requires only the randomness of CRS, not relying on its privacy, so CRS model is more practical than interactive model. The same year, De Santis *et al.* (1988) discuss NIZK in another model which is called NIZK with preprocessing. The idea of preprocessing model derives from one time pad (Shannon, 1949): In the preprocessing stage, the prover chooses a n-bit string vϵV and convinces the verifier (vϵV) through interactive zero knowledge proof; in the subsequent interactive stage, the prover constructs a proof of the statement to the verifier, then the verifier can verify the correctness of the statement according to vϵV. The disadvantage of preprocessing model is the prover and verifier need to interact first and the length of statement proved in the interactive stage is limited by the length of v. In addition, preprocessing model is stronger than CRS model because the two parties can generate CRS in the preprocessing stage. Comparing the two models, CRS model is more reasonable, general and practical. It is the widely accepted NIZK model now.

In Cramer and Damgard (2004) propose a secret key model of NIZK whose security depended not on CRS, but assuming an appropriate secret key to exist between the prover and verifier. In Groth and Lu, 2007; Groth and Ostrovsky (2007) put forward multi-string NIZK model. They point out that CRS needs to be generated by a trusted third party in the single string model. However it is difficult to find a suitable third party in practical applications. Therefore it can be considered that the common reference string is generated by multi parties as long as most of them are honest. Meanwhile, they also present the first NIZK proof system in the multi-string model.

NIZK proof Systems of NP problems: In early literatures, researches on NIZK are mainly focus on the existence and effective constructions of NIZK proof systems for NP languages.

Blum *et al* propose the first bounded NIZK proof system, that is, for different statements the proof system has to use different CRS's and the length of the statement is controlled by the length of CRS. Later, Blum, De Santis, Micali and Persiano present a more general NIZK proof system for 3*SAT* which allows a prover to prove many statements with the same CRS. However, the above proof systems are constructed based on specific mathematical problems.

Feige *et al.* (1990); Feige and Shamir (1990); Lapidot and Shamir (1990) present the first NIZK proof system for NP based on general assumptions and the construction is based on one-way permutations or certified trapdoor permutations for a polynomial time prover. At the same time, they also introduce a hiding bit model and use witness indistinguishability to turn bounded NIZK into general NIZK proof system which allows many provers to use the same random string to prove different statements. Lapidot and Shamir (1990) give the first publicly verifiable NIZK assuming the existence of one-way permutations. Blum *et al.* (1991) separately shows NIZK proofs of 3SAT problem and HC problem based on different assumptions, respectively. Then NIZK proof systems for general NP problem can be obtained by Karp reduction but this kind of constructions engage a very high level of complexity. Thereafter, Damgard (1993) designs NIZK proof system for SAT problem, making the construction of NIZK for NP problem more direct. Simultaneously, he also gives non-interactive statistical zero knowledge argument of HC problem under the preprocessing model.

Bellare and Yung (1996) point out that the trapdoor permutation used in NIZK proof system requires additional verification and put forward the corresponding solution. Following the hiding bit method, Kilian shows a NIZK proof system for SAT based on one-way permutations and the number of hiding bits is $O(n\log^c nk)$. Since then, Kilian (1994) improve the construction which reduces the number of hiding bits to $O(k n\log(n/\epsilon))$. De Santis *et al.* (2004) discuss the length of CRS in NIZK and shows a NIZK proof system for NP problem whose CRS length is $\Theta(n^{\epsilon}+\log(1/s))$", in which $e>0$ is constant and s is the reasonable error bound. Boyar *et al.* (2000) study short NIZK proofs and construct a NIZK proof system with the length of $O(mk(\log m+r))$, in which m is the number of gates in the circuit and k is the length of the commitment. Moreover, this study shows a NIZK proof system with length of $O(m(\log m+r)+rk)$ in the RO model as well and in specific applications, NIZK with appropriate length can be obtained by simulating RO.

NISZK and NIPZK: Statistical zero knowledge plays a significant role in both practical application and

theoretical study, because it reflects the inherent characteristics of zero knowledge and does not need to be constructed under cryptographic assumptions as computational zero knowledge. The existing results show that there is computational zero knowledge proof system for any PSPACE language and for SZK, we have SZK⊆AM∩coMA (Here we use SZK to denote "statistical zero knowledge" while SZK to denote the class of languages which have statistical zero knowledge proof systems. NISZK and similar notions are defined respectively.). However it is generally believed that NP⊈AM∩coAM, thus the studies of NISZK are only considered for specific non-NPC language.

Blum *et al.* (1991) propose the first non Interactive Perfect Zero Knowledge (NIPZK) proof system for quadratic non-residue problem in coNP. Ostrovsky (1991) proves that for any nontrivial language, the existence of SZK and NISZK proof or argument system is a sufficient condition for the existence of one way functions. Thereafter, De Santis *et al* do some further researches on NISZK and NIPZK. First, they give a NIPZK proof for quadratic residue and a new method that turns non-interactive proofs into interactive proofs which can not only keep the same zero knowledge characteristics but make the round of the converted interactive proof systems optimal. Then, they discuss the existence of PZK for quadratic non-residue and the lower bound of CRS in the model with fixed CRS length. De Santis *et al.* (1988) prove that NIZK is closed under complement by constructing a special language called "*ID*". Since then, De Santis *et al.* (2004) study the relationship between SZK and NISZK and prove that NIZK is closed under Karp reductions as well as some other logical operations and ultimately conclude that SZK = NISZK. With the help of Boolean circuit composition theory, De Santis *et al.* (2004) expand the scope of these two languages on the basis of the already known PZK and NIPZK. They point out that the languages got from specific language categories in NC^1 circuit composition all have NIPZK. Besides, the idea also applies to SZK. Pass and Shelat (2005) discuss NISZK in secret key model together with CRS model. They point out NIZK = NISZK = NIPZK = AM in the secret key model while in CRS model for non-adaptive definition, there is NISZK⊆AMncoAM∩coAM and for adaptive definition, there is NISZK⊂BPP/1. Additionally, for the language undecidable by non-uniform polynomial circuits, the necessary and sufficient condition of NIZK is the existence of one way function. Eventually they show an absolute result for the existence of NIZK: NIZK exists either for simple language only, or for all AM languages.

The above results indicate that for general NP language, non-interactive statistical (perfect) zero knowledge proof does not exist. Then, does non-interactive statistical (perfect) zero-knowledge argument exist? Groth (2006) give an affirmative answer. They propose the first NIPZK argument system for language SAT, thus prove that there is a NIPZK argument system for any NP language. They also give the first adaptive UC secure NIZK argument. Afterwards, Abe and Fehr (2007) put forward the first efficient NIZK argument system with adaptive soundness based on the KEA assumption which also applies to any NP problem.

NIZK for specific problems: Since its invention, researches on NIZK are mainly focused on the theoretical problems. Although it is once used to construct CCA-2 secure encryption schemes by Naor and Yung (1990) and signature schemes by Bellare and Goldwasser (1989), these results are just theoretical feasibility without practical applications. One of the important reasons is that the construction of NIZK is not efficient. Early researches are mainly focused on NIZK proof systems for general NP problems, so the NPC problems such as SAT'3SAT'HC or G3C are usually taken for consideration. While in practical applications, we instead consider certain types of problems (such as the computations in the bilinear group, etc.), therefore the NIZK proof systems for general NP problems have to be reduced to NIZK proof systems for specific problems which greatly sacrifices the efficiency. How to construct efficient NIZK proof systems seems to be the key to promote their applications.

In Groth and Ishai, 2008 analyze the reasons why the past NIZK proofs are inefficient and put forward the famous GS proof framework that applies to all basic operations in bilinear group. NIZK proof system can be obtained simply and efficiently through instantiating GS proof according to different application backgrounds which greatly simplifies the design of public key cryptographic algorithm and cryptographic protocol based on bilinear groups. Since then, Ghadafi *et al.* (2010) revise and expand GS proof to make it applicable to more bilinear groups. Later, Groth (2009, 2010a, 2010b, 2010c, 2011a, 2011b) makes further improvements on some aspects such as the computational efficiency and length of NIZK. Besides, Damgard and Thorbek (2007) shows a NIZK proof system of integer multiplications.

NIZK and IZK: The relationship, comparison and transformation between NIZK and IZK are also important research directions of zero knowledge proof systems. At first Blum *et al.* (1988) point out that CRS model is weaker

than interactive model, that is, NIZK proof system does not necessarily exist in language with IZK proofs. Then, is there a suitable model making NIZK and IZK equivalent?

In 2002, a new zero knowledge proof model known as the "HELP "model is proposed by Ben-Or and Gutfreund, (2003), in which a third party "Dealer" is assumed to exist. It is a probabilistic polynomial time algorithm that on input the statement to be proved, outputs the common reference string. In Ciocan and Vadhan (2007) prove that a language in AM has an interactive proof system only if there is a NIZK proof system in the HELP model. At the same time, they point out that this result applies to the computational and statistical zero knowledge, not relying on cryptographic a ssumptions. From then on, Chailloux *et al*. (2008) prove that NIZK and IZK are equivalent in the HELP model. In 1990, Fiat and Shamir exhibit a method that transforms interactive protocol into non-interactive protocol, known as "Fiat-Shamir heuristic" . The method can be used to turn public-coin IZK proofs into NIZK arguments. But hash function is used in this transformation, so the NIZK argument can only be proved to be secure in the RO model. In De Santis *et al*. (1994) present a new method that turns non-interactive proof systems into interactive proof systems which can not only keep the same zero knowledge characteristics but ensure the round complexity of the converted system to be optimal.

NIZK and Zap: In 2000, Dwork and Naor show a surprising result (Dwork and Naor, 2000): There exists two-round public-coin witness indistinguishable proof system that does not use CRS. The authors call the proof system zap. In a zap, the verifier first sends a random string to the prover; then the prover replies with a message to complete the proof. Zaps have many applications such as: The construction of concurrent zero knowledge, deniable authentication and ring signature (Bender *et al*., 2009),etc. The study also presents a construction of zap using NIZK and Verifiable Psedo-random Generator (VPRG).

As can be seen from the definition of zap it has an important link with NIZK. In 2004, De Santis *et al*. discuss the length of random string in zap and NIZK proof of NP problem. They point out that if there is zap for NP problem, then the length of random string used will be $\Theta(n^{\varepsilon}+\log(1/s))$ bits; if there is NIZK proof for NP problem, then the number of bit it used will also be $\Theta(n^{\varepsilon}+\log(1/s))$. In Groth (2006) propose a new method to construct NIZK proof as well as NIZK argument and give the first construction of non-interactive zaps.

APPLIED RESEARCHES OF NIZK

The inherent privacy and authentication properties of zero knowledge proof system make it widely used in the construction of cryptographic protocols. Generally speaking, IZK proof system is usually used to construct multi-round interactive protocol in the plain model, for example general two party and multi party secure computation and mostly for designing protocols in an abstract way while NIZK proof is usually integrated into the construction of specific, practical cryptographic algorithm and cryptographic protocols. This raises very high demands on the construction of efficient NIZK proof systems. At first, Blum *et al* point out that NIZK can be used to design public key encryption schemes secure against chosen ciphertext attack. However, this study only shows the possibility but doesn't give a specific construction. Since then, Naor and Yung (1990) put forward the first CCA secure public key encryption scheme on the basis of probabilistic encryption and NIZK. Bellare and Yung, 1993, present a new method to construct signature and message authentication protocol with the help of NIZK. And the scheme obtained is secure against adaptive chosen message attack. De Santis *et al*. (2004) extend the non-malleability of cryptographic protocols to NIZK and proposes a method to transform general NIZK into NMNIZK. At the same time, this study also gives an encryption scheme secure against adaptive chosen ciphertext attack.

On the other hand, NIZK is widely used in group signatures, ring signatures and electronic voting. NIZK is first used to construct a provably secure group signature scheme in the standard model by (Bellare *et al*., 2003) . Thereafter Groth uses NIZK to construct a group signature with constant size as well as a completely anonymous group signature scheme in the standard model. Zap is introduced to the construction of ring signature for the first time by Bender *et al*., 2009, Recently NIZK is used in shuffle verification by Groth, 2006, (Bayer and Groth, 2012; Groth, 2006, 2007, 2010b).

SUMMARIES AND OUTLOOK

In the recent 20 some years, researches on NIZK proof system and related theory have improved gradually. Recent research focuses are mainly concentrated in the application and efficiency improvement of NIZK proof system, including the following aspects:

- Efficient NIZK proof and NIZK argument system that apply to specific application backgrounds. Currently, the researches for NIZK efficiency are mainly

concentrated in the computation in bilinear group, so it is worth deeply studying how to construct highly efficient NIZK protocol applicable to other mathematical backgrounds

- Other cryptographic tools that cooperate with the existing proof systems. Recently, Abe *et al.* (2010) propose structure-preserving commitments and signatures which apply perfectly to GS proof system so that it enables the modular design of the protocols and at the same time ensuring the efficiency. At present, these researches are just beginning and there are still a lot of problems in the efficiency and application of these schemes

REFERENCES

Bender, A., J. Katz and R. Morselli, 2009. Ring signatures: Stronger definitions and constructions without random oracles. J. Cryptol., 22: 114-138.

Chailloux, A., D.F. Ciocan, I. Kerenidis and S.P. Vadhan, 2008. Interactive and noninteractive zero knowledge are equivalent in the help model. Proceedings of the 5th Theory of Cryptography Conference, March 19-21, 2008, New York, pp: 501-534.

De Santis, A., G. di Crescenzo and G. Persiano, 1994. The knowledge complexity of quadratic residuosity languages. Theor. Comput. Sci., 132: 291-317.

De Santis, A., G. di Crescenzo and G. Persiano, 2004. On ncl boolean circuit composition of non-interactive perfect zero-knowledge. Proceedings of the 29th International Symposium on Mathematical Foundations of Computer Science, August 22-27, 2004, Prague, pp: 356-367.

De Santis, A., S. Micali and G. Persiano, 1988. Non-interactive zero-knowledge with preprocessing. Proceedings of the Annual International Cryptology Conference, August 21-25, 1988, USA., pp: 269-282.

Shannon, C.E., 1949. Communication theory of secrecy systems. Bell. Syst. Technical. J., 28: 656-715.

Dwork, C. and M. Naor, 2000. Zaps and their applications. Proceedings of the 41st Annual Symposium on Foundations of Computer Science, November 12-14, 2000, Redondo Beach, CA., pp: 283-293.

Ciocan, D.F. and S. Vadhan, 2007. Interactive and noninteractive zero knowledge coincide in the help model. Cryptology ePrint Archive, Report 2007/389, October 3, 2007.

Lapidot, D. and A. Shamir, 1990. Publicly verifiable non-interactive zero-knowledge Proofs. Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, August 11-15, 1990, Santa Barbara, California, USA., pp: 353-365.

Ghadafi, E., N.P. Smart and B. Warinschi, 2010. Groth-sahai proofs revisited. Proceedings 13th International Conference on Practice and Theory in Public Key Cryptography, May 26-28, 2010, Paris, France, pp: 177-192.

Brassard, G., D. Chaum and C. Crepeau, 1988. Minimum disclosure proofs of knowledge. J. Comput. Syst. Sci., 37: 156-189.

Damgard, I., 1993. Non-interactive circuit based proofs and non-interactive perfect zero-knowledge with preprocessing. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques and Advances in Cryptology, May 24-28, 1992, Balatonfured, Hungary, pp: 341-355.

Damgard, I. and R. Thorbek, 2007. Non-interactive proofs for integer multiplication. Proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology, May 20-24, 2007, Barcelona, Spain, pp: 412-429.

Groth, J., 2006. Simulation-sound NIZK proofs for a practical language and constant size group signatures. Proceedings of the 12th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology, December 3-7, 2006, Shanghai, China, pp: 444-459.

Groth, J., 2007. Fully anonymous group signatures without random oracles. Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, December 2-6, 2007, Kuching, Malaysia, pp: 164-180.

Groth, J., 2009. Linear algebra with sub-linear zero-knowledge arguments. Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology, August 16-20, 2009, Santa Barbara, CA., USA., pp: 192-208.

Groth, J., 2010a. P airing-based non-interactive zero-knowledge proofs. Proceedings of the 4th International Conference on Pairing-Based Cryptography-Pairing, December 2010, Yamanaka Hot Spring, Japan, pp: 206.

Groth, J., 2010b. Short non-interactive zero-knowledge proofs. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, December 5-9, 2010, Singapore, pp: 341-358.

Groth, J., 2010c. Short pairing-based non-interactive zero-knowledge arguments. Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, December 5-9, 2010, Singapore, pp: 321-340.

Groth, J., 2011a. Efficient zero-knowledge arguments from two-tiered homomorphic commitments. Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, December 4-8, 2011, Seoul, South Korea, pp: 431-448.

Groth, J., 2011b. Efficient zero-knowledge proofs. Proceedings of the 4th International Conference on Cryptology in Africa: Progress in Cryptology, July 5-7, 2011, Dakar, Senegal, pp: 379-379.

Groth, J. and Y. Ishai, 2008. Sub-Linear Zero-Knowledge Argument for Correctness of a Shuffle. In: Advances in Cryptology, Smart, N. (Ed.). Springer, USA., ISBN: 978-3-540-78966-6, pp:379-396Springer, USA., ISBN: 978-3-540-78966-6, pp:379-396.

Groth, J. and S. Lu, 2007. A Non-Interactive Shuffle with Pairing based Verifiability. In: Advances in Cryptology, Kurosawa, K. (Ed.). Springer, USA., ISBN: 978-3-540-76899-9, pp: 51-67.

Groth, J. and R. Ostrovsky, 2007. Cryptography in the Multi-String Model. In: Advances in Cryptology, Menezes, A. (Ed.). Springer, USA., ISBN:3-540-74142-9, pp: 323-341.

Groth, J., R. Ostrovsky and A. Sahai, 2006a. Non-Interactive Zaps and New Techniques for Nizk. In: Advances in Cryptology, Dwork, C. (Ed.). Springer, USA., ISBN: 978-3-540-37432-9, pp: 97-111.

Groth, J., R. Ostrovsky and A. Sahai, 2006b. Perfect Non-Interactive Zero Knowledge for NP. In: Advances in Cryptology, Vaudenay, S. (Ed.). Springer, USA., ISBN: 978-3-540-34546-6, pp: 339-358.

Groth, J. and A. Sahai, 2008. Efficient Non-Interactive Proof Systems for Bilinear Groups. In: Advances in Cryptology, Smart, N. (Ed.). Springer, USA., ISBN: 978-3-540-78966-6, pp: 415-432.

Boyar, J., I. Damgard and R. Peralta, 2000. Short non-interactive cryptographic proofs. J. Cryptol., 13: 449-472.

Kilian, J., 1994. On the complexity of bounded-interaction and noninteractive zero-knowledge proofs. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 20-22, 1994, Santa Fe, NM., pp: 466-477.

Abe, M., G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo, 2010. Structure-Preserving Signatures and Commitments to Group Elements. In: Advances in Cryptology, Rabin, T. (Ed.). Springer, USA., ISBN: 978-3-642-14622-0, pp: 209-236.

Abe, M. and S. Fehr, 2007. Perfect Nizk with Adaptive Soundness. In: Theory of Cryptography, Vadhan, S.P. (Ed.). Springer, USA., ISBN: 978-3-540-70935-0, pp: 118-136.

Blum, M., A. de Santis, S. Micali and G. Persiano, 1991. Noninteractive zero-knowledge. SIAM J. Comput., 20: 1084-1118.

Blum, M., P. Feldman and S. Micali, 1988. Non-interactive zero-knowledge and its applications. Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago, Illinois, May 2-4, 1988, pp: 103-112.

Ben-Or, M. and D. Gutfreund, 2003. Trading help for interaction in statistical zero-knowledge proofs. J. Cryptol., 16: 95-116.

Bellare, M., D. Micciancio and B. Warinschi, 2003. Foundations of group signatures:Formal definitions, simplified requirements and a construction based on general assump-tions. Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques, May 4-8, 2003, Warsaw, Poland, pp: 614-629.

Bellare, M. and M. Yung, 1993. Certifying cryptographic tools: The case of trapdoor permutations. Proceedings of the 12th Annual International Cryptology Conference Santa Barbara, August 16-20, 1992, California, USA., pp: 442-460.

Bellare, M. and M. Yung, 1996. Certifying permutations: Noninteractive zero-knowledge based on any trapdoor permutation. J. Cryptol., 9: 149-166.

Bellare, M. and S. Goldwasser, 1989. New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, August 20-24, 1989, California, USA., pp: 194-211.

Naor, M. and M. Yung, 1990. Public-key cryptosystems provably secure against chosen ciphertext attacks. Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, MD., pp: 427-437.

Pass, R. and A. Shelat, 2005. Unconditional characterizations of non-interactive zero knowledge. Proceedings of the 25th Annual International Cryptology Conference, August 14-18, 2005, Santa Barbara, California, USA., pp: 118-134.

Cramer, R. and I. Damgard, 2004. Secret-key zero-knowlegde and non-interactive verifiable exponentiation. Proceedings of the 1st Theory of Cryptography Conference, February 19-21, 2004, Cambridge, MA., USA., pp: 223-237.

Ostrovsky, R., 1991. One-way functions, hard on average problems and statistical zero-knowledge proofs. Proceedings of the 6th Annual Structure in Complexity Theory Conference, June 30-July 3, 1991, Chicago, IL., pp: 133-138.

Goldwasser, S., S. Micali and C. Rackoff, 1989. The knowledge complexity of interactive proof-systems. SIAM J. Comput., 18: 186-208.

Bayer, S. and J. Groth, 2012. Efficient zero-knowledge argument for correctness of a shuffle. Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, April 15-19, 2012, Cambridge, UK., pp: 263-280.

Feige, U., D. Lapidot and A. Shamir, 1990. Multiple non-interactive zero knowledge proofs based on a single random string. Proceedings of the 31st Annual Symposium on Foundations of Computer Science, October 22-24, 1990, St. Louis, MO., pp: 308-317.

Feige, U. and A. Shamir, 1990. Witness indistinguishable and witness hiding protocols. Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA., pp: 416-426.

Oren, Y., 1987. On the cunning power of cheating verifiers: Some observations about zero knowledge proofs. Proceedings of the 28th Annual Symposium on Foundations of Computer Science, October 27-29, 1987, Los Angeles, California, pp: 462-471.