Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 1, October 2018, pp. 386~392
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i1.pp386-392

Review on Public Key Cryptography Scheme-Based Performance Metrics

Jasmin Ilyani Ahmad[1], Roshidi Din[2], Mazida Ahmad[3]
[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Kedah Branch, 08400 Merbok, Kedah, Malaysia
[2,3]School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia

Article Info

Article history:

Received May 11, 2018
Revised Jul 10, 2018
Accepted Jul 25, 2018

Keywords:

Public Key Cryptography
Scheme
Security
Space
Speed

ABSTRACT

Cryptography is a method used to establish secure data communication. The goal of cryptography is to send data to satisfy the criteria of confidentiality, data integrity, authentication and non-repudiation. In line with the goals, the performance metrics is the important evaluation criteria to be analyzed. This paper presents the review of performance metrics of Public Key Cryptography (PKC) that had been analyzed based on the PKC scheme from the previous researchers' effort since the last four decades. It also displayed the research pattern in different performance metrics over the years. The aim of this paper is to identify the key performance metrics which addressed by the researchers in previous studies. Finally, the critical concern of this paper which shows the overall PKC performance metrics also presented in this paper.

Corresponding Author:

Jasmin Ilyani Ahmad,
Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA Kedah Branch,
08400 Merbok, Kedah, Malaysia.
Email: jasmin.ilyani.ahmad@gmail.com

1. INTRODUCTION

Cryptography is the study of mathematical schemes that handle privacy and authentication issues in data security [1]. It is also defined as a technique to secure personal data from unauthorized users [2]. It was applied to send unreadable form of message over the transmission medium. Generally, cryptography uses keys to encrypt and decrypt the message. Cryptographic key is divided into two classes; private key cryptography and public key cryptography. Private key cryptography, where the sender and recipient share the same key to encrypt and decrypt the plain text and ciphertext accordingly. The main advantage of private key cryptography is that it is relatively fast. This is because of only one key involved in encryption and decryption. However, by using the same key it will lead the damage to the ciphertext because of if the key is known by third party, he or she will easily decrypt the ciphertext. Thus, public key cryptography was introduced to solve the weakness of private key cryptography. It requires two different keys; public key and private key. The key used to encrypt the plaintext and can share among everyone is called public key. While another pair of key which used to decrypt the ciphertext is kept secret and it is called private key. According to [3] the private key will only be secured as long as it is kept private. Other than that, the ciphertext that was encrypted using public key can be decrypted only with corresponding private key [4]. In public key cryptography, the recipient's public key is used to encrypt the plain text to the ciphertext while the recipient's private key is used to decrypt the ciphertext to the original plain text. These two keys must match and agreed each other to ensure authorize sender and recipient are in the communication process. Public key cryptography can solve the problems in private key cryptography which use same key to encrypt and decrypt

the message [5]. However, public key cryptography works based on different schemes. Each scheme applies their own techniques to achieve the cryptography goal.

The literature has shown a significant contribution to different schemes since it was invented in the last four decades. The schemes are evaluated based on different performance metrics in achieving the cryptography goal which to send data securely from sender to receiver through public network with high speed and efficient. Performance analysis is important in evaluating the strength and the efficiency of the proposed schemes. Even the cryptography concern is security; however speed and space are also the factors that effected the strength of the schemes proposed. This paper is established to review the different public key cryptography scheme based on performance analysis used to see research patterns for the last 40 years since they were invented. Meanwhile, this study had been conducted based on several steps which includes gathering the data, pre-processing data, classify the previous study based on metrics performance, evaluate data based on metrics performance classification and obtain the results.

2. PUBLIC KEY CRYPTOGRAPHY PERFORMANCE METRICS ON DIFFERENT PKC SCHEME

This section presents the performance metrics in evaluating the public key cryptography scheme. The schemes consist of Diffie-Hellman Key Exchange, RSA, McEliece, Goldwasser-Micali, ElGamal, Elliptic Curve, Digital Signature, Lattices, Fully Homomorphic, NTRU and GGH. Figure 1 shows the schemes and the year they were proposed. From the figure, Diffie-Hellman, RSA and McEliece are the earliest schemes introduced compared to others.

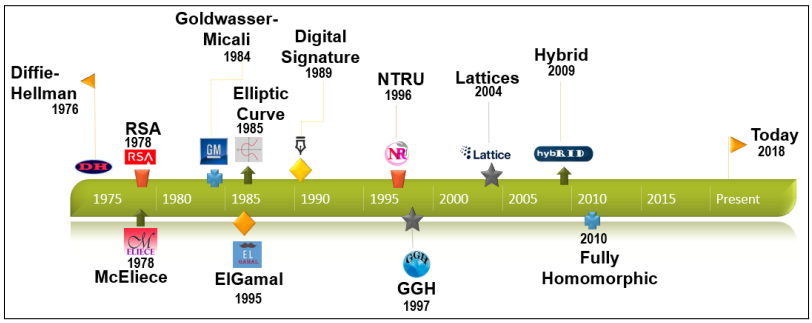

Figure 1. The timeline of cryptography schemes

Generally, each scheme was developed to offer facilities for users in data communication and transmission as well as to save the capacity, the computational time and to ensure the data protection will always be reliable. Thus, public key cryptography (PKC) is evaluated by these performance metrics to make sure the cryptanalysis is performing well in delivering secured data from sender to receiver through public networks. There are three performance metrics of PKC, which are security, speed and space [6-7]. According to [8] security is defined as all about confidentiality, integrity and availability. Other than that, computer and network security is about concerning in protecting the systems. Increasing the security usually will also increase the size of key that will use more space. The more space used, the slower the algorithm. In line with [2] an efficient cryptography algorithm probably uses less space after the encryption process in order to have fast processing. As stated by [9] fast processing is about the time needed in generating key, encrypting and decrypting process.

However, there are also integrated performance metrics that had been highlighted by the previous researchers which applied for different schemes; security and speed; security and space; speed and space; and security, speed and space. These performance metrics are used to evaluate the performance of the PKC schemes as shown in Figure 2. It also shows that most of the schemes including Diffie Hellman, RSA, McEliece, ElGamal, Elliptic Curve and GGH are more focused on security. Other than that, most of the scheme also shows attention on the integration of security and speed (digital signature and hybrid scheme); and security and space (lattices and fully homomorphic scheme). Only a few of the schemes focused on speed and space separately. On the other hand, GGH and lattices paid attention on space as the evaluation criteria for the scheme performance metrics as these schemes applied small key size and small ciphertext [10-11].

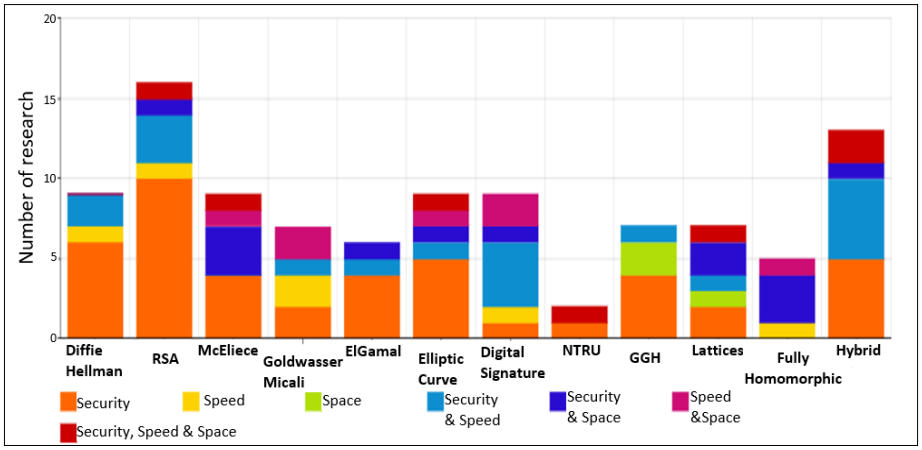

Figure 2. Performance Metrics on Different PKC Schemes

3. RELATED WORKS ON PERFORMANCE METRICS OF PKC SCHEMES

Basically, the main concern of PKC is the security itself where it must make sure that data transmit securely from sender to receiver over public networks. According to [2] cryptography provide a technique to secure personal data from unauthorized users. Other than that, the speed also plays the important roles as to ensure users can encrypt and decrypt faster. Moreover, not only security and speed, space also should be counted in the concern of PKC for the usage of devices that has limited space and resources. Some of the previous studies not only focused on security, speed and space separately, but they integrate the performance metrics for their schemes evaluation criteria for example security and speed; security and space; speed and space; and security, speed and space. Table 1 shows the previous research that focussing in different performance metrics that can be classified as single performance metrics and integrated performance metrics. Other than that, it also shows the schemes that are are divided into three categories which are conventional, trans-contemporary and contemporary schemes based on the year proposed.

Table 1. Research Focused on Performance Metrics for PKC Scheme Classification

		Conventional	Trans-Contemporary	Cotemporary
	Performance Metrics / Years	**2000**	**2010**	**2020**
Single Performance Metrics	Security	[12 - 16]	[17 - 22]	[23] – 53]
	Speed	[54] [55]	[56]	[57] [58]
	Space		[10]	[59]
Integrated Performance Metrics	Security & Speed	[1] [60] [61]	[62 - 66]	[67 - 76]
	Security & Space		[5] [77] [78] [79]	[80 - 88]
	Speed & Space	[89] [90]		[91 - 93]
	Security, Speed & Space	[94] [95]	[96]	[97 - 99]

Referring to Table 1, a few researches were implemented in the conventional years and almost no difference in the next trans-contemporary years. However, from the whole table it shows that most of the studies were concentrate in the contemporary years. On the other hand, almost all the research that focuses on single performance metrics paid attention on security. Only a few of the research look at the speed and space as their performance metrics in their proposed schemes. From the integrated performance metrics perspective, it also shows the same view where most of the research were done aggressively in the contemporary years and focused on the integration with the security performance metrics, which are security and speed; and security and space.

4. PREFERRED PERFORMANCE METRICS

From the seven performance-metrics discussed previously, it shows that there are three highest performance metrics popular in the previous studies which are security (44.44%); security and speed (20%); and security and space (14.44%). From the top three performance metrics, security shows the highest performance metrics that are popular among researchers which take 44.4% out of total research. On the other hand, space (2.22%), speed (5.56%), speed and space (5.56%) and security, speed and space (7.78%) shows the lowest percentage among the total previous studies. This is because, to upgrade the security, the key size and the ciphertext size will expand. Thus, it will affect the space. According to [100] if the space used is more where the block size and key size are larger, it will affect the speed of the algorithm and become slower.

From literature survey, in public key cryptography, these are the significant findings that are made based on the seven-performance metrics. Figure 3 shows the preferred performance metrics of PKC scheme which are security, then followed by security and speed; and security and space.

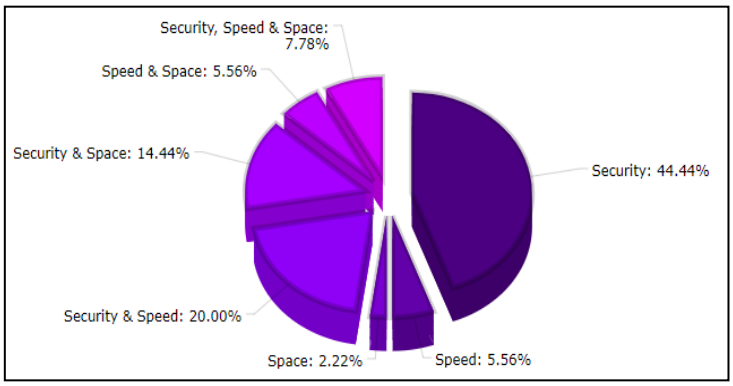

Figure 3. Performance Metrics Focused by Previous Studies

5. CONCLUSION

This paper studied an overview of seven performance-metrics for public key encryption; security; speed; space; security and speed; security and space; speed and space; and security, speed and space. They have their own strength to support the achieving of cryptography goal such as secured [23] [24] [25] [26] [27], fast [57] [58] and efficient [59]. Most of the previous researchers focus on security [33 - 53]; security and speed [67 -76]; and security and space [80 - 88] as their scheme performance metrics. Other than that, from the previous sections, it shows that most of the research were done aggressively in the contemporary years. However, lack of research focus on space alone because of high security and speed will lead of using more space. The findings clearly showed that the security; security and speed; security and space are the key performance metrics which addressed by the researchers in previous studies. Overall, this paper contributes suggestions and guidelines for future researchers in PKC field to choose and use the appropriate schemes based on the performance metrics that had been concentrated by the previous researchers.

REFERENCES

[1] W. Diffie, W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[2] A. Mushtaque, H. Dhiman, S. Hussain, and S. Maheshwari, "Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm: Based on Space Complexity," vol. 3, no. 4, pp. 283–286, 2014.
[3] A. V Meier, "The ElGamal Cryptosystem," pp. 1–13, 2005.
[4] L. Wang, H. Zhaot, and G. Bail, "cost-Efficient Implementation Cryptography on Embedded Systems," 2007.
[5] M. S. Hwang, C. C. Chang, and K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 2, pp. 445–446, 2002.
[6] A. Lutoria, "A Review on Different Cryptographic Encryption Decryption Algorithm," vol. 6, pp. 1–5, 2016.
[7] V. Kapoor, "A Hybrid Cryptography Technique to Support Cyber Security Infrastructure," vol. 4, no. 11, pp. 3995–4002, 2015.
[8] J. M. Anderson, "Why we need a new definition of information security," *Comput. Secur.*, vol. 22, no. 4, pp. 308–313, 2003.
[9] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-Performance and Lightweight Lattice-Based Public-Key Encryption," *Proc. 2nd ACM Int. Work. IoT Privacy, Trust. Secur. - IoTPTS '16*, pp. 2–9, 2016.

[10] S.-H. Paeng, B. E. Jung, and K.-C. Ha, "A Lattice Based Public Key Cryptosystem Using Polynomial Representations," *Lncs*, pp. 292–308, 2003.
[11] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-Key Cryptosystems from Lattice Reduction Problems," *Adv. Cryptol. - {CRYPTO} '97, 17th Annu. Int. Cryptol. Conf. St. Barbar. California, USA, August 17-21, 1997, Proc.*, vol. 1294, pp. 112–131, 1997.
[12] R. L. Rivest, A. Shamir, and L. Adleman, "{A} method for obtaining digital signatures and public key crypto systems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[13] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.
[14] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[15] J. Hoffstein, D. Lieman, J. Pipher, and J. H. Silverman, "Ntru : a Public Key Cryptosystem," pp. 1–17.
[16] P. Nguyen, "Cryptanalysis of the Goldreich – Goldwasser – Halevi Cryptosystem from Crypto ' 97," pp. 288–304, 1999.
[17] P. Loidreau and N. Sendrier, "Weak keys in the McEliece public-key cryptosystem," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1207–1211, 2001.
[18] L. Harn, M. Mehta, S. Member, and W. Hsin, "Integrating Diffie – Hellman Key Exchange into the Digital Signature Algorithm (DSA)," vol. 8, no. 3, pp. 198–200, 2004.
[19] O. Regev, "New Lattice Based Cryptographic Constructions," pp. 1–43, 2004.
[20] D. Boneh and G. Di Crescenzo, "Public key encryption with keyword search," *Adv. Cryptology- …*, 2004.
[21] R. Alfaris, M. R. Said, M. Othman, and F. Ismail, "Modified Diffie-Hellman Protocol By Extend The Theory of The Congruence," vol. 2, no. 11, pp. 842–848, 2008.
[22] S. Flonta and L. Miclea, "An extension of the El Gamal encryption algorithm," *2008 IEEE Int. Conf. Autom. Qual. Testing, Robot. AQTR 2008 - THETA 16th Ed. - Proc.*, vol. 3, pp. 444–446, 2008.
[23] A. Khalique, "Implementation of Elliptic Curve Digital Signature Algorithm," vol. 2, no. 2, pp. 21–27, 2010.
[24] S. Goldwasser, Y. Kalai, C. Peikert, and V. Vaikuntanathan, "Robustness of the Learning with Errors Assumption," 2010.
[25] M. J. Kakish, "SECURITY IMPROVMENTS TO THE DIFFIE-HELLMAN SCHEMES," vol. 8, no. July, pp. 79–85, 2011.
[26] A. S. Approach, "Modified RSA Algorithm," pp. 552–555, 2011.
[27] R. Thanuja and D. K. S, "A NEW APPROACH TO DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM," vol. 1, no. 3, pp. 534–535.
[28] P. Sharma, S. Sharma, and R. S. Dhakar, "Modified Elgamal Cryptosystem Algorithm (MECA)," *2011 2nd Int. Conf. Comput. Commun. Technol. ICCCT-2011*, pp. 439–443, 2011.
[29] M. Yoshino and Noboru, "Improving GGH Cryptosystem for Large Error Vector," *Isita 2012*, pp. 416–420, 2012.
[30] G. Moise, "On the attacks over the elliptic curve-based cryptosystems," *Proc. - 3rd Int. Conf. Emerg. Intell. Data Web Technol. EIDWT 2012*, pp. 244–249, 2012.
[31] P. Sehgal, N. Agarwal, S. Dutta, and P. M. D. R. Vincent, "Modification of Diffie-Hellman Algorithm to Provide More Secure Key Exchange," vol. 5, no. 3, pp. 2498–2501, 2013.
[32] M. P. Rewagad and M. Y. Pawar, "Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing," *Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013*, pp. 437–439, 2013.
[33] A. Kaushik, "Extended Diffie-Hellman Algorithm for Key Exchange and Management," vol. 3, no. 3, pp. 67–70, 2013.
[34] G. Mateescu and M. Vladescu, "Enterprises : combining different Cryptography techniques," pp. 659–662, 2013.
[35] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," *J. Cryptol.*, vol. 26, no. 1, pp. 80–101, 2013.
[36] H. Arshad and M. Nikooghadam, "Three-Factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems," 2014.
[37] Z. Tan, "RESEARCH ARTICLE A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems," 2014.
[38] M. Shankar, "H YBRID C RYPTOGRAPHIC T ECHNIQUE U SING RSA," vol. 6, no. 6, pp. 39–48, 2014.
[39] S. Deshmukh, "Hybrid cryptography technique using modified," vol. 5, no. 6, pp. 7302–7304, 2014.
[40] M. Thangavel, P. Varalakshmi, M. Murrali, and K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," *J. Inf. Secur. Appl.*, vol. 20, pp. 3–10, 2015.
[41] Y. Lu, L. Li, H. Peng, and Y. Yang, "An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem," *J. Med. Syst.*, vol. 39, no. 3, p. 32, 2015.
[42] S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, "An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography," *J. Med. Syst.*, vol. 39, no. 11, 2015.
[43] R. Ghosh, "AN EFFICIENT AND ROBUST MODIFIED RSA BASED SECURITY," vol. 6, no. 2, pp. 15–22, 2016.
[44] D. B. Khairnar and P. S. Kadam, "Secure RSA : Pair Wise Key Distribution using Modified RSA Algorithm," vol. 6, no. 4, pp. 383–387, 2016.
[45] K. Dheiaa, M. Alsabti, and H. R. Hashim, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB," vol. 12, no. 4, pp. 3631–3640, 2016.

[46] H. R. Hashim, "A New Modification of RSA Cryptosystem Based on The Number of The Private Keys," pp. 270–279.
[47] Y. Wang, W. Bao, Y. Zhao, H. Xiong, and Z. Qin, "An ElGamal Encryption with Fuzzy Keyword Search on Cloud Environment," vol. 18, no. 3, pp. 481–486, 2016.
[48] I. Conference and C. Technologies, "Secure Multi Server Authentication System using Elliptic Curve Digital Signature," pp. 0–3, 2016.
[49] Y. Sazaki, "The Development Android-Based SMS Security Software Using ECDSA with Boolean Permutation," pp. 26–30, 2016.
[50] D. Jagadiswary and D. Saraswady, "Estimation of Modified RSA Cryptosystem with Hyper Image Encryption Algorithm," vol. 10, no. February, pp. 1–5, 2017.
[51] K. Zhang, M. Tomlinsin, and M. Z. Ahmed, "A Modified McEliece Public Key Encryption System with a Higher Security Level," pp. 991–996, 2013.
[52] L. Van Thai, "McEliece cryptosystem based identification and signature scheme using chained BCH codes," pp. 122–127, 2015.
[53] E. Krouk and A. Ovchinnikov, "About One Modification of McEliece Cryptosystem based on Plotkin Construction," pp. 7–10, 2016.
[54] S. Boni, "Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm," vol. 130, no. 15, pp. 7–10, 1976.
[55] I. Introduction, "Fast Algorithms for," vol. 28, no. 1, pp. 210–236, 1985.
[56] "AN EFFICIENT MODIFIED ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM Tilahun Kiros Department of Computer Science and Engineering Mekelle Institute of Technology and Kumudha Raimond Department of Electrical and Computer Engineering," vol. 26, 2009.
[57] D. Stehlé and R. Steinfeld, "Faster Fully Homomorphic Encryption," 2010.
[58] H. Wang, H. Zhang, and S. Tang, "Key recovery on several matrix public-key encryption schemes," vol. 10, pp. 152–155, 2016.
[59] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning with Errors Over Rings ∗," no. 15848, pp. 1–34, 2013.
[60] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *The Deep Space Network Progress Report*, vol. 42, no. 44. pp. 114–116, 1978.
[61] M. Blum and S. Goldwasser, "An efficient probabilistic public key encryption scheme which hides all partial information," *Advances in Cryptology Proceedings of Crypto 84*, vol. 196, no. September 1984. pp. 289–302, 1985.
[62] E. Ramaraj, S. Karthikeyan, and M. Hemalatha, "A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)," pp. 78–86.
[63] Q. Tang and L. Chen, "Public-key encryption with registered keyword search," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6391 LNCS, pp. 163–178, 2010.
[64] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on ' n ' prime numbers," vol. 1, no. 2, pp. 63–66, 2013.
[65] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," *Proc. - 2012 Int. Conf. Adv. Comput. Sci. Appl. Technol. ACSAT 2012*, pp. 402–408, 2013.
[66] S. Mathur, "A MODIFIED RSA APPROACHFOR ENCRYPTING AND DECRYPTING TEXT AND IMAGES USING MULTI- POWER , MULTI PUBLIC KEYS , MULTI PRIME NUMBERS AND K- NEAREST NEIGHBOR ALGORITHM," vol. 1, 2016.
[67] P. Kuppuswamy, "ENRICHMENT OF SECURITY THROUGH CRYPTOGRAPHIC PUBLIC KEY ALGORITHM BASED ON BLOCK," vol. 2, no. 3, pp. 347–355, 2011.
[68] A. M. Sagheer, "Elliptic curves cryptographic techniques," *6th Int. Conf. Signal Process. Commun. Syst. ICSPCS 2012 - Proc.*, 2012.
[69] P. Kuppuswamy and S. Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm," *MIS Rev.*, vol. 19, no. 2, pp. 1–13, 2014.
[70] C. Peikert, "Lattice Cryptography for the Internet," pp. 1–25, 2014.
[71] S. A. Jaju and S. S. Chowhan, "A Modified RSA algorithm to enhance security for digital signature," *2015 Int. Conf. Work. Comput. Commun. IEMCON 2015*, 2015.
[72] S. K. Bhowmick, S. K. Das, and T. Chakraborty, "Available Online through ISSN : 0975-766X CODEN : IJPTFI Research Article," vol. 8, no. 4, pp. 26578–26583, 2016.
[73] M. A. Raji, F. Amiri, and M. Ahmadian, "A New secure email scheme Using Digital Signature with S / MIME," vol. 4, no. 3, pp. 56–62, 2016.
[74] M. H. Azaim, D. W. Sudiharto, and E. M. Jadied, "Design and Implementation of Encrypted SMS on Android Smartphone Combining ECDSA - ECDH and AES," pp. 18–23, 2016.
[75] P. S. Priyanka, "ENHANCED HYBRID CRYPTOGRAPHY," vol. 19, no. 2, pp. 108–113, 2016.
[76] A. A. Patil, "Hybrid Cryptography Mechanism for Securing," pp. 1–4, 2016.
[77] N. Gura, A. Patel, A. Wander, and H. Eberle, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs."
[78] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5299 LNCS, pp. 31–46, 2008.
[79] O. Regev, "On Lattices , Learning with Errors , Random Linear Codes , and Cryptography," no. 15848, pp. 1–37, 2009.
[80] M. Van Dijk and C. Gentry, "Fully Homomorphic Encryption over the Integers," pp. 1–28, 2010.

[81] A. Mandal, D. Naccache, and M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," pp. 1–24, 2011.
[82] Z. Brakerski, "Efficient Fully Homomorphic Encryption from (Standard) LWE."
[83] Q. Zhang, Z. Li, and C. Song, "The Improvement of digital signature algorithm based on elliptic curve cryptography," *2011 2nd Int. Conf. Artif. Intell. Manag. Sci. Electron. Commer.*, pp. 1689–1691, 2011.
[84] R. Lindner and C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption," pp. 319–320, 2011.
[85] R. Hooshmand, M. K. Shooshtari, T. Eghlidos, and M. R. Aref, "Reducing the Key Length of McEliece Cryptosystem Using Polar Codes," no. 92, pp. 104–108, 2014.
[86] R. J. Hwang, F. F. Su, Y. S. Yeh, and C. Y. Chen, "An efficient decryption method for RSA cryptosystem," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 1, pp. 585–590, 2005.
[87] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani, "Enhanced public key security for the McEliece cryptosystem," no. 132256.
[88] R. Singh, I. Panchbhaiya, A. Pandey, and R. H. Goudar, "Hybrid Encryption Scheme (HES) : An Approach for Transmitting Secure Data over Internet," *Procedia - Procedia Comput. Sci.*, vol. 48, no. Iccc, pp. 51–57, 2015.
[89] Josh Benaloh, "Dense Probabilistic Encryption," *In Proceedings of the Workshop on Selected Areas of Cryptography*. pp. 120–128, 1994.
[90] R. Rauscher, F. Bohnsack, Ý. Ü. Ý, and Ü. Ý, "Results of an Elliptic-Curve-Approach for Use in Cryptosystems μ," no. 1.
[91] R. Dhagat, "New Approach of User Authentication Using Digital Signature," pp. 8–10, 2016.
[92] I. Symposium, "Anissa Sghaier , Medien Zeghid , Mohsen Machhout University of Monastir , Faculty of Sciences , EfJELab , Monastir 5019 ," pp. 343–348, 2016.
[93] J. G. Filho, G. P. Silva, D. C. C. Im, C. Miceli, and P. N. C. E. Im, "A Public Key Compression Method for Fully Homomorphic Encryption using Genetic Algorithms," *19th Int. Conf. Inf. Fusion*, pp. 1991–1998, 2016.
[94] V. Miller, "Use of Elliptic Curves in Cryptography," *Adv. Cryptol. – CRYPTO'85*, vol. LNCS 218, pp. 417–426, 1986.
[95] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," *Algorithmic number theory*, pp. 267–288, 1998.
[96] T. P. Berger, P. Cayrel, P. Gaborit, and A. Otmani, "Reducing Key Length of the McEliece Cryptosystem."
[97] W. Luo and J. Tan, "PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH BASED ON FACTORING," pp. 6–8.
[98] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," *J. Electr. Syst. Inf. Technol.*, vol. 2, no. 3, pp. 296–313, 2015.
[99] V. Kapoor, "A Hybrid Cryptography Technique for Improving Network Security," vol. 141, no. 11, pp. 25–30, 2016.
[100] A. Al Tamimi, "Performance analysis of data encryption algorithms," *Retrieved Oct.*, vol. 1, pp. 399–403, 2008.