A Comparative and Analytical Study on Symmetric Key Cryptography

Bidisha Mandal
Department of Computer Science
& Engineering,
Calcutta Institute of Technology
Kolkata, India
Bidishamandal1994@gmail.com

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

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

Subhendu Sekhar Patra
Department of Computer Science
& Engineering,
Calcutta Institute of Technology
Kolkata, India
patrajgec@gmail.com

***Abstract--* Science and Technology are updating rapidly. Data are transferred through various communicative mediums. Hence always there been a major requirement of confidentiality and secure authorization of information to prevent the unauthorised access and attacks. Symmetric key cryptography is an integral part of cryptographic technique which ensures high security and confidentiality of data transmitted through the communication channel using a common key for both encryption and decryption. There are so many traditional symmetric key algorithms as well as some proposed algorithms which can provide high confidentiality along with authorized access of data. In this paper we made a comparison analysis of some of those proposed algorithms as well as the traditional algorithms of symmetric cryptography with the merits and demerits of those different types algorithm.**

Keywords— **Cryptography; CRL checking; CPA; DPA; ECC; ECDSA; MANET; S-Box; SKD algorithm; UWSN; VANET.**

I. INTRODUCTION

Cryptography, means Hidden Writing. Cryptography is a process of transforming a readable plain text into a cipher text. It follows two steps: encryption and decryption to achieve the data security. A secret key is being used to encrypt or decrypt the secret text. Before sending confidential data to recipient the plain text embedded with the secret key generates the unreadable cipher text and only the authorised person can decrypt it with the secret key. So any unauthorised person is unable to detect the original information. Based on the secret key used, cryptography broadly divides into two branches: Symmetric Key Cryptography and Asymmetric Key Cryptography. A shared secret key is used to encrypt the plain text or decrypt the cipher text in Symmetric Cryptography i.e. a common key is being used in Symmetric key cryptography for both encryption and decryption whereas in Asymmetric Cryptography a public key (known to everyone) used for encryption and a private key (only known to the recipient) is used for decryption [20]. Security of information depends on the encryption-decryption algorithm and the strength of secret key used [1]. Though various symmetric key algorithms are proposed and implemented so far, we have discus about some of them in this paper.

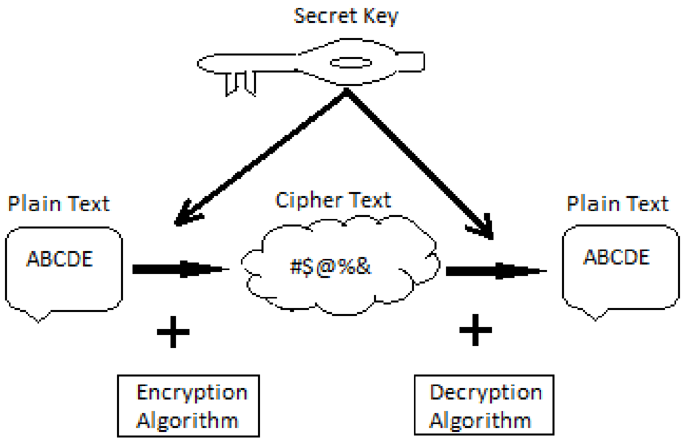

Fig. 1 Symmetric Key Cryptography

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

II. LITERATURE SURVEY ON TRADITIONAL SYMMETRIC KEY CRYPTOGRAPHY

In this section we made a survey on the traditional algorithm like AES, DES, 3DES, blowfish algorithm and made a comparison among them based on the basic features like key size, block size, number of rounds taken to encrypt or decrypt the data by those algorithm as well as we highlighted the cryptanalysis attacks which are able to break the security of those algorithms .

TABLE I . COMPARISON TABLE OF TRADITIONAL ALGORITHM

Algorithm	**Structure**	**Key Size (bits)**	**Block Size (bits)**	**Rounds**	**Security Drawbacks**
AES	Substitution permutation network	128, 192, 256	128	9	Side Channel attack [10]
DES	Balanced Feistal Network	56	64	16	Brute Force Attacks , Differential Cryptanalysis and Meet-In-The-Middle attacks [25]
3-DES	Feistal Network	168, 112, Or 56	64	48 DES equivalent rounds [10]	May be possible Theoretically
Blowfish	Feistal Network	32-448	64	16	Not yet detected

III. SURVEY ON NEWLY PROPOSED SYMMETRIC KEY CRYPTOGRAPHY

A novel sensor node capture attack detection and defence protocol known as SCADD protocol proposed by S.H.Jokhio *et al.*[17] to eliminate the probabilities of node compromise and node capture attacks in wireless sensor networks. Based on two major block elements i.e. node attack detection (NAD) block and defence advocating measure (DAM) block SCADD provides the security. In SCADD a self destructing protocol have been implemented in the DAM block which marks the intensity of attack and defence the attack by removing all important information from the sensor nodes memory.

A DPA resistance countermeasure circuit had been proposed by Po-Chun Liu *et al.*[18], which implements an AES engine using CMOS technology. This DPA resistance circuit consist of Galois ring oscillator sets (GaRO) and Fibonacci ring oscillator sets (FiRO). Random numbers are generated by connecting a feedback polynomial with the oscillator. Jun Wu *et al.* described an asynchronous AES substitution box (S-Box) based on null convention logic (NCL) [19]. This proposed NCL S-Box is most effective to resist the Differential Power Analysis (DPA) attack and Correlation Power Analysis (CPA) attack which are the well-known threat to the cryptographic chip implementing Field Programming Gate Array (FPGA). Low power consumption is one of the beneficial property of NCL S-Box. This Proposed S-Box consumes 22%-26% less power than the Synchronous S-Box. They implement the NCL S-Box using VHDL.

Albert Wasef *et al.* [3] proposed an expedite message authentication protocol (EMAP) for VANETs, which catalyses message authentication process. It superseded the time consuming CRL checking process. Message is authenticated by checking the sender's certificate, generated by a Trusted Authority (TA). A Key Hash Management Authentication code (HMAC) enhances the revocation checking process with a novel probabilistic key distribution mechanism. It reduces the message loss ratio due to message authentication delay and working at a speed of 124message verification per 300msec. An ID-based anonyms user authentication scheme with a cross-layer verification scheme was suggested by Subir Biswas *et al.* [8], using ECDSA incorporating an ID-based signature, where the common geographical position of sinning vehicles is consider as ID of this vehicle and any vehicle can authenticate the received message by using it own ID without depending on any trusted third party. The On Board Unit (OBU) integrated with GPS device detects the current position of participating OBU in the VANET. The verification mechanism approaches MAC (Medium Access Control) level priorities. Sohil Abbas *et al.* [6], proposed a new scheme to detect Sybil attacks on MANETs without using centralized third party or any localization technique such as directional antenna or GPS. It uses RSS (Received Signal Strength) for the detection of legitimate and Sybil nodes. It produces high true positives (around 90%) assuming that maximum speed up for any node is 10m/s i.e. 36 km/h. A self-configured network protocol [4] proposed on April, 2013 that allows data distribution and resources sharing among the users of a spontaneous wireless ad hoc network based on trust. This protocol uses asymmetric cryptography for device identification using public-private key and symmetric cryptography to exchange session keys between nodes. Tomasz Rams *et al.* [5], make a survey on self-healing group key distribution scheme for wireless sensor network . Any new node is able to join the network only if he/she knows anyone of this network. Existing member validate the new node using a Identity card(IDC) and IP address. It permits the group members to retrieve missing session keys from the recent key distributed broadcast message, without depending on additional transmission from the group manager. Session keys of self healing techniques generated based on SKD algorithms such as Polynomial based SKD algorithm and Exponential SKD algorithm.

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

Lingfang Zeng *et al.*, on June 2013[7], proposed a Self-Destructing Data System (Se Das), a proof-of-concept prototype with active storage techniques based on T10 OSD standard. Se das uses Shamir algorithm [2] [23] to generate a pair of key and user specifies the life time of each key for each authenticated user. On expiration of user specifies time sensitive information such as bank account number, Password, important documents becomes unreadable one for security and confidentiality of information.

Nguyen Ngoc Mai-Khanh *et al.* [9], proposed an integrated high-precision magnetic probe with Low Noise Amplifier (LNA) in a 0.18 µm CMOS for the near-field magnetic measurement on cryptographic LSI chip. This self-biased cascade LNA provides maximum gain up to 63 dB. Focused-Ion-Beam (FIB) technique is applied to driven away the Si-substrate under the coil region to enhance the coils performance. A 7mm x 9mm 2-D distributed magnetic field maps of an on board AES encrypted FPGA operating at 24 MHz, are measured by higher-special-resolution probe.

IV. COMPARISON STUDY ON SOME PROPOSED ALGORITHMS OF SYMMETRIC KEY CRYPTOGRAPHY, BY SOME RESEARCHER

We made a survey on newly proposed algorithm which are based on the traditional algorithms in order to increase the security level, computations efficiency. We made a comparison study to highlighted the basic property, advantages, drawbacks, attacks resisted by those proposed algorithm as well as mentioning their applications to analyse for the better algorithm.

TABLE II. COMPARISON TABLE OF SOME PROPOSED ALGORITHM

Method 1: A True Random-Based DPA resistance AES engine	
Property	1. This engine implements AES cryptography technique. 2. The AES engine incorporates CMOS technology. 3. DPA resistance circuit consisting of ring oscillator and linear feedback shift registers to generate random numbers.
Advantages	1.The proposed DPA resistance circuit resulting 6.2% area overhead without degrading the throughput which is about 2.97 Gb/s [18]
Prevents from Attacks	1.DPA attack
Downside	1.Random number generator could generate the same bytes of random number causes no change in the additional power consumption after resetting the system.
Applications	1.This proposed DPA resistance circuit can be applicable in the Cryptographic chip architectures.
Method 2: NCL S-Box (Null Convention Logic S-Box)	
Property	1. Based on null convention logic this S-Box implements AES algorithm and the cryptographic secret key has been fabricated with in a FPGA chip. 2.NCLS-Box implements clock free asynchronous circuits to avoid the clock related information leakage. 3. NCL S-Box consumes low power about 22% to 26% than the synchronous S-Box [19].
Advantages	1. Reduce noise and electromagnetic interference. 2. Consume low power. 3. Operates at high speed.
Prevents from Attacks	1. Side channel attack 2. DPA (Differential Power Analysis) attack 3. CPA (Correlation Power Analysis) attack
Downside	1. Critical to implement in AES hardwired circuit.
Applications	1.Applicable for energy constrained mobile crypto application. 2. Suitable for protect FPGA based crypto-chip.
Method 3: Expedite Message Authentication Protocol (EMAP) for VANETS	
Property	1. EMAP employs a fast and secured keyed HMAC function[21] for revocation checking. 2.EMAP is free from false positive property. 3. The modular feature of EMAP makes it intregrable with any PKI, without modifying the architecture of PKI. 4. Respecting the WAVE standard ,ECDSA is used to check the authenticity of certificate.
Advantages	1. Computational complexity of EMAP is O(1) whereas in case of normal binary search CRL checking O(log N_{rev}) and linear search CRL is O(N_{rev}) . 2. EMAP authenticate 124 messages per 300 msec. [3]. 3.EMAP decreases the message loss ratio and authentication delay.
Prevents from Attacks	1.Forging Attack 2.Replay Attack 3.Colluding Attack
Downside	1.In absence of Road Side Unit(RSU) ,OBU has no option to communicate with the Trusted Authority(TA). 2.Compared to the WAVE Standard EMAP increases communication overhead about 0.03 percent.
Applications	1.Applicable for both high and low density VANETs. 2.Applicable in any Network System incorporating PKI.
Method 4: A Self Configured Spontaneous Wireless Ad Hoc Network Protocol	
Property	**1**. In this protocol Data and resource sharing is secured based on trust among the members of the networks. Any new node is able to join the network only if he/she knows anyone of this network. Existing member validate the new node using a Identity card (IDC) and IP

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

	address. 2. It is self-configured using IP and DNAs of devices. Certificate Authority (CA) is distributed among the members. 3.ECC and RSA are used for session key distribution and user authentication and 128 bit AES is used for exchanging session key between trusted nodes [4]. 5. Short range resource sharing technology used to join the network.
Advantages	1. Users are free to join or leave the network. [11] based on trust between members of the network. 2.This protocol required less amount of memory storage 3. This protocol provides the opportunity of resource sharing without any infrastructure, even in the devices with limited resource.
Prevents from Attacks	1.Phishing 2.active or passive spoofing
Downside	1.This protocol works within a limited region and limited validation time of session key.
Application	1.Useful for source sharing technology like Bluetooth sharing, limited resource devices such as mobile, PDA, laptop [11].
Method 5: Group key distribution using self healing property	
Property	1. A resource rich, high computational powered node of a wireless sensor network considered as Group Manager (GM) who broadcast the session key at the very beginning of each session of a group conversation. 2.This scheme allows the group member to get a valid session key from the last broadcast message. 4. Session keys of self -healing techniques is generated based on SKD algorithms.
Advantages	1. Any member of the network is free to retrieve the lost session key from the last conversation, without any additional key request to the group manager [5]. 2. Members are permitted to spontaneously join or leave the group using the session key and their own private key.
Prevents from Attacks	1.This scheme prevents the unauthorized nodes to access the session key.
Downside	1.In self keying process maximum scheme lifetime is limited by maximum number of sessions 10-50 and size of broadcasted message limited to 64Kb and Maximum number of user is limited by the size of broadcast message [5].
Application	1.Multicast networks such as machine-to-machine system embedded sensor network, cellular and wireless network, cable and satellite TV etc.
Method 6: Detection of lightweight Sybil attacks	
Property	1.This scheme use RSS [12] for the detection of Sybil identity and whitewash identity. 2. It detects Sybil nodes based on data or resource sharing among the nodes belongs to the network.
Advantages	1.It produce 90% successful detection of Sybil node [6] as Sybil in MANETs, assuming the maximum speed up of nodes is 10m/s. 2. It omits the use of any centralized third party and any extra hardware such as GPS [12].
Prevents from Attacks	1. Whitewash Sybil attack. 2.Simultaneous Sybil attack.
Downside	1. It fails to detect the Sybil nodes when nodes are moving at a speed higher than 10m/s [6]i.e. at low node density.
Application	1.Useful for detection of Sybil nodes in wireless MAC layer 802.11 protocol.
Method 7: Se Das (A Self-Destructing Data System)	
Property	1.This prototype based on T10 OSD [14] standard with active object base storage [13] techniques. 2.It uses Shamir algorithm [2] to generate the user distributing key and each key has a user specified validation time. 3.It erase sensitive information from public cloud server (HDD or SSD).
Advantages	1.After expiration of validation time of distributing key, sensitive and confidential information are automatically becomes unreadable [7] to obtain the data privacy.
Prevents from Attacks	1.Hopping attacks 2.Sybil data-harvesting attack [26]
Downside	1. Confidential data becomes permanently unreadable if the encryption key is lost. 2.It increases the average latency of the native system for uploading and downloading data by 59.06% and 25.69% respectively [7].
Application	1.T10 OSD based cloud server.
Method 8: ID-BASED anonyms user authentication scheme and cross-layer verification	
Property	1.It utilized ECDSA [15] with an ID based signature verification scheme[16] and utilizes MAC layer priorities and proxy signature primitives. 2.Each On Board Unit (OBU) incorporated GPS device for the detection of the current Geographical location of this OBU, used as the ID of the signing OBU [8].
Advantages	1.It eliminates the dependency on any third party trusted authority for certificate revocation. 2.cross-layer approach provides clarity in VANETs message verification. 3.It speeds up the message authentication on high speed VANET or in some critical situation [24].
Prevents from Attacks	1.False message attack 2.Trust-based attacks 3. OBU tempering 4.DoS Attack
Downside	1.As OBU authenticate the received message using its

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

	own ID there is a chance to expose the user identity. 2.Any messages send from the area outside the range of OBU is declined [8]. 3. During the error communication between OBU and GPS ,OBU is unable to create the ID.
Application	1.High speed traffic network with IEE 802.11 MAC layer protocol.
Method 9: Integrated high-precision magnetic probe with low noise amplifier	
Property	1. It incorporates three stages self-cascade LNA in 0.8µm CMOS to measure the magnetic field [9]. 2. Two coils of 100µm x 100µm and 500µm x 100µm are used to measure MS-line (Micro-strip-line). 3. It's on board FPGA is AES encrypted. It implements FIB technique [22] to eliminate the Si-substrate.
Advantages	1.Probe gain is near about-34dB. 2. Multistage self-cascade of LNA provides wide bandwidth and higher gain about 63dB [9]. 3. The performance of Coils enhances using FIB technique.
Prevents from Attacks	1.Side Chanel attack
Downside	1.By detailed measuring and monitoring data depended emission of magnetic near-field of chip related secret information can be exposed.
Application	1. Applicable for identifying and estimating side channel attack, for measurements of magnetic field leakage and useful in Semiconductor industries.

V. Conclusion

In order to increase the security and confidentiality of information there are various types of Symmetric Keying Algorithms proposed so far based on the traditional algorithm (AES, DES, 3DES, Blowfish) of cryptography. We make a basic comparison among some of those traditional algorithms and we came to know that Blowfish is highly proposed algorithm to make an analysis for the better algorithm. Symmetric key cryptography provides security in various fields such as Ad Hoc Networks, network protocols, mobile sensor networks etc. An ID based anonyms user authentication process provides better security than the Expedite Message Authentication Protocol though it incorporated a HAMC function to speed up the authentication process. Algorithms like ID-RDPC useful for company oriented cloud storage where as a self destructing data system Se- Das provides security by destructing the sensitive data after a certain period. Applications like Detection of lightweight Sybil attacks. It's very useful in wireless MAC layer 802.11 protocols. In the fields of architecture Symmetric key cryptography is also applicable to make an efficient and secure chip. NCL S-Box is efficient to resist the DPA attacks as well as CPA attacks. So in terms of security, authenticity and data integrity we may be confident enough that Symmetric Key Cryptography is an efficient class and efficient in software whereas AES is Efficient in both Software and Hardware as well as among the newly proposed method AES is one of the most popular methods of Cryptography.

References

[1] Behrouz A. Forouzan, Cryptography and Network Security, Special Indian Edition, TATA McGraw Hill.

[2] A.Shamir, "How to share a secret", *Commun.ACM*, Vol. 22, no. 11, pp. 612-613,1979.

[3] Albert Wasef, Xuemin (Sherman) Shen,"EMAP: Expedite Message Authentication Protocol For Vehicular Ad Hoc Networks", IEEE TRANSACTION ON MOBILE COMPUTING in *IEEE Explore*, Volume.12, No.1, January 2013.

[4] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, Lourdes Penalver, "A Secure Protocol For Spontaneous Wireless Ad Hoc Networks Creation", IEEE TRANSACTION ON PARALLEL AND DISTRIBUTIVE SYSTEMS in *IEEE Explore*, Volume.24, No.4, April 2013.

[5] Tomasz Rams, Piotr Pacyna, "A Survey of Group Key Distribution Schemes with Self-Healing Property", IEEE COMMUNICATION SURVEYS & TUTORIALS in *IEEE Explore*, Volume.15, No.2, Second Quarter 2013.

[6] Sohil Abbas, Madjid Merabti, David Llewellyn-Jones, Kashif kifayat, "Lightweight Sybil Attack Detection in Manets", IEEE SYSTEMS JOURNAL in *IEEE Explore*, Volume.7, No. 2, June 2013.

[7] Lingfang Zeng, Shibin Chen, Quingsong Wei, Dan Feng, "Se Das: A Self-Destructing Data System Based on Active Storage Framework", IEEE TRANSACTIONS ON MAGNETTICS in *IEEE Explore*, Volume.49, No.6, June 2013.

[8] Subir Biswas, Jelena Misic, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY *in IEEE Explore*, Volume. 62, No.5, June 2013.

[9] Nguyen Ngoc Mai-Khanh, Tetsuya Iizuka, Makoto Yamada, Osamu Morita, Kunihiro Asada, "An Integrated High-Precision probe System in 0.18 Mm CMOS for Near-Field Magnetic Measurements on Cryptographic LSIs", IEEE SENSORS JOURNAL in *IEEE Explore*, Volume. 13, No.7, July 2013

[10] E Surya, C. Diviya, "A Survey on Symmetric Key Encription Algorithm" International Journal of Computer Science & Communication Networks, Volume 2(4), 475-477

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

[11] D. N. Rewadkar, Smita Karve, “Spontaneous Wireless Ad Hoc Networking: A Review”, in *IJARCSSE*, Volume. 3, Issue 11, November.

[12] M.S.Bouassida, G.Guette, M. Shawky and B. Ducourthial, "Sybil node detection based on received signal strength variation within VANETs", *Int. J. Netw. Security,* vol. 8, pp. 322-333,May 2009.

[13] M. Mesnier, G. Ganger and E. Riedel, "Object Based Storage", *IEEE Commun. Mag.*, vol. 41, no. 8, pp. 84-90,August 2003.

[14] R. Weber, "Information Technology-SCSI Object-Based storage device commands (OSD)-2",Technical committee T10,INCITS std,Rev. 5 January 2009.

[15] D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom, Mississauga, ON, Canada, Tech. Rep. August 1999.

[16] C. Cocks,"An Identity based encryption scheme based on quadratic residues", in *Proc. IMA Int. Conf.*, Cirencester, U.K. , Dec. 2001, pp. 360-363.

[17] S.H. Jokhio, J.A. Jokhio, A.h. kemp, "Node Capture attack detection and defense in wireless sensor network", IET Wirl. Sens. Syst., 2012,Vol. 2, ISS. 3, pp. 161-169

[18] Po-Chun Liu, Hsie-Chia Chang and Chen-Yi Lee,"A true random-based differential power analysis countermeasure circuit for an aes engine", IEEE Transactions on circuits and systems-II:Express Briefs, vol. 59, n0. 2, February 2012.

[19] Jun Wu, Yiyu Shi and Minsu Choi, "Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box", IEEE Transactions on Instrumentation and Measurement in *IEEE Xplore,* vol. 61, No. 10, Oct. 2012.

[20] www.webopedia.com/TERM/S/symmetric_key_cryptography.ht ml

[21] en.wikipedia.org/wiki/Hash-based_message_authentication_code

[22] www.fibics.com/fib/tutorials/intoduction-focused-ion-beam-system/4/

[23] www.cs.tau.ac.il/~bchor/Shamir.html

[24] www.ijsrp.org/research-paper-0614/ijsrp-p3093.pdf

[25] en.wikipedia.org/wiki/Meet_in_the_middle_attack

[26] www.ijstr.org/final-print/feb2014/Self-Destructing-Data-System-Based-On-Session-Keys.pdf

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