International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.295-304
http://dx.doi.org/10.14257/ijsia.2016.10.6.28

A Research Survey of Ring Signature Scheme and Implementation Issues

F. A. Alahmari[1], Turki. A. Alqarni[2] and Jayaprakash Kar[3]

[1,2]Department of Information Technology
[3]Department of Information Systems
Faculty of Computing & Information Technology
King Abdul-Aziz University, Kingdom of Saudi Arabia, Jeddah-21589
jgopabandhu@kau.edu.sa

Abstract

In this paper, we have presented a study on traditional group signatures, which is the Ring Signature T out of n threshold and discuss its implementation issues. Also, we outline the security issues. In threshold Signature Scheme the information can be encrypted and decrypted, only if T numbers out of n numbers (t<n) in the group use their secret keys. As compare to the traditional ring signature scheme, it is more efficient that can prevent spurious or fake messages issued in the name of a reputed group by a compromised personnel in the group.

Keywords*: key Replacement attack, threshold signature, El-Gammal Encryption, group signature*

1. Introduction

Ring and group signatures are technologies used for signing the data by an individual or some of the group members. Ring signature technology simply hides the individual who signs the data before sending. It is not an easy task to find out the original signer. Firstly, in 2001, Ron Rivest *et. al.*, developed the Ring signature and presented in ASIACRYPT. In the ring signature scheme, a group is defined and everyone has their own signature in the group. One individual or a group of individual can sign the data for encrypting or decrypting. Security of ring signature is computationally infeasible to find out the secret keys of individuals participating in the scheme keys that are required to generate the signature.

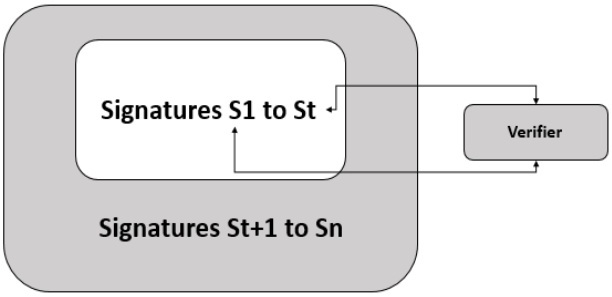
Ring signatures are like group signatures yet contrast in two key routes: initially, individual signatures cannot be modified and a group can be formed by any number of persons. Thus a signature, which is anonymous utilizing the multiple public keys is generally termed as a Ring Signature [12]. Ring signatures portray as an approach to release a mystery. For example, a ring signature could be utilized to give a mysterious signature from "a high-positioning White House official", without uncovering which official signature the message. The advanced signatures have broadly been utilized to give administrations, for example, element verification, information starting point validation, non-denial, and information uprightness. Mysterious computerized signatures are an exceptional sort of advanced signature. In a mysterious advanced signature plan, provided a computerized signature, an unapproved element, along with the verifier, can't find the endorser's identifier. However, such a plan still has the property that just a genuine underwriter can produce a legitimate signature. One of the real contrasts between a routine advanced signature furthermore, an unknown advanced signature is a way of the general population keys utilized for performing the signature check. To check a traditional advanced signature, the verifier adjusts utilization of the solitary open check key that is

ISSN: 1738-9976 IJSIA

bound to the endorser's identifier. To check a mysterious advanced signature, the verifier brings out the utilization of either an open our key or numerous open keys which aren't constrained only to an individual signer. The Ring signatures are regularly treated as a streamlined signature group, but gathering chiefs won't be there. In the event that ring signatures are identified with this thought of gathering signatures, they are without a doubt very diverse. From one point of view, the group signatures have the extra component which the obscurity of an end user might be renounced *i.e.,* the endorser could be followed by an assigned group chief and with regards to another point of view, the ring signatures permit more noteworthy adaptability: no incorporated group director or coordination among the different clients is required. In reality, clients might be unconscious about each other while they open keys will are created. In addition, the obscurity of the underwriter is genuinely insured. The first inspiration was to permit insider facts to be spilled namelessly. For instance, a high-positioning government authority can sign data regarding all the ring comparably high-positioning authorities.

Hence, data could be confirmed, then as originating from the somebody legitimate left out to uncover the real signer. Thus a ring signature gives the nameless of an endorser that implies that the verifier realizes the signer as an individual ring, yet is not aware of the endorser. Additionally, a real way to renounce the obscurity of the signer is not available. In 2004, Herranz and Saez gave some security decisions for ring signature plans. Dodis *et. al*., Proposed steady size ring signatures utilizing the Fiat-Shamir change. In the standard model Xu *et. al.,* Displayed a secure ring signature; however, their verification was not redressed. Next, Chow *et. al.,* in the standard model demonstrated the security plan of ring signature, however, in view of a new solid supposition. In 2007, Shacham and Waters, advanced the main productive ring signature, secure exempting the irregular oracles and in view of standard suspicions.

Threshold Signature Scheme is shown below in which the information can be encrypted and decrypted, only if T numbers out of n numbers (t<n) in the group entered their private password. This is really more efficient than that of the traditional ring signature scheme in preventing spurious or fake messages issued in the name of a reputed group by a compromised personnel in the group.



t = No of signers and n = Total members

Ring signature has security worries as it is a group focused signature: where each verifier could be persuaded that a member of the group had signed the message, yet the real signer stays obscure. A few ring signature plans in light of bilinear pairings have been proposed. Be that as it may, computational many-sided quality for matching algorithms of these ring signature plans becomes straight with the span of the ring. The Ring signatures normally loan themselves to an assortment of uses and can likewise be utilized to give an individual from a specific class of client's access to a specific asset without expressly recognizing this part. Here it is important to make note, that there might be situations when the outsider's unquestionable status is required for example, to demonstrate the resources were accessed. Thus the ring signatures, instead of specially appointed ID plans,

are required. At last, it is noticed in the application to assigned verifier signature, particularly during the connection of email. Hence, the ring signature empowers the email sender for signing the message concerning the ring accommodating the sender and the collector. The beneficiary is guaranteed where the email started in distinction to the sender however can't demonstrate this to any outsider hence it is adequate to utilize a ring signature plan that bolsters just rings with two sizes.

2. Related Works

Similar to the other works in this study we can see the implementation of the scheme of the threshold ring structure by t out of n certificate. The recent as well as the active set of Security models was implemented to validate the security. This model grabs the new adverse potential which is known as User partial key Replacement attack [2]. It is designed as an efficient and reasonable model for security, but they were not in use primarily. Then later the new scheme called Certificateless Theshold Ring Signature (CL-TR) have been introduced which is depending on the purpose of signature verification with the help of pairing operations. It has got a compressed size of the signature, there by a true to non-signers comparatively than that of real signers. In this study we can also find the implementation of 1-out-of-n CL-TRS which has got the largest powerful verification over the entire certificate less ring signature schemes currently present. Hence the study says that the implementation of security models for the purpose of fraudulent signature, also uncertainty of CL-TRS displays that they are powerful than the other security models [2]. It is distinguished to the similar method of security for regular PKI-based ring signature. The uncertainty to control all the production of mater public key and participant's keys with that of the previously used keys which are made competitor improves the definition to be efficient. The study of another important definition of ring security is the proposal of 1 out of n CL TRS and also t out f n CL TRS methods. It's more reliable than the CL-TRS security model. It is because of its more calculating capacity and powerful signature type than the C-TRS. In extension to that the signature size is thick, even to the sum non signer than original signers [2]. This study says about for every increase in the implementation of the ring members for actual signers there will be sufficient increase in the efficiency of the security scheme in which they are familiar with the threshold signatures, ordinary PKI-based settings or called the settings of identity based in which signature size similar to the original signers [2].

In this study we could find two distinct algorithms used to execute efficiently for the purpose of ring signature generation. However, they are given an integer size (I), these algorithms helps to find memory and time effectively with two distinct I/2-bit primes (e1, e2) such that the prime integer will be e=2e1e2+1.The primary algorithm which is known as naive algorithm deals with the storage of O(I)bits and to calculate in terms of average, O(I^4) basic bit operations [10].

The second algorithm deals with improvising of the calculating complexity of O (I^7/2) and also the average o (I^3/2) bits. These two algorithms are mainly considered for implementing in mobile devices [13][10]. In which mobile devices have time and space constraints. Hence the major goal of this paper is to increase the processing time. This is done only by reducing the amount of primality tests performed for the numbers having the size to be e j. Here two sets P1 and P2 prime numbers are generated in the intervals. To provide random uniform distribution. Each time prime number r is calculated to which set pi belongs. Finally, the primality is verified this process is iterated for several times till the needed processing is reached. So the amount of memory will increase with the corresponding increase in the prime numbers e1 and e2. [10] The estimation is based on the theoretical results. In this paper, we study about the key generation process for a ring signature protocol. Here two different approaches for key generation are concentrated for the purpose of preserving memory and processing time.

So in both algorithms Miller -Rabin Primarily test is utilized in which they have its computing complexity of O (I^3). The study says that both the methods are meaningful with respect to their original goals. However, the disadvantages of these methods are memory, which does not satisfy the processing time to the recent devices. The cost is more expensive that the memory needs to speed up the process [10][15].

The study of ring signature is studied in this paper, since it is categorized as a group oriented signature. It makes the group member to put sign in favor of the group without notifying his/her identification. [10] So the verifier reveals that the signature was reproduced by a member of the ring. But they cannot able to retrieve the signature. The convertible signature is implemented in order to find the real signer. It is made by converting the ring signature in a normal signature by producing the security information regarding the signature of ring. So the real message client can justify the owner of the ring signature whenever they are needed. In this method the other members who are in the group cannot derive the ownership of the ring signature [9][14] implemented derived ring signature based on the ElGamal signature schemes. Wang *et. al.,* produced the result that the convertibility scheme of Ren and Harn doesn't fulfill the results because of the single member accessibility. He says that everyone in the group of ring signature has the right to demand those who produce the ring signature. In this paper enhanced version of Ran and Harn's scheme were proposed to overcome the drawbacks of the previous scheme. [10] The introduced scheme permits the original message signer to determine the verifier that he/she has ability to generate the ring signature. The security analysis of the enhanced scheme is same as those of Ren and Harns scheme irrespective of the flexible message that is selected outbreaks in the model of random oracle.

From the study of this paper gathered knowledge about the generalized scheme of the ring signature. It is an innovative and appropriate cryptographic method. [10] This paper deals with the security scheme of the drawbacks of Ren and Harn's generalized signature. The improved scheme fulfills the convertibility. In this method, none can act like authentic signer to alter a ring signature into a normal by acknowledging protective information regarding the ring signature successfully. Furthermore, the secure generalized multi signer signature scheme was installed. It has made to raise the confidence level with increased efficiency. The protective analysis of implemented method is similar than the previous scheme. From this I came to know about the ring structure is efficient. [8] This paper deals about the design of the linkable ring signature scheme with definite anonymity. [8] The implementation of the unconditional anonymous linkable ring signature scheme has been restricted. Later on there was a found a solution to rectify the open problem. It is by providing a detailed concrete instance, which is tested to be the secure random oracle model. This paper has implemented other scheme where the construction is effective than the previous one. It implements only the computational anonymity. [8] The previous paper does not produce strong anonymity; in this paper, it was implemented like that to meet the strong anonymity. The efficiency of the scheme has done by comparing with the other schemes. It is found that the scheme used in this paper is more economical for signing and verification. No pairing operations required for this paper. Here the number of exponentiation and the multi bases exponentiation operation remains constant. Since the private keys own the person, it will calculate the actual signer easily. The security investigation is made by the computational analysis on which the system relies. To validate the protection of the system discrete logarithm issue is determined. If DLP is hard the linkable scheme of ring signature will be fraudulent in the Random Oracle Model. It is linkable when DLP is hard. Hence the study of this paper reveals that the method proposed in this paper provided it as a reliable one for having a linkable scheme of ring signature with unconditional anonymity. So the scheme produced in this paper is more economical and constructive. [8] This scheme is reverse to the public keys who own the signature and the condition is always untrue. It defines that the mandatory linkable ring signature cannot give strong anonymity, but this scheme results

in the strong anonymity under the analysis. [8] The security of this scheme depends on the random oracle model. The disadvantage of this study is that it reduces the size of the signature. The main drawback is that signature size should be independent to the users in the ring [8]. However, the ring signatures facilitate the user unspecified signature as a information on favor of group of users. [7] In this paper, the author implemented the first ring signature scheme. In which it has a size of O (log2N), the N is said to be the number of users in the ring. They successfully achieve this outcome by enhancing the Chandren *et. al.*,'s method (2007). It utilizes the common reference string and un communicated zero-knowledge proofs. The security analysis is made by themselves without depending on the random oracles. The design of ring signature consists of stepwise process. It consists of 4 probabilistic polynomial time (PPT) algorithms. The logarithmic sizes are constant and public. Here the signer knows where the verification to be made with the verification keys in the ring. It is based on the Boneh-Boyen signature method, where the signer constructs the signature. The signer chooses one-time signature keys. The message is signed preceding the signature scheme. In the next step signer need to hide the certifying signature. [7] Finally the person validates the committed verification key is the component of ring S. The security parameter is given as an input and it generates the common reference string. The next step is comprising o giving the common reference string as an input and it gives the public verification key as well as private signing key as an output. Finally, the input message is given with the ring it outputs a signature with a valid key pair by Key Gen. An input of message bearing a signature based on the rings of public key. The signature is verified perfectly. Hence based upon the study design of the first ring signature scheme is made. The logarithmic size produced in this scheme helps to give a number of users in the ring by providing uneven size as a result. The scheme in this paper requires common reference string for analyzing the security without depending on random oracles. [7] This article deals about the function of the group signatures. The main functions are the status of the signers and also the group which exists the important secure information needed for the signer's security. ("A New Type of Ring Signature Scheme Based on Group Signatures Idea", 2013) So in this paper I get to know about the operations and also the combined method of group signature along a ring signature to construct a ring group signature. It establishes the method of the groups available leaving out defining that who and which group's member of has implemented the signature. The major contribution of this article is a basic explanation of a ring group signature method and the privacy model. Both the framework and the objective of the scheme have been tested to be secured, and if the hidden group signature and the ring signature scheme are made to preserve. The structure of the RGS schemes depends on the description of GSs and RSs. The ring and the groups indicate the list of security parameters. The main criteria are the sizes, public relation and secret keys for the group provider. The ring group signature method be found in the form of an ordered list of protocols and the algorithms.

The group key generation algorithm develops their group key. ("A New Type of Ring Signature Scheme Based on Group Signatures Idea", 2013) The protocol which is made to join in each group member creates the values and documented in the group registration table. The values are run with the ring group signing algorithm that design the ring group signature. The values are run with the ring group signing algorithm that design the ring group signature Hence, in this paper the concept of ring group signatures has been implemented with the basic description of the order and the security. It devices the set of interesting properties, definiteness, signer-anonymity, signer-traceability, signer-non-frame ability and group-uncertainty. This paper gives the conferred construction of RGS scheme. It is validated that any RGS scheme succeeding this framework takes care of 5 properties till the GS scheme is protected. In this scheme the security analysis depends on the model of the random oracle. The resulting ring group signatures would assist any operations regarding the group signatures, where the group identities are receptive. ("A

New Type of Ring Signature Scheme Based on Group Signatures Idea", 2013). In this paper the discussion and comparative study of first ring signature is made. Revisit *et. al.*, (2001) who implemented the first ring signature. He implemented many other schemes expanding the authentic 1 out of n ring signature [6]. Taking for an example t out of n threshold ring signatures are defined, investigated regularly. Then later came to know that in threshold ring signature scheme, the careless irregular number generation will control the protection of threshold structure of the ring. Here in this paper it is described about the accountability of the deriving careless random number. It has given the explanation for the worries as well as achieve security analysis for the alterations. Hence from the study gathered information regarding the issues in the threshold ring signatures that are drawn from the generation of random numbers. The signer ambiguity and fraudulency seriously requires protective properties in ring structure schemes. This paper used a scheme which is a separable threshold of the ring signature. This scheme produces the security and it is validating in their paper [6]. Here the probability for assuming the real signer is taken as t/n. It generates the random numbers. The random numbers are located in the specific fields. There are no specifications to derive the random numbers.

The next step is the key generation, Here the signer is defined those who are not honest in the ring signature. The implementation of random numbers is to disclose the identification of non-signers. When needed. To drop down the signer ambiguity the random numbers produces the cryptographic hash functions. To summarize the algorithm, the careless random number initiates and gives the chance to invalidate the non-signers. The random number generation is a most avoided portion in the threshold ring signature schemes. This causes deadly damage to the signer ambiguity. When two or more signers use the random number generation the issues will be solved. This paper discusses about the random number generation and the disadvantage is it affects the signers noticed [6]. This paper discusses about the two new identifications based on the threshold ring signature schemes. In this scheme, any set of individual immediately induct the arbitrarily n-t individuals to achieve a publicly authenticated t-out-of-n signature in favor of the group of n members [4]. But still the original signers remain ideal. It is validated to be presently non-fraudulent over the adaptive chosen message and identification attacks and unqualified signer ambiguity inferior to the random oracle model. Trusted certification authority requires a traditional public key framework to provide a certificate to the identity and the public key of an individual [4][14]. This results in the issues of certificate management. To overcome the problem Shamir (2001) described an identity based public key cryptography which requires an authentic private key generator. Initially characterize the concept of ring structure by taking the trapdoor one-way function in to concern [3]. So the generated ring signature can assure the arbitrarily verifier regarding the message send by one of the member of the ring but none identified the real signer over the ring members. Hence the ring signature is taken into consideration and verified for the cost effectiveness for signature generation and verification. The study in this paper reveals that they use n+1 pairing operations and 4n exponentiation functions [4]. In this scheme it needs only 2 pairing operations and 2n+1 exponentiation functions. Based on the signature size it is studied that it is effective when the threshold ring signature scheme doesn't pair from polynomial [4].

3. Implementation Issues

Carlos Aguilar Melchor, Pierre-Louis Cayrel and Philippe Gaborit formerly [1] initiated the t-out of N Threshold Ring Signature. It works ultimately on the basis of shorter Distance Issue probably the Syndrom Decoding Issue. A particular public key is shared among most persons in this scheme with a little modifying of the Stern identification.

a. Common Implementation Aspects

Every application is performed only with the Stern Execution. These may include Java and C execution. They are the easy and quick means of implementing the approach. The t-out-of-N authentication is the only application to be processed with such cases and moreover the Fiat-Shamir Paradigm makes the use of generating the signature scheme.

	Key Formation, 20 key pairs	**Key Formation, average time per key pair**	**Authentication of 20 laps**	**Authentication, average time per lap**
Java	65254ms	3262ms	62871ms	3143 ms
C	166890ms	8344ms	19381 ms	969ms

b. The Java Implementation

Java Execution Process is normally works under the guidance of the Stern Implementation type of Java. There is a particular Static Configurator which performs the storage of extra condition classes like t and N which shows the direction to other sub parameters too. But everything works under the influence of only the Stern class that could not be modified at any case.

c. Implementation in 'C' Programming Language

Implementation in 'C' is a better evaluation scheme working under the similar category of Stern execution. The necessary input files can be taken from the storage classes of Stern type which indicates as such, they are the sub storage classes under the Main type.

d. Timing Schedule

The timing results obtained on Athlon X2 4200+, 2 GB memory and the parameters chosen are n=1024, r=512, w=32, N=10 and t=10.

The Java implementation produces faster key formation in comparison to the C Execution. But

The authentication is always better and faster in C the implementing process.

e. Implementation of GPU of a Protective Lattice-based Stream Cipher

As Fevrier explored [5] this is a process of building a lattice-based stream cipher under the protection basics with the help of Short Integer Solution (SIS). This is highly a protection based approach with a pseudo-arbitrary processor. This pseudo-arbitrary processor provides some order of sources which could be mingled with the existing source files. These mixed up source files provide a different approach of adopting high progress and effectiveness. Both the area and speed could be advanced with such approach method. This is hopefully a good method in recent times which other process methods really cannot do. Hence this construction will always result in better achievement of security.

f. Implementation of GPU of a Provably Secure Lattice-based Stream Cipher

Fevrier *et. al.,* constructed a lattice-based stream cipher using the provable secure hardness of the Short Integer Solution (SIS) problem as security basis [5]. They applied the standard approach of building a pseudo-random generator, which produces a sequence to be combined with the clear text. Moreover, as an alternative to gain efficiency both in terms of space and speed, they suggested the use ideal lattices in the cipher construction. Currently, there is no known attack that could exploit this choice.

3. Security Discussions

There are a lot of security issues posed with ring signature. Formerly let us begin with One-more-RSA-inversion issue. They are the most recent approaching issue which could be taken as an initiative for solving with the Chaum's RSA blind signature [3] program. They had posed as an extreme end problem so that it can be a better out coming process method. As a beginning level, they created a process and could be started with a great support.

This Blind signature Approach provides a digitaized processing in cryptography, especially with the cash handling processes. As this is a vital process to be handled seriously, the security issue comes to be a very essential handling program. For this problem, we use this approach which allows the person to provide required documents of Signature with a token which is highly confidential. That token cannot be shared with the other users and even bank personnel. This leads to the production of e-coin with a better validity. Hence their way of approach is really amazing with easy tasks and conditions. Better security could be provided with such a simple approach and even standardized range. They process on multiple areas with this RSA function and features as a base to achieve progress.

4.1. The Distance among Proofs and Practices

There is always a reality between the proofs and practices. [15] views of Crypto graphical methods of approach in earlier cases created a distance among the creating and executing methods. Because creation always differs widely from the execution problems. So the assumptions made was to exhibit RSA method of approach for the security threat. This was because of its cost effective nature and simple approaching. Experts in this area will always prefer to such approaches as they created a good strength at their mind and added ideas. Always preferring standardized method will result in best security. Their designs mostly concentrate on clear and direct idea work. So if these common basic methods are rejected, they can go for the other standard approaches. Even though the newer ones seem to be expensive, their replacement could be done in a better way for higher efficiency.

4.2. Creating New Assumptions

The strength of these functions could be progressed with better understanding and approaching functions. The designers could concentrate on more clear and precise basis for systematic security results so that it can be made even better. The problems could also be related to various multiple areas and tasks. There is a bilinear pairing method which is used for evaluating ID-based ring signature using singular elliptic or hyper elliptic curves. This is highly a better approach for improving efficiency and reducing the signature size with a factor of 2.

This could be a certified key, forming approach where security and key role are an essential thing. This proposal is highly based on the bilinear pairing. This approach is designed for the electronic type of vote or cash systems. But there are also proposed problem with such approaches parallel with ROS –issue. In order to overcome such issues we require minimum 1600 bits long q values. Hence this method also proves to be a common issue under progress. Standardized proof could be made sooner for such security issues.

5. Conclusion

In this paper, we have presented the survey of the ring signature scheme that highlights the current developments of ring signature, such as a novel ring signature scheme that implements the provision for exposing the rank of leaker, which could be useful in many cases and proposal of new algorithms that make the RSA problem even more difficult. Further, this survey addresses the computational anonymity issue of various ring signature schemes and exposed that many of the ring signature schemes are only safe as long as mathematical problems associated with the ring signature scheme remains unsolved.

Acknowledgements

We would like to thank to our supervisor Dr. Jayaprakash Kar for his valuable suggestions and comments that helped improving this work. This support is greatly appreciated.

References

[1] C. Aguilar Melchor, P. Cayrel, P. Gaborit and F. Laguillaumie, "A New Efficient Threshold Ring Signature Scheme Based on Coding Theory", *IEEE Trans. Inform. Theory*, vol. 57, no. 7, **(2011)**, pp. 4833-4842.
[2] S. Chang, D. Wong, Y. Mu and Z. Zhang, "Certificateless Threshold Ring Signature", *Information Sciences*, vol. 179, no. 20, **(2009)**, pp. 3685-3696.
[3] D. Chaum, "Blind signatures for untraceable payments", In D. Chaum, R. Rivest, and A. Sherman, editors, *Advances in Cryptology – CRYPTO' 82*, Lecture Notes in Computer Science, Plenum Press, New York and London, **(1982)**, pp. 199–203.
[4] L. Deng and J. Zeng, "Two new identity-based threshold ring signature schemes", *Theoretical Computer Science*, vol. 535, **(2014)**, pp. 38-45.
[5] F. Samedi, P. C. Pierrie-Louis and Rosemberg Silva, "Implementation on GPU of a provably secure lattice-based stream cipher", **(2011)**.
[6] P. Gauravaram and L. Knudsen, "Security Analysis of Randomize-Hash-then-Sign Digital Signatures", *Journal Of Cryptology*, vol. 25, no. 4, **(2011)**, pp. 748-779.
[7] C. Gritti, W. Susilo and T. Plantard, "Logarithmic size ring signatures without random oracles", IET Information Security, vol. 10, no. 1, **(2016)**, pp. 1-7.
[8] J. Liu, M. Au, W. Susilo and J. Zhou, "Linkable Ring Signature with Unconditional Anonymity", *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, **(2014)**, pp. 157-165.
[9] J. Ren and L. Harn, "Generalized Ring Signatures", IEEE Transactions On Dependable And Secure Computing, vol. 5, no. 3, **(2008)**, pp. 155-163.
[10] J., Piles, J., and Tornos, J., "Efficient ways of prime number generation for ring signatures", IET Information Security, vol. 10, no. 1, **(2016)**, pp. 33-36.
[11] J. Kar, "Online/Offline Ring Signature Scheme with Provable Security", *IEEE International Conference on Intelligence and Security Informatics (IEEE ISI 2015*), US, **(2015)**, pp. 197-197.
[12] J. Kar, "Low Cost Scalar Multiplication Algorithms for Constrained Devices", *International Journal of Pure and Applied Mathematics*, vol. 102, no. 3, pp. 579-592.
[13] J. "Provably Secure Online/Off-line Identity-Based Signature Scheme for Wireless Sensor Network", *International Journal of Network Security*, Taiwan, vol. 16, no.1, **(2014)** Jan., pp. 26-36.
[14] J. Kar, "Authenticated Multiple-Key Establishment Protocol for Wireless Sensor Networks", "Case *Studies in Secure Computing Achievements and Trends", CRC Press, Taylor and Francis (New York)*, Chapter-04, Catalogue No- K21540, Print ISBN: 978-1-4822-0706-4, eBook ISBN: 978-1-4822-0707-1, DOI: 10.1201/b17352-5, **(2014)**, pp. 67–88.
[15] Wagner, "A generalized birthday problem", *Advances in Cryptology-Crypto 2002*, LNCS 2442, Springer-Verlag, **(2002)**, pp. 288-303.

Authors

F. A. Alahmari, is pursuing M.S in Information Technology at Faculty of Computing & Information Technology, IT Department, King Abdul-Aziz University, Kingdom of Saudi Arabia, Jeddah. His current research interest is on Security and Privacy in Cloud Computing, Data Science and Cryptography.

Turki. A. Alqarni, is pursuing M.S in Information Technology at Faculty of Computing & Information Technology, IT Department, King Abdul-Aziz University, Kingdom of Saudi Arabia, Jeddah. His current research interest is on Network Security, Cryptography and development of security protocols for social media.

Jayaprakash Kar, has received his M.Sc and M.Phil in Mathematics from Sambalpur University, M.Tech and Ph.D in Computer Science (Cryptographic Protocols) from Utkal University, India. Currently he is working as Assistant Professor in the Department of Information Systems, Faculty of Computing and Information Technology. He is actively associated with Information Security Research Group, King Abdulaziz University, Saudi Arabia. His current research interests is in development and design of provably secure cryptographic protocols, and primitives using Elliptic Curve and Pairing based Cryptography

