A comparative survey of symmetric and asymmetric key cryptography

Sourabh Chandra
Assistant Professor
Department of Computer Science & Engineering,
Calcutta Institute of Technology
Kolkata, India
sourabh.chandra@gmail.com

Smita Paira
B.Tech Student
Department of Computer Science & Engineering,
Calcutta Institute of Technology
Kolkata, India
smtpaira@gmail.com

Sk Safikul Alam
Assistant Professor
Department of Computer Science & Engineering,
Calcutta Institute of Technology
Kolkata, India
mail2safikul@gmail.com

Dr.(Prof.) Goutam Sanyal
Professor
Department of Computer Science & Engineering,
National Institute of Technology
Durgapur, India
nitgsanyal@gmail.com

***Abstract*- Network security is an important aspect of information sharing. Attempts have been made to remove various insecurities over internet. For this, many technological implementations and security policies have been developed. The amount of data, transferred, is not a factor. The basic factor is, how much security, the channel provides while transmitting data. Cryptography is one such technique, which allows secure data transmission without losing its confidentiality and integrity. Based on the key distribution, cryptography is further classified into two major types-Symmetric Key Cryptography and Asymmetric Key Cryptography. In this paper, we have surveyed the traditional algorithms, along with the proposed algorithms based on their pros and cons, related to Symmetric and Asymmetric Key Cryptography. We have also compared the importance of both these cryptographic techniques. The proposed algorithms proved to be highly efficient in their respective grounds but there are certain areas that remained open, related to these algorithms, and have not yet been thoroughly discussed. This paper also presents an appropriate future scope related to these open fields.**

***Keywords*- Cryptography, Symmetric Key Cryptography, Asymmetric Key Cryptography, Public Key, Private Key, encryption, decryption, DPA,CPA, FPGA.**

I. INTRODUCTION

Cryptography is the technique of writing secrets. This secures data and information from any internal or external attacks. Thus, it provides integrity, confidentiality, non-repudiation and authenticity to the secret data. The concept of cryptography is based on two main terms-plain text and cipher text. The original message is called the plain text and the encrypted version of the message is called the cipher text. The cipher is finally decrypted to get the original message. Cryptography is broadly classified into two main types. These are symmetric key encryption technique and asymmetric key encryption technique.

A. Symmetric Key Cryptography

Symmetric key cryptography is also called secret-key or shared key cryptography. In this type of mechanism, the sender and receiver shares a common key for both encryption and decryption [42]. The method follows self-certification method i.e. the key is self-certified. The key needs to be shared through secret communication. If it is compromised then the encrypted message can be easily decrypted by the attacker. This type of cryptographic technique is required because it provides faster service without using many resources [43]. Various algorithms have been developed so far to describe symmetric key cryptography. These are AES, DES, 3DES, Blowfish.

978-1-4799-5748-4/14/$31.00 © 2014 IEEE

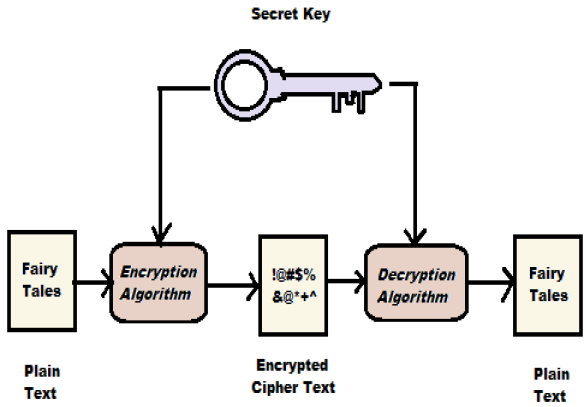

Fig.1. Symmetric Key Cryptography

B. *Asymmetric Key Cryptography*

The asymmetric key cryptography is known as public key cryptography. In this technique, the sender uses a public key of the receiver for encryption and the receiver uses his private key to decrypt the message. The concept of self-certification is absent here instead digital signatures are used to certify the keys. This method is more convenient and provides better authentication as the privacy remains intact [43]. There are various algorithms to implement this encryption mechanism. These are RSA, Diffie-Hellman, ECC and Digital Signature Algorithm.

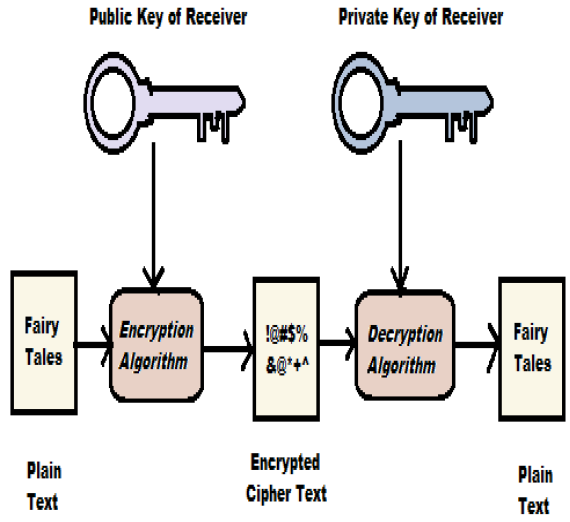

Fig.2. Asymmetric Key Cryptography

II. COMPARISON STUDY ON GENERAL SYMMETRIC KEY ALGORITHMS

The different algorithms for symmetric key cryptography are classified below.

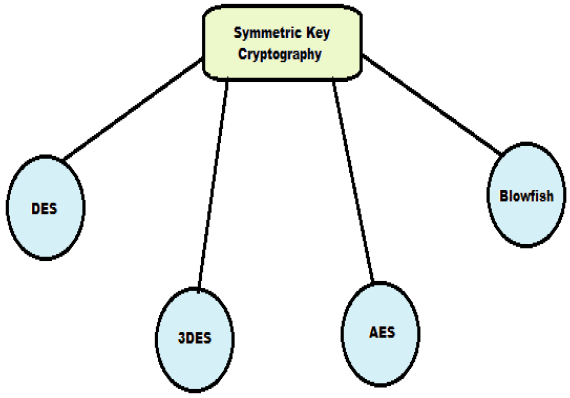

Fig.3. Classification of Symmetric Key Algorithms

TABLE 1. COMPARISON TABLE FOR DIFFERENT SYMMETRIC KEY ALGORITHMS

Method	DES	3DES	AES	Blowfish
Developed By	IBM and US government in 1974	IBM in 1978	National Institute of Standards and Technology (NIST)	Bruce Schneier in 1993
Structure of algorithm	Feistel Network	Fiestel Network	Substitution and Permutation Network	Fiestel Network
Key Length	56 bits	Three 64-bit keys, with overall key length of 192 bits [47]	128-bit, 192-bit, 256-bit	Variable key length with maximum key length of 448 bits
Block size	64	64	128	64
No. Of rounds	16	48	9	16
Vulnerabilities	brute force attack, man in the middle attack	Some theoretical attacks	Side channel attacks	Not prone to attacks.
Efficiency	Slow	Relatively slow in software [44]	Efficient in both Software and Hardware	Highly efficient in Software

III. COMPARISON STUDY ON GENERAL ASYMMETRIC KEY ALGORITHMS

The different algorithms for asymmetric key cryptography are classified below.

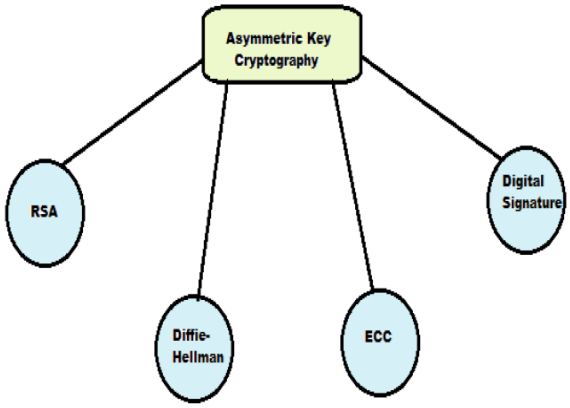

Fig.4. Classification of Asymmetric Key Algorithms

TABLE 2. COMPARISON TABLE FOR DIFFERENT ASYMMETRIC KEY ALGORITHMS

Method	Rivest-Shamir-Adleman (RSA)
Features	General form is (d, e) where d represents the private key and e represents the public key. Both encryption and decryption uses the same function [44].
Advantages	It is difficult to produce the private key from the public key and modulus, thus it is highly secure. Computing the reverse of e is very difficult for the attackers [45].
Downsides	Complexity of generating the key [46]. The process is quite slow. It has not been proved that it is equivalent to the factorization method and factorising a large number is very difficult.
Security Solutions	Key length should be larger than 1024 bits [45].
Method	Diffie-Hellman
Features	It is based on sharing the secret cryptographic key. This key is used for both encryption and decryption purposes. It relies on hardness of the discrete logarithms [53].
Advantages	As the symmetric key is of very short length (256 bits), the algorithm is quite fast [48].
Downsides	The longer the symmetric key is used the more attacks it will face [50]. More vulnerable to Man in the Middle attacks [49].
Security Solutions	Frequent key changing is essential. Development of Station-to-Station protocol defeats Man in the Middle attacks. The development of digital signature is also a solution to the attacks.
Method	Elliptical Curve Cryptography (ECC)
Features	It computes the keys through elliptic curve equations [51].
Advantages	It can yield security using a 164 bit key and is more advantageous than RSA and Diffie Hellman algorithms [51]. It consumes less power and provides better utilities to batteries.
Downsides	It increases the size of encrypted message and is more complex and difficult to implement, compared to RSA [52].
Security Solutions	Introduction of Elliptic Curve Digital Signature Algorithm (ECDSA) [53].The Authenticated key agreement protocol, ECMQV protects against Man-in-the-Middle attacks.
Method	Digital Signature Algorithm (DSA)
Features	It consists of a pair of large numbers, computed based on some algorithms to authenticate data [54]. The signatures are generated through private keys and are verified using public keys.
Advantages	It is very fast and provides non-repudiation and authenticity [55]. It secures the data against various attacks like Man-in-the-Middle attacks and is more advantageous than other asymmetric key algorithms.
Downsides	Digital signatures have short life span. They are not compatible with each other and thus complicate sharing [55].
Security Solutions	Verification software is necessary. Digital certificates should be bought from trusted authorities.

IV. COMPARISON STUDY OF NEWLY PROPOSED SYMMETRIC KEY ALGORITHMS

TABLE 3. COMPARISON TABLE FOR THE NEWLY PROPOSED SYMMETRIC KEY ALGORITHMS

Method	Algorithm against DPA attacks for both chips and Logic Circuits [12][13]
Characteristics	The model equations are first compared to that of CPA and then applied to AES and DES

	algorithms.
Advantages	It increases the robustness against the DPA attacks.
Pitfalls	Increasing the bus width will increase the number of keys. Hence, detection of correct key becomes difficult.
Implementations	Crypto chips and static logic circuits.
Method	Instruction Set Extensions for Symmetric Key algorithms [14]
Characteristics	It includes the codesign of hardware and software paradigms to achieve physical security, flexibility, portability and better performance with hardware implementations.
Advantages	It reduces execution time, program code size and increases the throughput.
Pitfalls	Embedded systems without any modified processor increases overhead, data transfer latency and other complexities.
Implementations	Medical databases, e-mails, e-commerce, e-banking, etc.
Method	Parallel hardware architecture for AES-GCM algorithm[15]
Characteristics	It optimizes a number of logic gates and then compares the performance of S-Boxes with ASIC 65 nm CMOS technology.
Advantages	It provides both authenticity and confidentiality simultaneously for sensitive data.
Pitfalls	If the area effort increases, the overhead delay increases. If the critical path delay increases, the sub pipelining of the system cannot increase its frequency.
Implementations	Various hardware and software
Method	Fast encryption algorithm for multimedia (FEA-M) [16][18]
Characteristics	It uses resynchronization process for chosen and known plain text attacks.
Advantages	It provides an efficient alternative against breakability of FEA-M to various attacks.
Pitfalls	The process has weakness in the algebraic structures used.
Implementations	Has various multimedia applications
Method	Key transfer protocol for secret sharing applications [17]
Characteristics	It uses various threshold and secret sharing schemes for key exchange. It highlights both message authentication and conditional access.
Advantages	It allows the generation of different keys for the different set of receivers. It employs minimum computational requirements and does not depend on any mathematical assumptions.
Pitfalls	The process consumes much time.
Implementations	Satellite, internet, cable networks, etc.
Method	Rekeying architecture based on Tree Parity Machine [19]
Characteristics	It uses TDMA with a single TPM unit. It implements both FPGA and ASIC realization using VHDL.
Advantages	It is cost effective, consumes less time with a limited bandwidth and overhead.
Pitfalls	Key lifetime is short. It reduces the storage area by increasing the cycles for generating the output bit.
Implementations	Embedded system environments.
Method	Instruction Level distributed Processor (COBRA) [20]
Characteristics	It provides flexibility through reconfiguration. It maps and implements the algorithms using COBRA assembly language. Data is gathered using cycle counts.
Advantages	It provides both high speed processing and security. It provides an efficient implementation of a variety of block ciphers and can achieve a through of 622 Mbps.
Pitfalls	The block ciphers to be tested should be of varying efficiency and performance.
Implementations	Various network encryption implementations like ATM.

Method	Compression and Encryption scheme based on arithmetic coding and coupled chaotic systems [21][24]
Characteristics	It depends on zero-order arithmetic coding using bit streams generated by CCS PRBG. Algorithms are tested using text files.
Advantages	It is highly secure and is not vulnerable to attacks against arithmetic coding and plain texts.
Pitfalls	The zeroth order suffers about 6% over other techniques.
Implementations	Various ad hoc networks.
Method	Operation Centred approach of fault detection [22]
Characteristics	It enumerates the arithmetic and logical operations and then analyses the efficiency and hardware complexity using 11 symmetric ciphers.
Advantages	It can perform the analysis even if the error propagation is non-linear. Detection coverage is 100%
Pitfalls	Analysis of multiple bit error is complicated.
Implementations	Ad Hoc networks, etc.
Method	Sharing Session Key component algorithm [25]
Characteristics	Messages are protected through radio links and are clear for network operator. The algorithm operates so long the communication is disputed to endanger public safely.
Advantages	It improves symmetric key encryption technique by providing non-repudiation and end-to-end security to each individual in communication.
Pitfalls	Key Escrow Trust Organization cannot recover the session key. It has finite computing capacity and less power.
Implementations	Digital Mobile communications, E-commerce
Method	Symmetric key encryption algorithm based on 2-d geometry [26]
Characteristics	It includes both the properties of circle and circle centred angles. It provides high confidentiality with less computational complexity.
Advantages	In every steps of encryption, it produces fixed size messages.
Pitfalls	Floating point operations limit the size of block to encode. Hardware implementation is tricky.
Implementations	E-commerce, banking, stock trading, etc.
Method	Method of Digital Signature based on combined symmetric key algorithm [27]
Characteristics	It depends on both symmetric and hardware technology. It uses timestamps as a factor of such symmetric key algorithms.
Advantages	The key is time variant and maintenance free. It deciphers faster and has a simple key management compared to asymmetric digital signature algorithms.
Pitfalls	The process is slight lengthy.
Implementations	Various transactions like e-commerce, etc
Method	Hill-Shift-XOR encryption technique for image encryption[28]
Characteristics	Encryption is performed using block wise XOR operations. It can operate in color, gray scale and binary images.
Advantages	It is reliable where cryptanalysis is quite difficult. It is robust.
Pitfalls	The technique is relatively slow.
Implementations	Digital data protection, copy protection, etc.
Method	DJSA Symmetric key algorithm [29]
Characteristics	Unlike the MSA method [30] it uses a key matrix of size 65536 and each cell stores 2 character patterns.
Advantages	It provides high protection against Brute force attack and can encrypt a file of less than or equal to 2 MB.
Pitfalls	If the file size is very big, the process becomes slow.
Implementations	If the file size is very big, the process becomes slow.

Method	NJJSAA Symmetric key algorithm [31]
Characteristics	The process performs key exchange and XOR operations for both encryption and decryption.
Advantages	It is better than other general cryptographic algorithms. It can encrypt both large and small files.
Pitfalls	The process is slight lengthy.
Implementations	Government sectors, banks, database encryption, etc.
Method	DJMNA Symmetric key algorithm [32]
Characteristics	It combines both MGVC and DJSA methods. The order of these algorithms depends on the random matrices developed during the process.
Advantages	The encrypted message is very hard to decrypt using any Brute Force attack.
Pitfalls	The process is complex and lengthy.
Implementations	Password encryption, mobile network, ATM network, etc.
Method	Symmetric key based RFID authentication protocol [33]
Characteristics	It implements three protocols that use same block cipher by implementing same RF based hardware.
Advantages	This protocol improves the RFID system by providing security against various attacks at low computational cost.
Pitfalls	The process is lengthy.
Implementations	Communication networks, business houses, etc.
Method	Wireless Secret key generation algorithm in multiuser networks [34]
Characteristics	It works in multiuser networks and checks how such diversity affects secret key randomness.
Advantages	It increases the randomness performance and reduces the execution time.
Pitfalls	Update of secret key is necessary for proper security.
Implementations	Various wireless communication networks.

Method	Symmetric key encryption algorithm based on linear geometry[36]
Characteristics	Both substitution and transposition techniques are applied to secure a secret image over any unreliable communication. It generates a random matrix and shuffles the ciphered bytes among N bytes of secret files.
Advantages	Robust and potential to the security needs of digital images. Correlation value for both secret and encrypted image is one.
Pitfalls	----------
Implementations	Medical, commercial and military systems.
Method	Symmetric key encryption algorithm based on cyclic elliptic curve and chaotic system [37]
Characteristics	It provides authentication using neural networks. It performs the encryption for 256-bit plain image to 256-bit cipher image using eight 32-bit registers. Based on piecewise non-linear chaotic map, the method generates pseudorandom bit sequences for round keys.
Advantages	Large key space, faster, good encryption effect and sensitive to small changes.
Pitfalls	If the change in media data is quite smaller than the adjustable parameter ranging, then the algorithm fails.
Implementations	Various business requirements.
Method	Secure protocol using the property of Quantum Wave Function [38]
Characteristics	At a given time, the state of a particle is managed by position and momentum. The physical significance of a particular wave function depends on a linear vector space.
Advantages	It prevents attack on user's password using quantum computing efficiency. It

	prevents compromising passwords and can replace the bounded key length classical encryption algorithms.
Pitfalls	----------
Implementations	Various hardware implementations.

V. COMPARISON STUDY OF NEWLY PROPOSED ASYMMETRIC KEY ALGORITHMS

TABLE 4. COMPARISON TABLE FOR THE NEWLY PROPOSED ASYMMETRIC KEY ALGORITHMS

Method	Prime Number Generation[1]
Characteristics	Prime numbers are generated randomly from a large series using the divisibility tests.
Advantages	Scrambled messages using two prime factors become difficult to break. So, data remains highly secured.
Pitfalls	The bit length of the prime numbers should be pre determined. Generating big prime numbers is quite difficult.
Implementations	Money transfer, business transactions, diplomatic communications, books, audio, video, etc.
Method	Image security through asymmetric watermarking algorithm [2][3][4][5]
Characteristics	Embedding and detection are done separately using private and public key respectively. It is based on linear algebra.
Advantages	This algorithm is highly efficient as it provides a double layer security level for protecting digital data. It is simple and saves the computational cost.
Pitfalls	If a particular integer is big then the watermark is not detected to the original encrypted images.
Implementations	Copy protection frameworks [12]
Method	Cryptanalysis using COPACOBANA[6]
Characteristics	It consists of 120 field programmable gate arrays. It can solve various computations without any mathematical breakthrough.
Advantages	It helps in faster RSA factorization and can secure ECC. It provides a cost effective service.
Pitfalls	To make the overall machine design cost effective, many small FPGA modules are designed. This requires extra space.
Implementations	Useful tool for parallel computational problems [13]
Method	Generation of a multimode multiplier [7]
Characteristics	The multimode multiplier consists of four phases and uses a series of right shifting and additions.
Advantages	The multimode multiplier consists of four phases and uses a series of right shifting and additions.
Pitfalls	The multimode multiplier wastes power if operated in AES mode. The power consumption is high.
Implementations	It can be applied to various polynomial fields and helps in matrix-vector multiplications.
Method	Master-key-encryption-based multiple group key management scheme (MKE-MGKM) [8]
Characteristics	The MKE-MGKM is used to tackle various multicast groups existing in a single network.
Advantages	The MKE-MGKM is simple and requires less memory storage for the keys.
Pitfalls	Communication overhead is greater than storage overhead.
Implementations	Various broadcasting like TV and wireless mobile networks.
Method	Asymmetric Public Key Traitor Tracing Schemes [9]
Characteristics	It uses a multiplicative cyclic group of very big prime order and then it evaluates an oblivious polynomial.
Advantages	It traces the traitor, in digital content, responsible for the construction of pirate keys, ensuring non-repudiation.
Pitfalls	Broadcasting streams are quite expensive. There is a trade off between protection and

	content distribution.
Implementations	Various entertainment devices like TV.
Method	Feigenbaum encryption method of messages [10]
Characteristics	It uses two pairs of asymmetric private keys. It makes use of a logistic difference equation.
Advantages	It, specially the double F-sequence coding, makes a better use of the encryption technique in the messages and can confuse the attacker who employs nearly the correct keys.
Pitfalls	The requirements are time consuming which cannot be satisfied by an efficient computer program.
Implementations	Various online communication mediums.
Method	Asymmetric DNA algorithm [11]
Characteristics	It encrypts the plain text using the existing biological information from the DNA public databases. It is implemented in BioJava and Matlab
Advantages	It does not require several iterations for derivation of keys and the keys can be retrieved. It is more reliable and powerful than OTP DNA algorithm.
Pitfalls	The process is lengthy and kills the execution time.
Implementations	Researches in DNA computations.
Method	Key assessment scheme for secure broadcasting [23]
Characteristics	The scheme employs ECC cryptographic algorithm. The number of encryption keys depends on the access control policies.
Advantages	It is highly efficient. Storage of decryption keys in tamper resistance device is easier.
Pitfalls	Security solutions especially in case of smart cards are not cleared.
Implementations	TV systems, electronic subscription, etc.

Method	Method for increasing security in RSA [35]
Characteristics	It eliminates the distribution of n large numbers whose factors become difficult to design using RSA algorithm.
Advantages	It protects the messages from the mathematical factorization attacks which the general RSA algorithm suffers from.
Pitfalls	It increases the time complexity.
Implementations	Various hardware and software
Method	Model based on Pretty Good Privacy (PGP) to secure E-Commerce through Asymmetric Key encryption technique [39]
Characteristics	It implements the RSA algorithm for encryption or decryption purposes. It is based on PGP and dual signature method.
Advantages	It provides security issues at various levels like transaction level, reply attacks, mutual authentication, Network and transport level, etc.
Pitfalls	----------
Implementations	Biometric system, Internet banking, ATM machine, Key exchange and Digital signature, etc.
Method	Technique based on Elliptical Curve Cryptography (ECC) through the implementation of hidden generator point in WSNs [40]
Characteristics	Digits are extended beyond two bits for representing k, where k is any integer in prime field as the ECC is represented as T=k*G where G are the points on elliptic curve. The 192-bit values are stored in a 24*8 array.
Advantages	It provides better security against the physical node capture and man in the middle attacks.
Pitfalls	The communication cost is high as it requires multiple computations.
Implementations	Various Wireless Sensor Networks

Method	Hardware/software codesign of ECC for Resource constrained applications [41]
Characteristics	It helps in binary field multiplication in software. It also offers instruction set extensions and presented a coprocessor for binary multiplication.
Advantages	It is highly efficient in terms of performance and area.
Pitfalls	Nothing has been mentioned about power consumption.
Implementations	Brand protections, etc.

VI. FUTURE SCOPE

For efficient data transmission, cryptography is an ultimate solution. Many algorithms have developed so far, based on both Symmetric and Asymmetric key Cryptography. The algorithms are effective in ensuring data privacy, integrity, authenticity and non-repudiation. However, there are certain areas that still remain open. Quantum cryptography is considered to be an excellent replacement for Diffie-Hellman algorithm as the data transferred through it highly secured. But it cannot provide protection against the classical bucket brigade attacks. Methods could be developed to overcome this problem. Scrambled messages using two prime factors provide high security to data. Methods could be generated to remove the difficulty of generating large prime numbers.

VII. CONCLUSION

Both Symmetric and Asymmetric Key algorithms are highly efficient in securing the transferred data over any communication medium. In this paper, we have highlighted the basic as well as proposed algorithms related to these cryptographic techniques. In Symmetric Key Cryptography, a single key is for both encryption and decryption purposes. The sharing of this key becomes sometimes insecure. On the other hand, Asymmetric Key Cryptography uses two separate keys to prevent any unethical access to the data. The public key remains public and the private key is not shared. This technique ensures better security than the former. Moreover, the use of Digital Signatures in case of Asymmetric Key Cryptography provides high data confidentiality and non-repudiation. Yet, Symmetric Key Cryptography has many well known applications because of its simplicity.

REFERENCES

[1] Arun Kejariwal, " Cryptic primes", *IEEE Potentials*, pp. 43-45, Feb./Mar. 2004, IEEE

[2] Minoru Kuribayashi and Hatsukazu Tanaka, "Fingerprinting Protocol for Images Based on Additive Homomorphic Property", *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2129-2139, Dec. 2005, IEEE

[3] Subramania Sudharsanan, " Shared Key Encryption of JPEG Color Images**",** *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp. 1204-1211, Nov. 2005, IEEE

[4] G. Boato, N. Conci, and V. Conotter, F.G.B. De Natale, and C. Fontanari, "Multimedia asymmetric watermarking and encryption", E*lectronics Letters*, vol. 44 no. 9, April 2008, IEEE

[5] Boato, G., De Natale, F.G.B., and Fontanari, C.: 'An improved asymmetric watermarking scheme suitable for copy protection', *IEEE Trans. Signal Process.*, 54 (7), pp. 2833–2834, 2006, IEEE

[6] Tim Gu¨neysu, Timo Kasper, Martin Novotn_y, Christof Paar, and Andy Rupp, "Cryptanalysis with COPACOBANA", *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1498-1513, Nov. 2008, IEEE

[7] Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, "An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 4, pp. 553-563, April 2010, IEEE

[8] Min-Ho Park, Young-Hoon Park, Han-You Jeong, and Seung-Woo Seo, "Key Management for Multiple Multicast Groups in Wireless Networks", *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1712-1723, Sept. 2013, IEEE

[9] Aggelos Kiayias and Moti Yung, "Breaking and Repairing Asymmetric Public-Key Traitor Tracing", pp.1-16, IEEE

[10] Robert M. Bevensee, "Feigenbaum encryption of messages", *IEEE Potentials*, pp. 39-41, Feb. /Mar. 2001, IEEE

[11] Radu Terec, Mircea-Florin Vaida, Lenuta Alboaie, and Ligia Chiorean, "DNA Security using Symmetric and Asymmetric Cryptography", *The Society of Digital Information and Wireless Communications*, vol-1, no-1, pp. 34-51, 2011, IEEE

[12] Massimo Alioto, Massimo Poli, and Santina Rocchi, "Differential Power Analysis Attacks to Precharged Buses: A General Analysis for Symmetric-Key Cryptographic Algorithms", *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, pp. 226-239, July-Sept. 2010, IEEE

[13] Massimo Alioto, Massimo Poli, and Santina Rocchi, "A General Power Model of Differential Power Analysis Attacks to Static Logic Circuits", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 5, pp. 711-724, May 2010 , IEEE

[14] Sean O'Melia and Adam J. Elbirt, "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 11, pp. 1505-1518, Nov. 2010, IEEE

[15] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, "Efficient and High-Performance Parallel Hardware Architectures for the AES-GCM", *IEEE Transactions on Computers*, vol. 61, no. 8, pp. 1165-1178, Aug. 2012, IEEE

[16] Miodrag J. Mihaljevic´, Ryuji Kohno, "Cryptanalysis of Fast Encryption Algorithm for Multimedia FEA-M", *IEEE Communications Letters*, vol. 6, no. 9, pp. 382-384, Sept. 2002, IEEE

[17] Ahmet M. Eskicioglu and Edward J. Delp, "A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING APPLICATIONS TO INFORMATION SECURITY", *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 816-824, Nov. 2002, IEEE

[18] Miodrag J. Mihaljevic, "On Vulnerabilities and Improvements of Fast Encryption Algorithm for Multimedia FEA-M", *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1199-1207, Nov. 2003, IEEE

[19] Markus Volkmer and Sebastian Wallner, "Tree Parity Machine Rekeying Architectures", *IEEE Transactions on Computers*, vol. 54, no. 4, pp.421-427, April 2005, IEEE

[20] Adam J. Elbirt and Christof Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography", *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 5, pp. 468-480, May 2005, IEEE

[21] Ranjan Bose and Saumitr Pathak, "A Novel Compression and Encryption Scheme Using Variable Model Arithmetic Coding and Coupled Chaotic System", *IEEE Transactions on Circuits and Systems—I: Regular Papers*, vol. 53, no. 4, pp. 848-857, April 2006, IEEE

[22] Luca Breveglieri, Israel Koren, and Paolo Maistri, "An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers", *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 635-649, May 2007, IEEE

[23] Elisa Bertino, Ning Shang, and Samuel S. Wagstaff Jr., "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 2, pp. 65-70, April-June 2008, IEEE

[24] Chung-Ming Ou," Design of Block Ciphers by Simple Chaotic Functions", *IEEE Computational Intelligence Magazine*, pp.54-59, May 2008, IEEE

[25] Hsiao-Kuang Wu, Shu-ching Yang, and Yung-Tai Lin, "The Sharing Session Key Component (SSKC) Algorithm for End-to-End Secure Wireless Communication", pp. 242-250, IEEE

[26] Mohammad Jabed Morshed Chowdhury and Tapas Pal, "A New Symmetric Key Encryption Algorithm based on 2-d Geometry", *2009 International Conference on Electronic Computer Technology*, pp. 541-544, IEEE

[27] Wu Suyan, Li Wenbo, and Hu Xiangyi, "Study of Digital Signature with Encryption Based on Combined Symmetric Key", IEEE

[28] Bibhudendra Acharya, Sambit Kumar Shukla, Saroj Kumar Panigrahy,Sarat Kumar Patra, and Ganapati Panda, "H-S-X Cryptosystem and Its Application to Image Encryption", *2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pp.720-724, IEEE

[29] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, and Asoke Nath, "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm", *2011 International Conference on Communication Systems and Network Technologies,* pp. 89-94, IEEE

[30] A.Nath, S.Ghosh, and M.A.Mallik, "Symmetric key cryptography using random key generator", *Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010*, vol-2,pp. 239- 244

[31] Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan Chakraborty, and

Asoke Nath, "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", *2011 International Conference on Communication Systems and Network Technologies*, pp. 125-130, IEEE

[32] Debanjan Das, Megholova Mukherjee, Neha Choudhary, Asoke Nath, and Joyshree Nath, "An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm", *2011 World Congress on Information and Communication Technologies*, pp. 1199-1204, IEEE

[33] Guangyu Zhu and Gul N. Khan, "SYMMETRIC KEY BASED RFID AUTHENTICATION PROTOCOL WITH A SECURE KEY-UPDATING SCHEME", *2013 26th IEEE Canadian Conference of Electrical And Computer Engineering (CCECE)*, IEEE

[34] Seon Yeob Baek and Jongwook Park, "A Study on Wireless Secret Key Randomness in Multiuser Networks", *ICTC 2013*, pp. 1048-1052, IEEE

[35] Rohit Minni, Kaushal Sultania, Saurabh Mishra, and Prof Durai Raj Vincent, "An Algorithm to Enhance Security in RSA", *4th ICCCNT 2013*, pp. 1-4, IEEE

[36] Prabir Kr. Naskar, Ayan Chaudhuri, and Atal Chaudhuri, "A Secure Symmetric Image Encryption Based on Linear Geometry", *2014 Applications and Innovations in Mobile Computing (AIMoC)*, pp. 67-74, IEEE

[37] Ankita Baheti, Lokesh Singh, and Asif Ullah Khan, "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System and Authentication using Neural Network", *2014 Fourth International Conference on Communication Systems and Network Technologies",* pp. 664-668,IEEE

[38] Wafa Elmannai, Khaled Elleithy, Varun Pande, and Elham Geddeda, "Quantum Security using Property of a Quantum Wave Function", IEEE

[39] Ankur Chaudhary, Khaleel Ahmad, and M.A. Rizvi, "E-commerce Security Through Asymmetric Key Algorithm", *2014 Fourth International Conference on Communication Systems and Network Technologies,* pp.776-781, IEEE

[40] Ravi Kishore Kodali, "ECC with Hidden Generator Point in WSNs", *2014 IEEE Region 10 Symposium*, pp. 131-136, IEEE

[41] Andrea Höller, Norbert Druml, Christian Kreiner, Christian Steger, and Tomaz Felicijan, "Hardware/Software Co-Design of Elliptic-Curve Cryptography for Resource-Constrained Applications", *DAC '14 June 01 - 05 2014*, IEEE

[42]www.webopedia.com/TERM/S/symmetric_key_cryptography.html

[43]voices.yahoo.com/comparing-symmetric-asymmetric-key-encryption-6329400.html

[44]www.cs.usfca.edu/~brooks/S04classes/cs480/lectures/algs.pdf

[45]www.encryptionanddecryption.com/algorithms/asymmetric_algorithms.html

[46]scialert.net/fulltext/?doi=itj.2013.1818.1824

[47] www.vocal.com/cryptography/tdes/

[48]home.cyber.ee/ahtbu/CDS2011/SandraNetsajevaSlides.doc

[49]searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange

[50]learningnetwork.cisco.com/servlet/.../WP_Palmgren_DH.pdf

[51]searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

[52]www.ehow.com/info_12226350_advantages-disadvantages-elliptic-curve-cryptography-wireless-security.html

[53]vanilla47.com/PDFs/Cryptography/Miscellenea/Eliptic%20Curve%20Cryptography/A_tutorial_of_elliptic_curve_cryptography.pdf

[54]searchsecurity.techtarget.com/definition/Digital-Signature-Standard

[55] lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/