Analysis Review on Public Key Cryptography Algorithms

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 Jun 3, 2018
Revised Aug 1, 2018
Accepted Aug 13, 2018

Keywords:

PKC Algorithms
PKC Schemes
Public Key Cryptography

ABSTRACT

This paper presents several Public Key Cryptography (PKC) algorithms based on the perspective of researchers' effort since it was invented in the last four decades. The categories of the algorithms had been analyzed which are Discrete Logarithm, Integer Factorization, Coding Theory, Elliptic Curve, Lattices, Digital Signature and Hybrid algorithms. This paper reviewed the previous schemes in different PKC algorithms. The aim of this paper is to present the comparative trends of PKC algorithms based on number of research for each algorithm in last four decades, the roadmap of PKC algorithms since they were invented and the most chosen algorithms among previous researchers. Finally, the strength and drawback of proposed schemes and algorithms 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 a technique defined in data security to ensure there is no unauthorized person to get the original message[1-2]. Generally, cryptography is divided to two categories which are private key cryptography and public key cryptography. Actually, in public key cryptography (PKC), the public key's recipient is used to encrypt the plain text to the ciphertext while the private key's recipient is used to decrypt the ciphertext to the original plain text [3]. In fact, the literature has shown a significant contribution to different PKC algorithm since the first scheme was invented since the last four decades. The PKC algorithms are analysed to see the trends of preferred algorithms in the previous studies. This paper is established to review the different public key cryptography algorithms to see research patterns for the last 40 years since they were invented. Thus, the main aim of this paper is to identify the significant PKC algorithm based on ranking or portion of research done in the last decade. The remaining sections of this paper is organized as follows. Section 2 presents the overview of public key cryptography algorithms based on different schemes. Then, Section 3 shows the findings obtained from the previous studies, and discussion about the trends, roadmap and the most chosen PKC algorithms among previous researchers. Next, Section 4 will conclude the research contribution in this paper.

2. RELATED REVIEW

A lot of methods and techniques were introduced and applied to make sure cryptography is success to be implemented. In public key cryptography, where two different keys are used to encrypt and decrypt respectively [4], many types of schemes were introduced. The schemes proposed by the previous researchers use techniques that can be categorized under different group of algorithms. This section presents the PKC algorithms, the schemes proposed by the previous researchers in each algorithms together with the scheme techniques, strenghts and drawbacks. The schemes consist of Diffie-Hellman, RSA, McEliece, Goldwasser-Micali, ElGamal, Elliptic Curve, Digital Signature, NTRU and GGH. Those PKC schemes were grouped under different algorithms based on their techniques used. According to [5] schemes are generally categorized into number theory based, lattices-based and codes-based. Basically, it can be divided into few categories of algorithms which are Discrete Logarithm, Integer Factorization, Coding Theory, Elliptic Curve, Lattices, Digital Signature And Hybrid. Each scheme was developed to fulfil users' needs such as to ensure the security of the scheme as well as to save space and time during data communication. Figure 1 shows the classification of PKC algorithms with the relevant schemes.

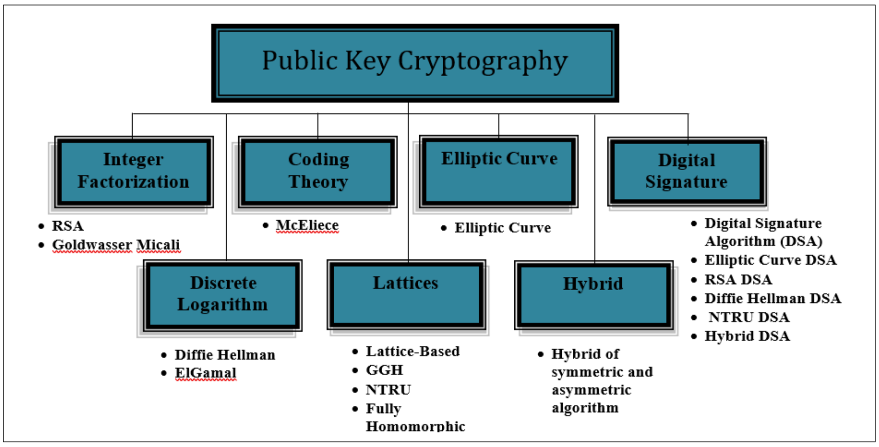


Figure 1. Public Key Cryptography algorithms classification

Discrete Logarithm problem is a mathematical problem that occurs in many settings and explains that it is tough to compute the exponent given a power in a known multiplicative group [3]. The schemes developed under Discrete Logarithm algorithm are Diffie-Hellman and ElGamal cryptosystem. Diffie-Hellman was invented in 1976 that brought new direction of cryptography that introduced key exchange protocol which based on discrete logarithm problem [6]. Even the scheme is secure and fast, however, it was difficult to reverse the encryption process. Many researchers had improvised the original Diffie-Hellman to increase speed of key generation and to generate and exchange keys over an insecure network scheme by using simple arithmetic equations [7]. There are also schemes proposed to improvise the security of Diffie-Hellman cryptosystem by reducing possibility of a known plaintext attacks [8-9] and man-in-the-middle attacks [10-11]. Meanwhile, from the security perspective, [12] cryptosystem was proposed to introduce digital signature scheme which is also based on Diffie-Hellman discrete logarithm problem and key distribution scheme. However, the key size should be large and the speed become slower. Several researchers had proposed their schemes to overcome the drawback of ElGamal cryptosystem [13-14] and to secure against mathematical and brute-force attacks [15]. On the other hand, RSA [16] and Goldwasser-Micali [17] cryptosystem are the popular schemes in Integer Factorization algorithm. RSA is based on the idea of factoring the two large prime numbers. The security of this scheme is depended on the difficulties to factor the numbers. Several previous researchers modified the original RSA scheme by increasing the number of private keys [18], use two public keys [19], use three prime numbers [20], use four prime numbers [21], and use 'n' prime numbers instead of two [22-24].The modified schemes were proposed to increase the security as well as to increase the speed of encryption and decryption time. However, when the key size increased, it consumes more time for large files [25], [21]. Otherwise, Goldwasser-Micali cryptosystem introduced quadratic residuosity modulo composite integers where factorization is unknown. The security of the scheme relies on the quadratic residuosity harden. Nevertheless, one most important drawback of this scheme was required large number of random bits and produce large amounts of ciphertext [17]. In order to overcome the problem, several schemes had been introduced that are capable of encrypting one bit at a time [26]. Instead, the technique used in schemes grouped in Coding Theory algorithm are based on codes for example Polar codes [27] and Goppa codes [28]. One of the scheme in this algorithm is McEliece cryptosystem which was faster than RSA in encrypting and decrypting message [28]. Even McEliece has a fast polynomial time decoding algorithm, it encrypts same message more than once and produce large key size which use of more space. Many earlier researchers improvised the existing scheme by decreasing the public and private key lengths [27], [29] , reducing the complexity of the scheme [30-32] and increasing the encryption and decryption speed [31].

Alternatively, lattices algorithm's technique is based on learning with errors assumption to solve shortest vector problem (SVP) and shortest independent vector problem [33]. The schemes under this algorithm includes Lattice-based, GGH, NTRU and Fully Homomorphic cryptosystem. One of the important criteria of lattices algorithm is it can contribute on saving the space by reducing the public key size [33-35]. Thus, because of the criteria it is also suitable for Internet of Things (IoT) devices [5] which is lightweight and has limited space. Other than that, lattices algorithm also has high security performance where it is suitable for cloud computing (GGH cryptosystem [36], Fully Homomorphic [37-39]) and public network which is the Internet (GGH cryptosystem [40], Lattice-based [41]). However, several researchers stated the drawback of their schemes which cannot achieve sufficient security without large parameters [42] and public key was too large for any practical system [43]. In contrast, basically Elliptic Curve algorithm was defined discrete logarithm problem which upgrade Diffie-Hellman Key Exchange protocol and provide small key size with faster implementation [44]. Then, several researchers improvised their schemes on security [45-48]. However, the schemes becomes more sophisticated and it requires more theoretical knowledge of Mathematics [49]. Moreover, the higher the security, the slower the encryption will be [50]. On the other hand, Digital Signature also one of the public key cryptography algorithms purposely making the receiver believes the message had been received from authorized sender without any modification during transmission. Digital signature consists of schemes which are Digital Signature Algorithm (DSA), Elliptic Curve DSA, Diffie Hellman DSA, RSA DSA, NTRU DSA and Hybrid DSA. Most of the schemes under Digital Signature algorithm were concentrate on security and space which also suitable for modern network office and link in online transactions [51]. Besides, because the schemes have smaller key size, it is suitable for constrained devices such as pagers, cellular phones and smart cards [52]. Moreover, these schemes also applied in different application such as email [53], short message service (SMS) [54] and cloud computing [55]. Hybrid algorithm basically provide the integration between public key cryptography and private key cryptography schemes [56-61]; between public key cryptography schemes [62] or between private key cryptography schemes [63]. Most of the schemes in Hybrid algorithm were focused on security and, security and speed because of the integration of different cryptography schemes will strengthen the security mechanism by combining the strengths of encryption of each form [58], [60], [63]. However, hybrid cryptography schemes have extra steps on encryption and decryption which give impact to the time required [62] and may contain problems on efficient computation and powerful encoding systems [56].

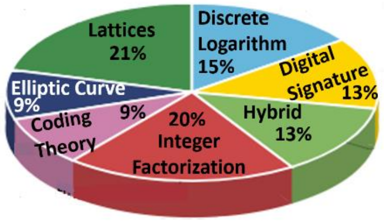
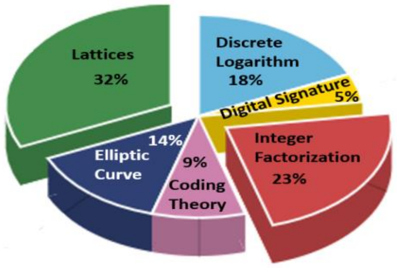
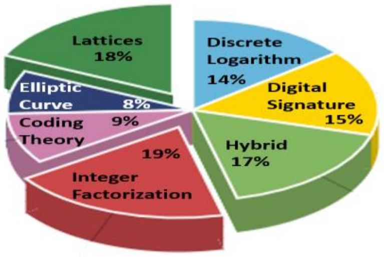
3. FINDINGS AND DISCUSSION

The literature survey was done on the previous research within last four decades. This is due to the form of public key cryptography which started in last 40 years with Diffie-Hellman and RSA schemes. This section shows the trends of previous studies in PKC algorithm. Other than that, this section also discussed about the roadmap of each algorithm which shows the popularity of it among researchers. Moreover, it also shows the most chosen algorithm among the researchers within last decade.

3.1. Research Trends in Public Key Cryptography Algorithms

Generally, this section is analyzing the research from all category of PKC algorithm within the last four decades. There are a lot of researchers' effort that contributes in cryptography field based on the amount of research. Table 1 shows the percentage of research in each PKC algorithm within the last four decades. From the total previous research, only 22% of the research done from 1976-2006, whereas 78% of the research came from 2007 until now as shown in the table. This situation shows that there is an increment in PKC research work for the last ten years compared to 30 years before it. From the year 1976 until today, it is illustrated that most of the previous researchers focused on Integer Factorization and Lattices algorithm with 20% and 21% respectively. Whereas the percentage of research done in Discrete Logarithm algorithm is 15% out of the total research within the last four decades. Other than that, research done in Hybrid and Digital Signature algorithm take only 13% each out of the total pie chart. However, number of research done in Elliptic Curve and Coding Theory algorithm were the most less compared to the others which only 9% each. Besides, from the 22% of research done within 1976-2006, Table 1 shows that there is no study on Hybrid algorithm during that timeline. Moreover, number of research in Digital Signature also less which only 5% from the total research. However, during that time, researchers had focused on Lattices and Integer Factorization which take 32% and 23% respectively. This is due to the advantages of Integer Factorization which has high security performance [25], [64], [65] and Lattices with the benefits on security and space [5], [33-34], [43], [66-67].

Table 1. Percentage of Research in PKC Algorithm

Years	Percentage of Total Research	Percentage of Research Based on Algorithms	Ranking on Chosen Algorithms
1976 - Today	100%		• Lattices • Integer Factorization • Discrete Logarithm • Digital Signature • Hybrid • Elliptic Curve • Coding Theory
1976 – 2006 (about 30 years)	22%		• Lattices • Integer Factorization • Discrete Logarithm • Elliptic Curve • Coding Theory • Digital Signature • Hybrid
2007 – Today (about 10 years)	78%		• Integer Factorization • Lattices • Hybrid • Digital Signature • Discrete Logarithm • Coding Theory • Elliptic Curve

Referring to Table 1, for the last ten years, the trends of preferred algorithm is look similar where Integer Factorization and Lattices still get more attention by the researchers even the percentage were decreased where it was only 19% and 18% respectively. This is because of research in Hybrid shows extreme increment from 0% to 17%. Other than that, research in Digital Signature also shows 10% increment. This situation shows that Hybrid and Digital Signature algorithm were extremely popular among researchers in this decade because it supports wireless technologies [58-59], Internet [63] and online transaction [61]. However, from the chart it also shows that lack of study on Elliptic Curve lately due to the requirement on theoretical knowledge of Mathematics [49]. Moreover, Coding Theory also shows the unpopularity among previous researchers because it requires large memory capacity [30] and provide large key size [28]. On the other hand, Hybrid and Digital Signature algorithm shows that the research in these algorithms were became more dominant within last ten years compared to the last thirty years before it, with the growth about 4% and 2% respectively. However, Discrete Logarithm, Integer Factorization, Lattices and Elliptic Curve algorithms shows the drop percentage between last four decades and last decades with 1% to 3% decline. On the other hand, Coding Theory algorithm shows no difference between both pie charts with only 9% of the researchers that were interested in this algorithm within last four decades. Overall, Lattices and Integer Factorization had shown a high ranking among other PKC algorithms.

3.2. The Roadmap of PKC in Last Four Decades

Figure 2 shows the roadmap of previous research done in different algorithm based on years. Based on the figure, there is an increment in number of research done for all PKC algorithm within last ten years. It found that in the last ten years, most of the researchers focused on the dominant algorithm which are Integer Factorization and Lattices. It also shows the same view where Integer Factorization and Lattices algorithm were focused within the first 30 years since the first scheme was invented. Nevertheless, even Hybrid and Digital Signature cannot compete with the dominant algorithms, they showed the highest increment for the last ten years. Thus, it seems that they are relevant in this modern daily life as can support wireless, Internet and online transaction applications. On the other hand, Coding Theory and Elliptic Curve algorithm shows only few number of research done in both different timeline, meaning that people are not interested on it. However, in other words, it can be stated that all the algorithms showed an increment in the number of research done previously.

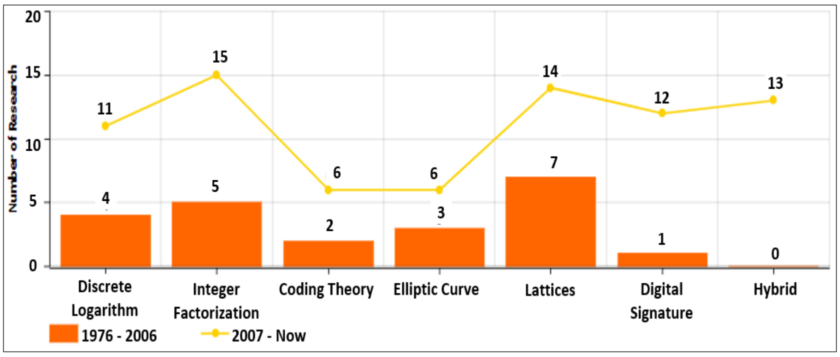


Figure 2. Number of research in PKC algorithm based on years

3.3. The Most Chosen PKC Algorithm

Figure 3 shows the two most chosen algorithms by the previous reseachers in last decade are Integer Factorization with 19% followed with Lattices algorithm with 18%. This is due to the advantages of the algorithm with high security level and computational time.

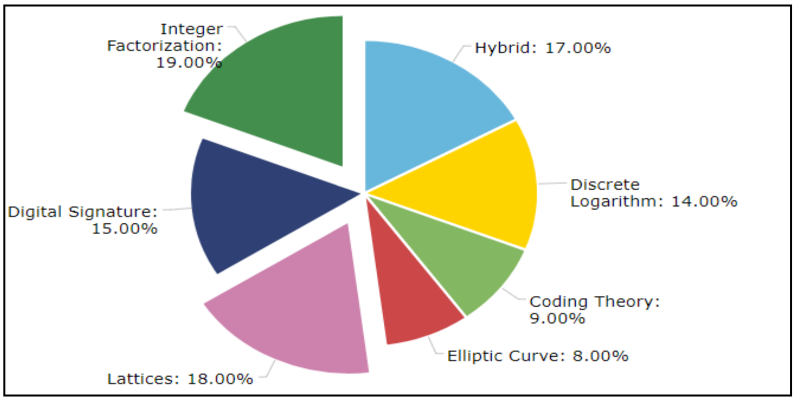


Figure 3. Research on PKC algorithm in last decade

Those schemes almost have similar advantage which is good in security. However, from the findings, the less chosen algorithm by the previous researchers are Elliptic Curve and Coding Theory with 8% and 9% respectively. This is due to the weaknesses of those algorithm where it requires theoretical knowledge of Mathematics (Elliptic Curve) requires large memory capacity (Coding Theory).

4. CONCLUSION

This paper is presented and explored several PKC algorithms to observe the development of these algorithm in since the last four decades. Based on the literature survey, it can conclude that public key cryptography research was very passive within 30 years since it was invented. However, in the last 10 years, the research in this area was so aggressively done. It is found that the most of the research were focused on Lattices (21%) and Integer Factorization (20%) algorithm. Overall, this paper contributes a platform for other researchers in PKC field to choose and use the appropriate algorithm based on the previous studies. In the next future effort, it is expected that few algorithms will be analysed in order to evaluate the strengths and weaknesses each of them.

REFERENCES

[1] 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.

[2] S. K. Rakeshkumar, "Performance Analysis of Data Encryption Standard Algorithm & Proposed Data Encryption Standard Algorithm," vol. 7, no. 10, pp. 11–20, 2013.

[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] 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.

[6] W. Diffie, W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] S. Boni, "Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm," vol. 130, no. 15, pp. 7–10, 1976.

[8] 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.

[9] M. J. Kakish, "SECURITY IMPROVMENTS TO THE DIFFIE-HELLMAN SCHEMES," vol. 8, no. July, pp. 79–85, 2011.

[10] A. Kaushik, "Extended Diffie-Hellman Algorithm for Key Exchange and Management," vol. 3, no. 3, pp. 67–70, 2013.

[11] R. Thanuja and D. K. S, "A NEW APPROACH TO DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM," vol. 1, no. 3, pp. 534–535.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[18] H. R. Hashim, "A New Modification of RSA Cryptosystem Based on The Number of The Private Keys," pp. 270–279.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] A. K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm," vol. 2, no. 1, pp. 159–163, 2015.

[24] P. P. Paul, "Implementing the Information Security using Modified RSA Algorithm with the Help of N Prime Number," pp. 18055–18062, 2016.

[25] 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.

[26] Josh Benaloh, "Dense Probabilistic Encryption," *In Proceedings of the Workshop on Selected Areas of Cryptography*. pp. 120–128, 1994.

[27] 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.

[28] 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.

[29] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani, "Enhanced public key security for the McEliece cryptosystem," no. 132256.

[30] L. Van Thai, "McEliece cryptosystem based identification and signature scheme using chained BCH codes," pp. 122–127, 2015.

[31] T. P. Berger, P. Cayrel, P. Gaborit, and A. Otmani, "Reducing Key Length of the McEliece Cryptosystem."

[32] 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.

[33] O. Regev, "On Lattices , Learning with Errors , Random Linear Codes , and Cryptography," no. 15848, pp. 1–37, 2009.

[34] R. Lindner and C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption," pp. 319–320, 2011.

[35] V. Lyubashevsky, C. Peikert, and O. Regev, "On Ideal Lattices and Learning with Errors Over Rings ∗," no. 15848, pp. 1–34, 2013.

[36] H. W. Kim and D. Choi, "Information security applications: 16th international workshop, WISA 2015 Jeju Island, Korea, August 20???22, 2015 revised selected papers," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9503, pp. 146–158, 2016.

[37] 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.

[38] D. Stehlé and R. Steinfeld, "Faster Fully Homomorphic Encryption," 2010.

[39] Z. Brakerski, "Efficient Fully Homomorphic Encryption from (Standard) LWE."

[40] 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.

[41] C. Peikert, "Lattice Cryptography for the Internet," pp. 1–25, 2014.

[42] P. Nguyen, "Cryptanalysis of the Goldreich – Goldwasser – Halevi Cryptosystem from Crypto ' 97," pp. 288–304, 1999.

[43] M. Van Dijk and C. Gentry, "Fully Homomorphic Encryption over the Integers," pp. 1–28, 2010.

[44] V. Miller, "Use of Elliptic Curves in Cryptography," *Adv. Cryptol. – CRYPTO'85*, vol. LNCS 218, pp. 417–426, 1986.

[45] 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.

[46] 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.

[47] H. Arshad and M. Nikooghadam, "Three-Factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems," 2014.

[48] Z. Tan, "RESEARCH ARTICLE A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems," 2014.

[49] 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.

[50] R. Rauscher, F. Bohnsack, Ý. Ü. Ý, and Ü. Ý, "Results of an Elliptic-Curve-Approach for Use in Cryptosystems µ," no. 1.

[51] 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.

[52] A. Khalique, "Implementation of Elliptic Curve Digital Signature Algorithm," vol. 2, no. 2, pp. 21–27, 2010.

[53] 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.

[54] 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.

[55] 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.

[56] P. S. Priyanka, "ENHANCED HYBRID CRYPTOGRAPHY," vol. 19, no. 2, pp. 108–113, 2016.

[57] V. Kapoor, "A Hybrid Cryptography Technique for Improving Network Security," vol. 141, no. 11, pp. 25–30, 2016.

[58] A. A. Patil, "Hybrid Cryptography Mechanism for Securing," pp. 1–4, 2016.

[59] 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.

[60] 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.

[61] E. Ramaraj, S. Karthikeyan, and M. Hemalatha, "A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)," pp. 78–86.

[62] S. Deshmukh, "Hybrid cryptography technique using modified," vol. 5, no. 6, pp. 7302–7304, 2014.

[63] 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.

[64] D. Jagadiswary and D. Saraswady, "Estimation of Modified RSA Cryptosystem with Hyper Image Encryption Algorithm," vol. 10, no. February, pp. 1–5, 2017.

[65] R. Ghosh, "AN EFFICIENT AND ROBUST MODIFIED RSA BASED SECURITY," vol. 6, no. 2, pp. 15–22, 2016.

[66] A. Mandal, D. Naccache, and M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," pp. 1–24, 2011.

[67] Z. Brakerski and G. Segev, "Better security for deterministic public-key encryption: The auxiliary-input setting," *J. Cryptol.*, vol. 27, no. 2, pp. 210–247, 2014.