**Bulletin of Electrical Engineering and Informatics**
Vol. 10, No. 1, February 2021, pp. 487~492
ISSN: 2302-9285, DOI: 10.11591/eei.v10i1.2493


# Research trends review on RSA scheme of asymmetric cryptography techniques

**Mohd Saiful Adli Mohamad[1], Roshidi Din[2], Jasmin Ilyani Ahmad[3]**
[1]School of Quantitative Science, UUM College Arts and Sciences, Universiti Utara Malaysia, Kedah, Malaysia
[2]School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia, Kedah, Malaysia
[3]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Kedah, Malaysia

**Article Info**

***Article history:***

Received Apr 9 , 2020
Revised Jun 17, 2020
Accepted Jul 30, 2020

***Keywords:***

Integer factorization
Public key cryptography
RSA scheme

**ABSTRACT**

One of the cryptography classifications is asymmetric cryptography, which uses two different keys to encrypt and decrypt the message. This paper discusses a review of RSA scheme of asymmetric cryptography techniques. It is trying to present the domains of RSA scheme used including in public network, wireless sensor network, image encryption, cloud computing, proxy signature, Internet of Things and embedded device, based on the perspective of researchers' effort in the last decade. Other than that, this paper reviewed the trends and the performance metrics of RSA scheme such as security, speed, efficiency, computational complexity and space based on the number of researches done. Finally, the technique and strengths of the proposed scheme are also stated in this paper.



***Corresponding Author:***

Roshidi Din,
School of Computing, UUM College Arts and Sciences,
Universiti Utara Malaysia,
06010, Sintok, Kedah, Malaysia.
Email: roshidi@uum.edu.my

## 1. INTRODUCTION

Data security is a main concern in communication to ensure the data is transfer securely from sender to receiver through communication media. One of the techniques used in data security is cryptography. This is done by changing the original message to the unreadable form before data transmission through public network. The data is secured if the third party could not understand the original message. The process of changing the original message or plaintext to an unreadable form or cipher text is called encryption, while the backward process of it is called decryption. According to Mushtaque *et al.* [1] cryptography can be described as a practice to keep the data secure from the illegal users. The point of cryptography is to ensure data is send in a secure environment over network by encrypting the data to an unreadable form [2]. Other than that, in cryptography, keys are used to ensure the confidentiality of data. Only the authorized person which has the authority to use the key can encrypt and decrypt the message.

Basically, cryptography is classified into symmetric and asymmetric cryptography. The symmetric cryptography mechanism involves with only a key. This key will be used by the sender and receiver in data communication to encrypt and decrypt message respectively. One of the advantages of symmetric cryptography is relatively fast due to only one key involves in the data communication. However, because of this technique uses only one single key, the message is not safe if the key is seen by the unauthorized users. Thus, it will be easy for them to decrypt the message illegally. Hence, in order to solve the problem in symmetric cryptography, the asymmetric cryptography was initiated. The asymmetric cryptography mechanism involves with two different keys which are known as public and private key [3]. The public key

can be shared among the senders to encrypt whereas the private key is used to decrypt the ciphertext and kept secret to the authorized receiver only. As long as the private key is kept secret, it is said to be secured [4]. Normally, in asymmetric cryptography, the public key is used to encrypt the original plaintext while the private key is used to decrypt the unreadable text. Other than that, in asymmetric cryptography, many schemes were introduced to perform the encryption and decryption process for data communication such as Diffie-Hellman, RSA, McEliece, Goldwasser-Micali, and ElGamal.

On the other hand, those introduced schemes can be classified in different cryptography algorithms based on the technique used. The cryptography algorithms include discrete logarithm, integer factorization, coding theory and elliptic curve. Schemes are normally categorized to theory-based, lattices-based and codes-based [5]. RSA scheme [6] is one of the asymmetric cryptography scheme which is categorized under integer factorization algorithm. The scheme is depends on a two prime number factoring technique. The strength and security of this scheme depends on the complexity of factoring the prime numbers. In order to increase the strength including the speed in encryption and decryption of the schemes, early researchers have improved the initial scheme by rising the number of private keys [7], by utilizing two public keys [8], three prime numbers [9], four prime numbers [10], and 'n' prime numbers rather than two [11-13].However, as the size of the key increases, it will take more time for larger files [10, 14].

The previous literature has shown an important contribution to RSA scheme since it was created. The performance metrics, domains and techniques are studied to perceive the trends and the research patterns of RSA scheme in earlier studies within last decade. The continuing sections of this paper is organized with section 2 that presents the overview of RSA scheme, section 3 demonstrates the findings gained from the earlier studies, and discussions related to the techniques, the domains and the performance metrics of RSA scheme between earlier researchers. Finally, section 4 will conclude the research contribution in this paper.

## 2. OVERVIEW OF RSA SCHEME

RSA scheme was introduced in 1978 which uses the factoring technique of two prime numbers [6]. The RSA scheme uses asymmetric cryptography system that involves two types of key; public and private key for the encryption and decryption processes respectively. The public key is placed in a public file, and the decryption procedure is kept secret by the user. In order to encrypt the plaintext, a pair of positive integers is generated. In the same way, to decrypt the cipher text, a pair of positive integers is then generated. These prime numbers are very large and the factorization of it will be hidden from others. However, by using RSA scheme, the original message can easily be accessed by knowing the transmission of the public key if there is no difficulty involved in the data transmission [10].

Other than that, in order to increase the security of the RSA scheme, [11] also modified the RSA scheme based on 'n' prime numbers is modified. It was proposed to provide higher data security being sent over public network where 'n' prime numbers are difficult to decompose and not easily breakable [12]. Hence, [15] the two prime numbers can be modified to have four prime numbers to increase the complexity of the existing RSA scheme. RSA method assured confidentiality, integrity, authenticity, and non-reputability. The RSA security relies on the computational power to factor the prime numbers. Thus, it is hard to break the RSA scheme as long as it is complicated to factor the integers [16]. Therefore, the most important thing is the proficiency in producing large prime numbers [17].

A modified scheme that based on RSA was proposed, which utilized four prime numbers, together with two public keys for encryption and used a private key for decryption [18]. Thus, this scheme is efficient and robust. Moreover, these two public keys are sent at different time. On the other hand, [19] another scheme was proposed which utilizing four prime numbers. Rather than sending a public key, this proposed scheme sends two public keys to the receiver. Moreover, the analysis of the algorithm becomes more complicated as it uses four prime numbers and two cipher texts for each message. Hence, resulting an increase in the security. However, the speed of RSA decryption is affected, making the chinese remainder theorem (CRT) use it to enhance the speed. Moreover, [20] modified RSA is also proposed which is combined with Montgomery multiplication and chinese remainder theorem (CRT). Although the scheme's execution time is faster, it is not fit for embedded device due to a large key size. Besides, the implementation of RSA encryption with chinese remainder theorem (CRT) which conceal multiple plaintexts in one ciphertext was also introduced [21]. Nevertheless, this scheme speeds up the decryption process of RSA.

Khairnar and Kadam proposed a technique that implements RSA scheme using key pairs and Euclidean algorithm to make it more secure [14]. Moreover, it avoids mathematical and brute force attacks. However, when using this proposed scheme, the key size increased from 512 bit to 1024 bit. Therefore, it spends more time for a larger file and only a single file can be encrypted and transmitted. Other than that, in order to strengthen the RSA scheme, it was modified by implementing several public and private keys [22]. The proposed scheme is depending on the key length as well as on several public and private keys to decrypt the message. On the other hand, the RSA algorithm works by adding some complexity to the three keys [23].

The proposed scheme had increased the security and complexity of the algorithm's speed while maintaining encryption and decryption time. Besides, a secured cryptography mechanism was modified by using multiple encryption which prevents the system from the attacks [24].

On the other hand, a different approach for image encryption was introduced [25]. This approach encrypts the image matrix using three large prime numbers. The benefit of this scheme is it is safe against attacks in the image transmission process. Furthermore, data is not lost in the image decryption process. Besides, the decrypted image is totally different from the original image. Other than that, a cryptography using RSA algorithm to encrypt images by HEX function was also proposed to generate a ciphered image text [26, 27]. This proposed scheme is suitable for secured transmission of images over the Internet. The RSA scheme used was modified for both numeric and images for biometrics. Biometrics will extract the characteristics and then encrypt it using hyper image encryption algorithm [28] to be stored in a database. This scheme had improved the recognition accuracy, thus improved security.

## 3. RSA SCHEME DOMAIN

This section shows the research pattern of the RSA scheme domain. It also discusses the domains, performance metrics and techniques of RSA scheme which demonstrate the most focused area of RSA scheme among researchers in last decade. There are many researchers' works that have contributed in RSA scheme based on the number of the research. Figure 1 shows the pie chart of RSA domain focused by the most researchers.

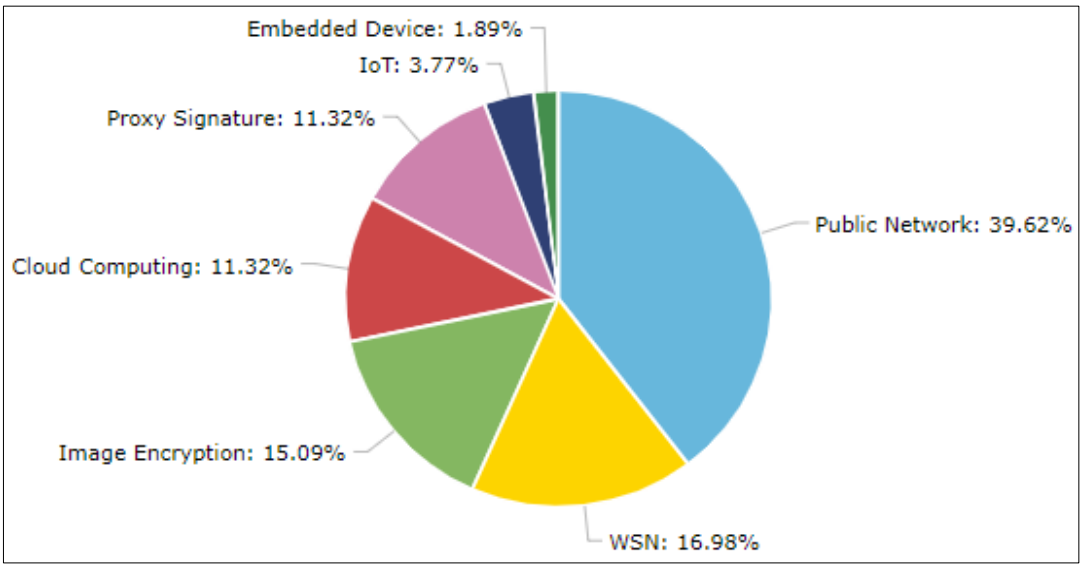


Figure 1. Percentage of RSA scheme's domain for the last decade

From the pie chart, it is clarified that most of the earlier researchers emphasised on public network domain with 39.62%, followed by wireless sensor network (WSN) domain with 16.98%. Next domain is image encryption which contributes about 11.32%. On the other hand, cloud computing and proxy signature domain have shown the same effort by the researchers with only 11.32% each. However, Internet of Things (IoT) and embedded device have shown the lowest percentage of the RSA domain focused by the researchers with only 3.77% and 1.89% respectively. This is because RSA is not suitable for embedded device and IoT which is space constraints since it has large key size [29].The main strength of RSA is security [30, 31] which is suitable for public network and WSN to transmit the sensitive and private information [32] as shown in Figure 2.

Figure 2 illustrates that security is the main attention of RSA [24-40], followed by efficiency [41-45] and speed [20, 29]. However, due to large key size, RSA lack to focus the other performance evaluation used including computational complexity, space, computational efficiency, cost and time complexity. Besides that, based on the previous researches within the last decade, the RSA original techniques were improvised in order to adopt the scheme into various applications as to maintain or enhance the security and speed of the scheme. Table 1 shows the literature of the techniques applied on RSA scheme.

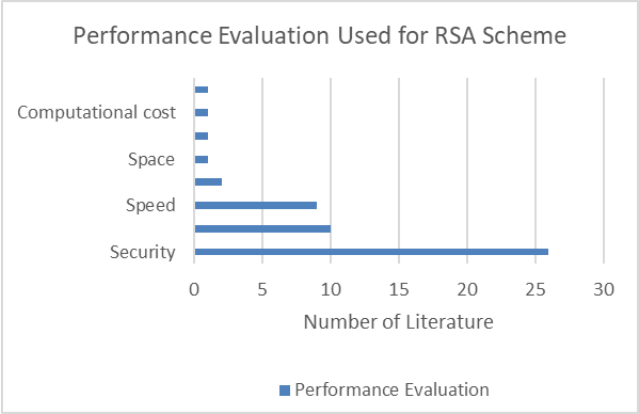


Figure 2. Performance evaluation used for RSA scheme

Table 1. The summary of RSA techniques and strengths

| Techniques | Authors | Strength |
|---|---|---|
| Use for prime of numbers, two public keys for encryption and a private key for decryption | [18] | More secure, Less vulnerable to Brute-Force Attack. The public key is sent separately twice. High communication overload |
| Use four prime numbers | [15] | Increased the complexity–highly secured, not easily breakable |
| | [18] | The analysis of algorithm become more difficult |
| Use the encryption algorithm of RSA cryptosystem with three larges prime numbers to encrypt the corresponding matrix | [24] | Strong security mechanism for data security by using multiple encryptions |
| | [9] | Faster than the original algorithm in encryption and decryption process and generating public and privacy key |
| Strengthen the RSA algorithm by using multiple public and private keys | [21] | RSA depends not only on the key length to decrypt the message. It also depends on several public and private keys |
| Work on the RSA algorithm by adding some complexity three keys | [23] | Increase the security complexity algorithms speed while maintaining encryption and decryption time |
| Modify the RSA algorithm with N prime number | [13] | In this algorithm encryption is done binary file it so can applicable for any kind of data |
| | [11] | Increased security<br>Provide more efficiency and readability |
| Modify the RSA algorithm with N prime number using K-Nearest algorithm | [12] | Not easy to decompose because it depends on prime numbers<br>Reduce the redundant messages occurred in RSA- can save space |
| Modify the RSA cryptosystem by increasing the number of private keys | [7] | Gives the RSA cryptosystem a higher security |
| Combine Montgomery multiplication, Chinese remainder theorem (CRT) with RSA Scheme | [20] | Execution time faster |
| RSA algorithm that uses Chinese remainder theorem (CRT) with purposes of the concealing multiple plaintexts in one chipper-text | [21] | The new algorithm can also take advantages of current methods that speed up the decryption process of RSA |

Based on the table, it can be stated that many techniques introduced by the earlier researchers in order to enhance the security, efficiency and speed of the scheme. The technique is about modifying the prime number as well as modifying the key. The larger the number of prime numbers and the larger the key, the more complicated the scheme, thus it will increase the scheme security.

## 4. CONCLUSION

This paper has presented and studied on several RSA schemes since last decade. Based on the literature survey, it can be concluded that even the RSA schemes' weakness has a large key size, the strength is security and it can be implemented on such applications that are based on the Internet technology. It also shows that there are many efforts that have been proposed by previous researchers in the last decade.

## ACKNOWLEDGEMENTS

The authors wish to thank the Ministry of Higher Education Malaysia in funding the grant under the Fundamental Research Grant Scheme (FRGS), S/O Code 14450 with Research and Innovation Management Centre, Universiti Utara Malaysia, Kedah for the administration of this study.

## REFERENCES


[1] M. D. A. Mushtaque, H. Dhiman, S. Hussain, and S. Maheshwari, "Evaluation of DES, TDES, AES, blowfish and twofish encryption algorithm: Based on space complexity," *International Journal of Engineering Research & Technology,* vol. 3 no. 4. pp. 283-286, 2014.

[2] S. K. Rakeshkumar, "Performance analysis of data encryption standard algorithm & proposed data encryption standard algorithm," *International Journal of Engineering Research and Development*, vol. 7, no. 10, pp. 11-20, 2013.

[3] L. Wang, H. Zhao, and G. Bai, "A cost-efficient implementation of public-key cryptography on embedded systems", *2007 Int. Workshop on Electron Devices and Semiconductor Technology (EDST)*, pp. 194-197, 2007.

[4] A. V Meier, "The elgamal cryptosystem," *Joint Advanced Students Seminar*, 2005.

[5] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-performance and lightweight lattice-based public-key encryption," *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pp. 2-9, 2016.

[6] R. L. Rivest, Adi Shamir, and Leonard Adleman, "A method for obtaining digital signatures and public key crypto systems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[7] H. R. Hashim, "A new modification of RSA cryptosystem based on the number of the private keys," *American Scientific Research Journal for Engineering, Technology, and Sciences*, no. 24, no. 1, pp. 270-279, 2016.

[8] S. Mathur and D. Gupta, "A modified RSA approachfor encrypting and decrypting text and images using multi-power , multi public keys, multi prime numbers and k- nearest neighbor algorithm," *AICTC '16: Proceedings of the Int. Conf. on Advances in Information Communication Technology & Computing*, vol. 1, no. 54, pp. 1-6, 2016.

[9] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 402-408, 2012.

[10] M. Thangavel, P. Varalakshmi, M. Murrali, and K. Nithya, "An enhanced and secured RSA key generation scheme (ESRKGS)," *Journal of Information Security and Applications*, vol. 20, pp. 3-10, 2015.

[11] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on 'n' prime numbers," *International Journal of Engineering and Computer Science*, vol. 1, no. 2, pp. 62-66, 2012.

[12] A. K. Hussain, "A modified RSA Algorithm for security enhancement and redundant messages elimination using k-nearest neighbor algorithm," *International Journal of Innovative Science, Engineering & Technology,* vol. 2, no. 1, pp. 159-163, 2015.

[13] Md Wasim and P. Paul, "Implementing the information security using modified RSA algorithm with the help of N prime number," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 10, pp. 18055-18062, 2016.

[14] D. B. Khairnar and P. S. Kadam, "Secure RSA: Pair wise key distribution using modified RSA algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 4, pp. 383-387, 2016.

[15] P. K. Panda and S. Chatoppadhyay, " A Hybrid Security Algorithm for RSA Cryptosystem, " *In 2017 4th International Conference on Advanced Computing and Communication Systems, IEEE*, pp. 1-6, 2017.

[16] D. Aggarwal and U. Maurer, "Breaking RSA generically is equivalent to factoring," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6251-6259, Nov. 2016.

[17] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption", *Proceedings of 2011, 6th International Forum on Strategic Technology*, pp. 1118-1121, 2011.

[18] R. Ghosh, "An efficient and robust modified RSA based security," *Journal of Computer Science Engineering and Information Technology Research*, vol. 6, no. 2, pp. 15-22, 2016.

[19] M. Bayat and M. R. Aref, "An Antribute-based tripartite Key Agreement Protocol," *International Journal of Communication Systems*, vol. 28, no. 8, pp. 1419-1431, 2015.

[20] L. Qiu, Z. Liu, G. C. C. F. Pereira, and H. Seo, "Implementing RSA for sensor nodes in smart cities," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 807-813, 2017.

[21] A. Mansour, A. Davis, M. Wagner, R. Bassous, H. Fu, and Y. Zhu, "Multi - asymmetric cryptographic RSA scheme," *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, pp. 1-8, 2017.

[22] A. E. Mezher, "Enhanced RSA cryptosystem based on multiplicity of public and private keys," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3949-3953, 2018.

[23] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-badri, "Modified RSA-based algorithm: A double secure approach," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 6, pp. 2818-2825, 2019.

[24] A. Chavan, A. Jadhav, S. Kumbhar, and I. Joshi, "Data transmission using RSA algorithm,"*International Research Journal of Engineerin and Technology*, vol. 6, no. 3, pp. 34-36, 2019.

[25] K. D. M. AlSabti and H. R. Hashim, "A new approach for image encryption in the modified RSA cryptosystem using MATLAB," *Global Journal of Pure and Applied Mathematics*, vol. 12, no. 4, pp. 3631-3640, 2016.

[26] S. Anandakumar, "Image cryptography using RSA algorithm in network security" *International Journal of Computer Science Engineering and* Technology, vol. 5, no. 9, pp. 326-30, 2015.

[27] A. S. Al Najjar, "Implementation color-images cryptography using RSA algorithm," *International Journal Advance Research in Computer Science Software Engineering*, vol. 7, no. 11, pp. 181-185, 2017.

[28] D. Jagadiswary and D. Saraswady, "Estimation of modified RSA cryptosystem with hyper image encryption algorithm," *Indian Journal of Science and Technology*, vol. 10, no. 7, pp. 1-5, 2017.

[29] U. Gulen, A. Alkhoidary, and S. Baktir, "Implementing RSA for wireless sensor nodes," *Sensors (Switzerland)*, vol. 19, no. 13, p. 2864, 2019.

[30] C. Meshram, "Discrete Logarithm and Integer Factorization using ID-based Encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 2, pp. 160-168, 2015.
[31] E. R. Arboleda, J. L. Balaba, and J. C. L. Espineli, "Chaotic rivest-shamir-adlerman algorithm with data encryption standard scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 219-227, 2017.
[32] N. A. Hasan and Alaa K. Farhan, "Security improve in ZigBee protocol based on RSA public algorithm in WSN," *Engineering and Technology Journal*, vol. 37, no. 3B, pp. 67-73, 2019.
[33] W. Liang and Z. Yonggui, "A new personal information protection approach based on RSA cryptography," *2011 IEEE International Symposium on IT in Medicine and Education*, pp. 591-593, 2011.
[34] R. Minni, K. Sultania, S. Mishra, and D. R. Vincent, "An algorithm to enhance security in RSA," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1-4, 2013.
[35] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimeh, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2, pp. 1430-1437, 2020.
[36] G. Zhao, X. Yang, B. Zhou, and W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks" *2010 2nd International Conference on Signal Processing Systems*, pp. V2-640-V2-643, 2010.
[37] R. Kayalvizhi, M. Vijayalakshmi, and V. Vaidehi, "Energy analysis of RSA and ELGAMAL algorithms for wireless sensor networks," *International Conference on Network Security and Applications*, pp. 172-180, 2010.
[38] G. Sharma, S. Bala, and A. K. Verma, "An improved RSA-based certificateless signature scheme for wireless sensor networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 82-89, 2016.
[39] J. Singh, V. Kumar, and R. Kumar, "An RSA based certificateless signature scheme for wireless sensor networks," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 443-447, 2015.
[40] P. Satapathy, N. Pandey, and S. K. Khatri, "NFC car keys by using RSA cryptography in WSN security," *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 143-147, 2019.
[41] Abdullah Said Alkalbani, T. Mantoro, and A. O. M. Tap, "Comparison between RSA hardware and software implementation for WSNs security schemes," *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M)*, pp. E84-E89, 2010.
[42] C-Y. Cheng, I-C. Lin, and S-Y. Huang, "An RSA-like scheme for multiuser broadcast authentication in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, p. 743623, 2015.
[43] R. Kumar and H. K. Verma, "An advanced secure (t, n) threshold proxy signature scheme based on RSA cryptosystem for known signers," *2010 IEEE 2nd International Advance Computing Conference (IACC)*, pp. 293-298, 2010.
[44] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229-235, 2017.
[45] M. R. Asaar, M. Salmasizadeh, and W. Susilo, "A short identity-based proxy ring signature scheme from RSA," *Computer Standards & Interfaces*, vol. 38, pp. 144-151, 2015.

## BIOGRAPHIES OF AUTHORS

**Mohd Saiful Adli Mohamad** received his Bachelor of Science in Mathematic and Master of Science in Mathematic from Universiti Teknologi Malaysia (UTM) in 2006 and 2008 respectively. He later completed his Ph.D from Universiti Kebangsaan Malasysia (UKM) in 2017. He is currently a Senior Lecturer in School of Quantitative Science in UUM with research interests in developing cryptographic algorithm for long-term security.

**Roshidi Din** received his Bachelor of Information Technology and Master of Science in Information Technology degrees from Universiti Utara Malaysia (UUM) in 1996 and 1999 respectively. He later completed his Ph.D from Universiti Sains Malaysia (USM) in 2015. He is currently at the School of Computing, UUM. His current research interests are more on the application of Discrete Mathematics in various areas especially in Information Security, Steganography and Steganalysis, and Natural Language Steganology.

**Jasmin Ilyani Ahmad** received his Bachelor of Science in Mathematic and Master of Science in Mathematic from Universiti Putra Malaysia (UPM). She is a Senior Lecturer in Universiti Teknologi Mara (UiTM) at Sungai Petani, Kedah, Malaysia. Currently, she is a Ph.D student, School of Computing (SOC), Awang Had Salleh Graduate School (AHSGS), Universiti Utara Malaysia, Sintok, Kedah, Malaysia.