International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 38708-38713

A Novel Zero Knowledge Protocol based on Bin Packing Problem

Debajit Sensarma,
Research Fellow, Department of Computer Science and Engineering, University of Calcutta, Kolkata, India
debajit.sensarma2008@gmail.com

Samar Sen Sarma,
Professor, Department of Computer Science and Engineering University of Calcutta, Kolkata, India
sssarma2001@yahoo.com

Abstract
Zero Knowledge Protocol is an interactive proof system where one party (Prover) proves a statement to another party (Verifier) without yielding anything beyond the validity of assertion. Now-a-days, communication protocols are vulnerable to impersonation attack and the performance of the protocol degrades because without proper security, any time an eavesdropper or an intruder may listen in on the communication. Zero Knowledge protocol tries to cope with this type of situation. In this paper, we proposed a novel Zero Knowledge Protocol using well known Bin Packing Problem considering it as a special case of 3-PARTITION problem..

Keywords: Interactive Proofs, Zero Knowledge, Bin Packing, NP, 3-PARTITION, Proof Systems.

I. Introduction

With the development of the technology, there is a massive increase of data exchange. These data, exchanged through the various mediums contains sensitive information (e.g. password of bank account, other critical security information) and if an eavesdropper or an intruder gets access to these private data, then it can have very bad impact in our society. Generally, malicious persons try to copy someone's behavior by listening to the communication and gaining enough information about either one of the two parties involved in the exchange of information. There are several solutions exist, like private key cryptography, public key cryptography [1, 2]. But still there is an authentication problem (e.g. Man-in-the-middle attack). Zero knowledge proofs try to cope with this problem in general, which is an interactive protocol where a Prover can prove the validity of statement to the Verifier without disclosing any other secret information. Such statement is generally mathematical problem which belongs to class NP or NP-Complete. Bin Packing Problem is a well know NP-Complete or NP-Hard problem [3].It is also one of the most known combinatorial optimization problems. In the bin packing problem, objects of different sizes are to be packed into a finite number of bins or containers each of capacity C in a way that minimizes the number of bins used. 3-PARTITION problem is also a strongly NP-Complete problem. The problem is to decide whether a given multi-set of integers can be partitioned into triples that all have the same sum.

In this work we have considered an instance of Bin Packing Problem which is a special case of 3-PARTITION problem, where number of objects n=3m have to be packed in m bins and $C/4 < s_i < C/2$ where s_i is the size of objects.

The paper is organized as follows: Section II describes the preliminaries associated with the proposed protocol; Section III depicts the related works. In section IV, proposed protocol has been given. Section V describes the proposed protocol with an example. Finally section VI concludes the paper.

II. Preliminaries

A. Parties in Zero Knowledge Protocol:

There are two parties involved in this protocol.

- **Prover:**

Prover has some information which he/she wants to prove to the Verifier without telling the secret to the Verifier.

- **Verifier:**

Verifier asks the Prover a sequence of questions to find out if Prover really knows the secret or not, but he/she learn nothing about the secret even by cheating or by not abide by the protocol.

B. Features of Zero Knowledge Protocol:

This protocol has following features [4].

- **The Verifier cannot learn anything from the protocol:**

The Verifier gets no information from the protocol such that he/she could learn about the secret by him/herself without the Prover, i.e. no knowledge is transferred.

- **The Prover cannot cheat Verifier:**

If the Prover does not know the secret, he/she can only succeed with good luck. But after several rounds, the probability for successful cheating becomes very low.

- **The Verifier cannot cheat the Prover:**

If Verifier does not obey the protocol, he/she cannot get any information out of the protocol. Only Prover can convince him/herself that he/she knows the secret.

- **The Verifier cannot pretend to be the Prover to any third Party:**

As no information leaked from the protocol to the Verifier, Verifier cannot masquerade as Prover to any outside third party.

C. Properties of Zero Knowledge Protocol:

Zero Knowledge Protocol must satisfy three properties [5].

i) **Completeness:** If the statement is true, the honest Prover can convince the honest Verifier.

ii) **Soundness:** If the statement is false, Prover cannot convince the honest Verifier by cheating that the statement is true.

iii) **Zero Knowledge:** If the statement is true, the Verifier who is cheating cannot learn anything about the secret.

The first two properties are belongs to interactive proof systems and the third one makes the protocol zero knowledge.

D. Types and Modes of Zero Knowledge Protocol:

Zero Knowledge Protocol has following types and modes [4].

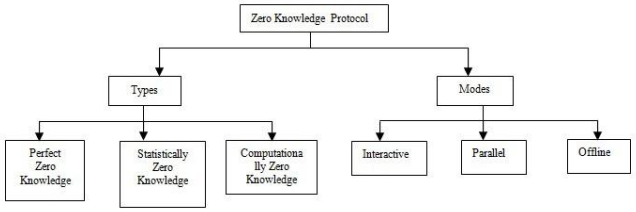

Figure.1. Types and Modes of Zero Knowledge Protocol scheme

E. Basic Interactive Proof Protocol:

The interactive proof in general a challenge and response protocol which consists of specified number of rounds and two probabilistic algorithms [6, 7] for Prover and verifier. They both have the random number generator which is private and they perform private operations. In this protocol Prover and Verifier both agrees on input 'x'. The objective is to convince the Verifier that 'x' has some specified property. This is based on several rounds and each round consists of challenge of Verifier and response of Prover. For example, in each round Prover and Verifier performs following general steps.

i) Receive message from other parties (Verifier/ Prover).

ii) Perform private computation.

iii) Send message to the other party.

At the end of the proof, Verifier can accept or reject depending on Prover's replies. In addition, an interactive proof is said to be *proof of knowledge* if it abide by soundness and completeness properties.

F. Applications of Zero Knowledge Protocols:

Zero knowledge Protocol has applications mainly in cryptography and security protocols requiring authentication (e.g. Fiat-Shamir protocol [8], Feige-Fiat-Shamir Proof of Identity [9], Guillou-Quisquater protocol [10]). Besides this, these protocols are used for many real-time applications like e-voting [11], watermark verification [12], Sky's VideoCrypt [13], Microsoft's Next Generation Secure Computing Base (NGSCB) [13], Secret Sharing Scheme [27] etc.

G. Bin Packing Problem:

In classical one-dimensional Bin Packing Problem, a sequence of items L = (a_1, a_2,…, a_n) is given, each of size $S(a_i) \in (0,1]$ and the goal is to pack them into minimum number of unit-capacity bins (i.e. partition them into a minimum number m of subsets B_1, B_2, …, B_m such that $\sum_{a_i \in b_j} S(a_i) \leq 1$, $1 \leq j \leq m$).

In the view of constraint satisfaction problem Bin Packing problem is a problem of partitioning the set L under a sum constraint i.e. divide L into a minimum number of blocks, called bins such that the sum of sizes of the items in each bin is at most a given capacity C>0 [3, 14].

H. 3-PARTITION problem:

Given 3n integers i_1, $i_{2,}$…, i_{3n} and v= 1/n $\sum_{k=1}^{3n} i_k$, find sets S_1, S_2, …, S_n with $|S_k| = 3$, such that $\forall$ k, $\sum_{j \in S_k} i_j$ = v.

The 3-PARTITION problem remains NP-Complete when every integer 'i' is strictly between v/4 and v/2 (i.e. $v/4 < i_k < v/2$) [3].

Theorem 1: 3-PARTITION Problem is strongly NP-Complete.

In [15] authors originally proved 3-PARTITION to be strongly NP-Complete, by reduction from 3-DIMENSIONAL MATCHING (3-DM). They first reduces 3-DM to 4-PARTITION, then to 3-PARTITION problem, where 4-PARTITION is analogous to 3-PARTITION with 4n integers and $v/5 < i_k < v/3$.

III. Related Works

Zero Knowledge Protocols has numerous applications in the area of cryptography and security protocol that required authentication. Goldwasser et al. [6] first introduced the interactive proof system. Since then it is a very attractive research area. Blum et al. [16] proposed a Zero Knowledge Proof scheme based on Hamiltonian cycle in large graph. Finding Hamiltonian cycle in a graph graph is a NP-Complete problem [17].Next, in [18] Goldreich et al. proposed a Zero Knowledge Proof system for an NP-Complete problem GRAPH 3-COLORABILITY [3, 17]. The problems states that, A graph G (V, E) is said to be 3 colorable if there exists a mapping ϕ : V→ {1, 2, 3}, such that every two vertices are assigned difference colors. They have also showed that all languages in NP, have a Zero Knowledge Proof system [18]. Next, Mohajeri et al. [19] proposed a Zero Knowledge Proofs for Independent set and Dominating set problem, Vertex cover problem [20]. There are many problems that are considered to have a Zero Knowledge Proof system, like-Graph Isomorphism [18, 21], Graph Non-Isomorphism [18], Clique Problem [22], Graph Clustering Problem [23], Discrete Logarithm Problem [24], Quadratic Residue Problem [25], Satisfiability Problem [26] etc.

IV. Proposed Zero Knowledge Protocol

In this work, an extreme case of Bin Packing Problem has been considered. Suppose, there are n=3m objects, with m bins of capacity C. The size of objects are $s_1, s_2, \ldots, s_n$ are such that $C/4 < s_i < C/2 \ \forall i = 1, \ldots, n$ and $\sum_{i=1}^{n} s_i = m*C$. Thus, any two objects fit into a bin, but more than three never fit. Now, the problem is to decide whether objects can be packed into m bins such that every bin contains exactly three objects. This problem is exactly same as 3-PARTITION problem defined in section II.

Theorem 2: Bin Packing Problem is strongly NP-Complete.

Proof. The proof is done by reducing instance of 3-PARTITION problem to the instance of Bin Packing Problem as follows-for a given instance I of the 3-PARTITION problem, construct an instance I′ of Bin Packing Problem which has 3m objects with sizes $s_1, s_2, \ldots, s_{3m}$ respectively and m bins with capacity C. We now prove the claim that there exists a feasible solution to an instance I iff the instance I′ has its optimal solution such that each bin exactly contains three objects.

If I has a solution i.e. there exists sets $t_1, t_2, \ldots, t_n$ with $|t_i|=3$, such that $\forall i, \sum_{j \in t_i} s_j = C$, and we can put each t_i into a bin so that each bin has exactly three objects.

Conversely, if I′ has a solution such that each bin has no more than three objects, then we claim that, we can use the items of each bin to form a solution of 3-PARTITION problem. This is because we have 3m objects and m bins and each bin has exactly three objects. It is clear that, each object is fully packed into one bin otherwise by pigeonhole principle some bin will have more than three objects, which is not possible. Thus, each bin b_i contains exactly three non-spilt objects whose total size is C and can be used to form a set t_i. This proves the theorem.

A. Protocol:

- ***Prover:***

Assume, Prover knows the packing of the objects with size $s_1, s_2, \ldots, s_{3m}$ in the bins $B_1, B_2, \ldots, B_m$ respectively with $\forall$ m, $|B_m| = 3$ and $\forall$ m, $\sum_{j \in B_m} s_j = C$.

1. Compute $M = \sum_{i=1}^{3m} s_i$.
2. Generate $P_1, P_2, \ldots, P_{3m}$, where P_i is chosen uniformly at random from $\{0, \ldots, M\}$.
3. Calculate $Q_1, Q_2, \ldots, Q_{3m}$, where $s_i + P_i \equiv Q_i$ Mod M+1 (where i=1,....,3m).
4. Commit (but hide)

   $\forall i, A_i \equiv \sum_{j=1}^{3m} B_i P_j$ Mod M+1 (i=1,2, …, m) and

   $A' = \sum_{j=1}^{m} A_j$ Mod M+1.

   $\forall i, D_i \equiv \sum_{j=1}^{3m} B_i Q_j$ Mod M+1 (i=1,2, …, m) and

   $D' = \sum_{j=1}^{m} D_j$ Mod M+1.

   Where $\forall i$, $B_i = 1$ indicates $S_j \in B_i$ (j=1,…,3m) and $B_i = 0$, otherwise.

4. Commit (but hide) the following table by permuting columns and s_i.

Table 1

S	s_1	s_2 …
P	P_1	P_2 …
Q	Q_1	Q_2 …
$s_i \in B_1$?	0/1	0/1 …
…	…	…
$s_i \in B_m$?	0/1	0/1 …

- **Verifier:**

Verifier asks to see one of the following.

1. All triples (s_i, P_i, Q_i) (checking that $s_i + P_i \equiv Q_i$ Mod M+1 (where i=1,....,3m)).
2. $Q_1, Q_2, \ldots, Q_{3m}, B_1, B_2, \ldots, B_m, A'$ and $D_1, D_2, \ldots, D_m$. (Checking that, $\forall i, \sum_{j=1}^{3m} B_i Q_j \equiv D_i$ Mod M+1 (i=1,2, …, m) and $A' + \sum_{j=1}^{m} D_j \equiv 3*C$ Mod M+1).
3. $P_1, P_2, \ldots, P_{3m}, B_1, B_2, \ldots, B_m, A_1, A_2, \ldots, A_m$ and D'. (Checking that, $\forall i, \sum_{j=1}^{3m} B_i P_j \equiv 0$ Mod M+1 (i=1,2, …, m) and $\sum_{j=1}^{m} A_j + D' \equiv 3*C$ Mod M+1).

If any check fails then verifier rejects immediately.

Claim 1: Above Protocol is a Zero Knowledge Scheme.

- **Completeness:**

If Prover knows the packing of objects into the bins $B_1, B_2, \ldots, B_m$ respectively, then it is easy to verify that there is no way for him/her to be caught by the verifier if he follows the protocol.

- **Zero Knowledge:**

In this protocol P_i is generated randomly and similarly Q_i also. Also every time column permutation of the table as well as permutation of s_i's are revealed. Next, Prover's answers do not reveal the original packing of objects. In each round verifier will only learn S or P_i or Q_i or the object s_i is in B_j (i=1,…3m, j=1,…m) or not. But all answers needed at a time to discover the original packing. If Prover does not know the

packing but somehow knew in advance what the verifier would ask to see in each round, the Prover could cheat. For example, if Prover knew before that the Verifier would ask to see option 1 of the protocol, he/she could generate arbitrary random numbers which will satisfy the condition. Likewise, Prover could satisfy the Verifier for other two options by generating random instances. Verifier could simulate the protocol because he/she knows what he/she will ask to see. Thus from the information revealed in each round, the verifier could gain no information about the packing.

- **Soundness:**

If the Prover does not know the information of the original packing, he/she could guess a question what the Verifier will ask and generate option 1, option 2 or option 3 accordingly. With the guess work, the chance of fooling Prover is 3^{-n}, where n is the number of rounds. If n is large, then the probability to make Verifier fool becomes very low.

V. Illustration with an Example

1. S = {49, 26, 30, 28, 26, 47, 27, 42, 25}
2. C =100
3. M = $\sum_{j \in S} s_j$ = 300
4. B_1 = {49, 26, 25}, B_2= {47, 27, 26}, B_3= {42, 30, 28}.

- **Prover:**

Prover knows B_1, B_2, B_3 and following table is generated, Prover hides all of the cells of the table from the Verifier.

Table 2

S	26	47	28	30	26	42	25	27	49
P	90	213	83	21	73	197	81	299	147
Q	116	260	111	51	99	239	106	25	196
$s_i \in B_1$?	0	0	0	0	1	0	1	0	1
$s_i \in B_2$?	1	1	0	0	0	0	0	1	0
$s_i \in B_3$?	0	0	1	1	0	1	0	0	0

- **Verifier:**

Verifier sees the following table.

Table 3

S	*	*	*	*	*	*	*	*	*
P	*	*	*	*	*	*	*	*	*
Q	*	*	*	*	*	*	*	*	*
$s_i \in B_1$?	*	*	*	*	*	*	*	*	*
$s_i \in B_2$?	*	*	*	*	*	*	*	*	*
$s_i \in B_3$?	*	*	*	*	*	*	*	*	*

Verifier has three choices.

1. Verifier asks to proof $s_i + P_i \equiv Q_i$ Mod M+1(where i=1,....,3m). Prover just reveals the part of the table.

Table 4

S	26	47	28	30	26	42	25	27	49
P	90	213	83	21	73	197	81	299	147
Q	116	260	111	51	99	239	106	25	196
$s_i \in B_1$?	*	*	*	*	*	*	*	*	*
$s_i \in B_2$?	*	*	*	*	*	*	*	*	*
$s_i \in B_3$?	*	*	*	*	*	*	*	*	*

2. Verifier asks to proof $\forall$ i, $\sum_{j=1}^{3m} B_i Q_j$ (Mod M+1) $\equiv$ D_i (Mod M+1) and $A' + \sum_{j=1}^{m} D_j$ (Mod M+1) $\equiv$ 3*C (Mod M+1), (j=1,…, m). In response Prover opens the following part of the table.

Table 5

S	*	*	*	*	*	*	*	*	*
P	*	*	*	*	*	*	*	*	*
Q	116	260	111	51	99	239	106	25	196
$s_i \in B_1$?	0	0	0	0	1	0	1	0	1
$s_i \in B_2$?	1	1	0	0	0	0	0	1	0
$s_i \in B_3$?	0	0	1	1	0	1	0	0	0

3. Verifier ask to proof $\forall$ i, $\sum_{j=1}^{3m} B_i P_j \equiv 0$ Mod M+1 (i=1,2, …, m) and $\sum_{j=1}^{m} A_j + D' \equiv 3*C$ Mod M+1. In response Prover reveals the following table.

Table 6

S	*	*	*	*	*	*	*	*	*
P	90	213	83	21	73	197	81	299	147
Q	*	*	*	*	*	*	*	*	*
$s_i \in B_1$?	0	0	0	0	1	0	1	0	1
$s_i \in B_2$?	1	1	0	0	0	0	0	1	0
$s_i \in B_3$?	0	0	1	1	0	1	0	0	0

VI. Conclusion

The Zero knowledge protocols are primarily used in the design of various cryptographic protocols to provide

authenticity. In this paper, a novel zero knowledge protocol has been proposed based on Bin Packing Problem by considering it as a special case of 3-PARTITION problem. Here, the positive use of a NP-Complete problem is pointed out. In future we would like to improve our protocol by using timer, where Prover will be given a specific time period to reply the challenges of the Verifier and also want to apply this protocol in numerous real life applications, in various two party and multi-party cryptographic protocols.

Acknowledgment
The authors would like to thank University Of Calcutta, West Bengal, India, Department of Science & Technology (DST), New Delhi, for financial support and the reviewers for their constructive and helpful comments and specially the Computer without which no work was possible.
.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2011.
[2] A. Kahate, *Cryptography & Network Security*. Tata McGraw-Hill Education, 2011.
[3] M. R., Garey and S. J. David, *Computers and intractability*. Vol. 29. wh freeman, 2002.
[4] H. Aronsson, Zero knowledge protocols and small systems.
[5] D. Catalano, R. Cramer, I. Damgard, G. Di Crescenzo, D. Pointcheval, & T. Takagi, *Contemporary Cryptology*. Springer Science & Business Media., 2006.
[6] S. Goldwasser, M. Silvio, and R. Charles, "The knowledge complexity of interactive proof-systems." *Proceedings of the seventeenth annual ACM symposium on Theory of computing*. ACM, 1985.
[7] G. I. Simari, "A primer on zero knowledge protocols." *Department de Ciencias e Ingeniaria de la Computacion*, 2002.
[8] A. Fiat and S. Adi, "How to prove yourself: Practical solutions to identification and signature problems." *Advances in Cryptology—CRYPTO'86*. Springer Berlin Heidelberg, 1987.
[9] U. Feige, F. Amos, and S. Adi, "Zero-knowledge proofs of identity." *Journal of cryptology* 1.2, 1988: 77-94.
[10] L. C. Guillou and J. J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge", *Advances in Cryptology-Crypto\'88*, vol. 403, pp.216-231.
[11] L. Fouard, D. Mathilde, and L. Pascal, "Survey on electronic voting schemes." *Survey on Electronic Voting Schemes* 2007.
[12] K. Gopalakrishnan, M. Nasir, and L. Vora, Poorvi, "Protocols for watermark verification." *IEEE MultiMedia* 4,2001: 66-70.
[13] P. T. Tuyls, and M. Bruce, "Efficient implementation of zero knowledge protocols." U.S. Patent No. 7,555,646. 30 Jun. 2009.
[14] D. Sensarma, and S. Sen Sarma. "A NOVEL GRAPH BASED ALGORITHM FOR ONE DIMENSIONAL BIN PACKING PROBLEM.", *Journal of Global Research in Computer Science* 5.8 (2014): 1-4.
[15] M. R., Garey and S. J. David, "Complexity results for multiprocessor scheduling under resource constraints." *SIAM Journal on Computing* 4.4, 1975: 397-411.
[16] M. Blum, "How to prove a theorem so no one else can claim it." *Proceedings of the International Congress of Mathematicians*. Vol. 1. 1986.
[17] R. M. Karp, "Reducibility among combinatorial problems." springer US, 1972.
[18] O. Goldreich, M. Silvio, and W. Avi, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems." *Journal of the ACM (JACM)* 38.3, 1991: 690-728.
[19] J. Mohajeri, "Zero-Knowledge Proofs for Independent Set and Dominating Set Problems." *Combinatorics Advances*. Springer US, 1995. 251-254.
[20] J. Mohajeri, "A Zero-Knowledge Proof for Vertex Cover Problems." *Scientia Iranica* 6.1, 1999: 39-43.
[21] D. Grigoriev, and S. Vladimir, "Zero-knowledge authentication schemes from actions on graphs, groups, or rings." *arXiv preprint arXiv:0802.1661*, 2008.
[22] A. Juels, and P. Marcus, "Hiding cliques for cryptographic security.", *Designs, Codes and Cryptography* 20.3, 2000: 269-280.
[23] A. Santis De, G. Crescenzo Di, O. Goldreich, & G. Persiano, "The graph clustering problem has a perfect zero-knowledge interactive proof.", *Information processing letters* 69.4, 1999: 201-206.
[24] C. Tang, L. Zhuojun, and L. Jinwang, "The Statistical Zero-knowledge Proof for Blum Integer Based on Discrete Logarithm.', *IACR Cryptology ePrint Archive* 2003, 2003: 232.
[25] S. Goldwasser, M. Silvio, and R. Charles, "The knowledge complexity of interactive proof-systems.", *Proceedings of the seventeenth annual ACM symposium on Theory of computing*. ACM, 1985.
[26] G. Brassard, and C. Claude, "Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond.", *Foundations of Computer Science, 1986., 27th Annual Symposium on*. IEEE, 1986.
[27] A. De Santis, Crescenzo G. Di, and P. Giuseppe, "Secret sharing and perfect zero knowledge." *Advances in Cryptology CRYPTO'93*. Springer Berlin Heidelberg, 1994.

BIOGRAPHIES

Debajit Sensarma is presently pursuing his PhD degree from the department of Computer Science and Engineering, University of Calcutta, Kolkata, India with DST INSPIRE Fellowship. He has published several papers in International journals and conferences.

Dr. Samar Sen Sarma is presently working as the Professor of the department of Computer Science and Engineering, University Of Calcutta, Kolkata, India. He has published several papers in International journals and conferences.