A Study and Analysis on Symmetric Cryptography

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

Siddhartha Bhattacharyya
Department of Information Technology
RCC Institute of Information TechnologyKolkata, India
dr.siddhartha.bhattacharyya@gmail.com

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

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

***Abstract*— Technology is advancing day-to-day. For a better and faster technology, information security is a must. This requires data authentication at the execution levels. Cryptography is a useful tool through which secure data independency can be established. It uses two basic operations namely encryption and decryption for secure data communication. A large number of cryptographic techniques have been proposed and implemented so far. In this paper, we have surveyed some of the proposed mechanisms based on Symmetric Key Cryptography and have made a basic comparison study among them. The basic features, advantages, drawbacks and applications of various Symmetric Key Cryptography algorithms have been mentioned in this paper.**

Keywords*— *Cryptography;Symmetric key cryptography; Asymmetric key cryptography; Blowfish; Peer-to-Pee; Reed-Solomon codes; Public key certificate.

I. INTRODUCTION

Cryptography is the art of transforming a readable text (plain text) into an unreadable one (cipher text) which ensures data privacy. The word "crypto" mean "hidden" and "graphy" mean "to write". It is concerned with information security, data encryption, data authentication and access control. There are two types of cryptography- Symmetric Key (Secret Key) cryptography and Asymmetric Key (Public Key) cryptography. In this brief, we have discussed some of the proposed algorithms based on Symmetric Key cryptography. Symmetric Key Cryptography uses a common key (Secret key) for both encryption and decryption purposes. Thus, it is more effective to the Asymmetric Key counterpart. Various algorithms and mechanisms have been developed so far to implement Symmetric Key cryptography. We have discussed some of them in the coming sections.

Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai (Sponsors)

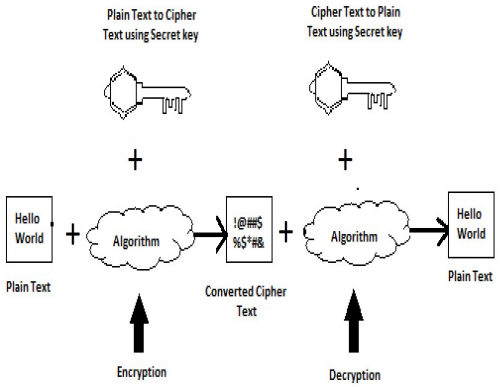

Fig.1. Symmetric Key Cryptography

II. GENERAL ALGORITHM FOR SYMMETRIC CRYPTOGRAPHY

There are various algorithms for symmetric key cryptography such as AES, DES, 3DES, RC4, Blowfish, etc. In this section, we have described these basic symmetric key algorithms.

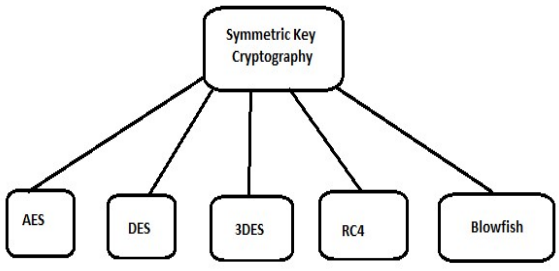

Fig.2. Classification of Symmetric Key Cryptography algorithms

978-1-4799-7613-3/14/$31.00

A. Advanced Encryption Standard(AES)

AES was started by NIST (National Institute of Standards and Technology) in January 1997. It is more robust than the DES algorithm and has a minimum block size of 128 bits for both encryption and decryption purposes. It first substitutes bytes, then shifts the rows, then mixes column and finally add the round key. It can secure both sensitive and unclassified materials.

B. Data Encryption Standard (DES)

This algorithm was developed by IBM in 1997 and operates on a block size of 64 bits. The encryption process is divided into 16 stages, consisting of eight S-Boxes. It shuffles the bits first, then proceeds with non linear substitutions and finally employs XOR operation to get the result.The sub key of a particular round is combined with the result using XOR operation. The decryption process involves reverse order of sub keys.

C. Triple Data Encryption Standard (3DES)

It is an enhanced form of DES algorithm. It is highly reliable and has an overall key length of 192 bits [76]. It first divides the key into three sub keys of 64-bits each. The remaining procedure is same as that of DES algorithm except that the process is repeated three times. The first key encrypts the data which is decrypted by the second key. The third key again encrypts the decrypted data. However, it is not much potential to protect the data for a longer period of time.

D. RC4 Algorithm

This algorithm was developed by Ronald Rivest. It requires successive exchange of state entries, based on key sequence. The key length is variable ranging from 1 to 256 bytes. It generates pseudo-random bytes to generate the stream, which is then XORed to convert the plain text into cipher text. The encryption technique is 10 times faster than the DES algorithm.

E. Blowfish Algorithm

It is the most efficient algorithm among all existing encryption algorithms. The key length is variable ranging from 32 bits to 448 bits. It has got a block size of 64 bits. The procedure consists of two basic steps. At first, key expansion is done. The P-array consists of 18 sub keys of 32-bit each. There are four 32-bit S-boxes which contains 256 entries each. Then the data encryption is done using XOR operations. It has a wide range of applications where the key not frequently changed. In 1993, Bruce Schneier designed Blowfish as an alternate encryption technique to others.

III. Survey Of Symmetric Cryptography

Karlheinz Hafner et al. [1] proposed a self-testing cryptographic chip to secure data over communication networks and hard disks. It provides autonomous data transfer and has various key management functions. The pilot chip was named as the Siemens Coprocessor Unit for rapid encipherment, or simply SICURE.The chip is divided into a collection of self-testable modules. The total fault coverage is obtained by taking the average fault coverage of the individual modules. It provides low hardware penalty with high fault coverage. A VLSI implementation of cryptography known as VINCI was presented by R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner [2].Unlike the self-testing chip, the VINCI implements both encryption and decryption techniques in a single hardware component. The cryptographic chip executes DES algorithm with a throughput of 20 Mbps or more, whereas VINCI has a throughput of more than 177 Mbps. So, it can be applied in high speed network protocols like FDDI or ATM.The processing speed of VINCI is higher than the data Encryption Algorithm (IDEA) developed by Lai and Massey[3][4].It incorporates an eight stage pipelining where each computation uses a hardware unit that operates in parallel. Unlike BIST, it helps in fault localization. It incorporates boundary scan schemes and self-testing through hardware redundancy, concurrent controller check, computation of invariant,etc.The self-testing scheme is further studied in details by H. Bonnenberg in 1993[5].In 1996,David Naccache and David MRaYhhi [6] surveyed the pre-existing crypto-dedicated microprocessors and proposed the possible evaluations of some microprocessors. The problem of inserting a chip into a card is removed by the smart cards. Hence, they provide better processing capacities, storage and portability. The executing programs are written in ROM which cannot be modified. This guarantees the control of the code. The quality of the cards along with public key cryptography provides solutions to many security problems. The card gathers all elements into a single chip to prevent illegal access. True Random Based Differential Power Analysis (DPA) Countermeasure circuit for an AES Engine had been proposed by Po-Chun Liu, Hsie-Chia Chang and Chen-Yi Lee [7].According to them, DPA attack is a big threat to the crypto chips as it can disclose the secret key efficiently without much effort. Several methods had been proposed earlier to resist these attacks but it increases the hardware cost and degrades the throughput. The proposed circuit has an area and power overhead of 6.2% and 18.5% respectively without any throughput degradation. Sami Rosenblatt et al. [80] presented a self-authenticated chip architecture to minimize the OEM database overhead using an intrinsic fingerprint of embedded DRAM. It provides a high level of hardware security. The protocol stores the location of each domain and offsets their respective FPS as secret keys. It uses simple superimpose and offset function to emulate high security encryption.

Gilles Brassard et al. [8] defined the privacy and correctness of unconditionally secure Oblivious Transfer [9]. They defined the notion of zigzag functions by deterministic and probabilistic polynomial-time algorithms both. It bridges

Oblivious Transfer and self-intersecting codes. It prevents any uncertainty or delay present in the channel [10]. They defined Oblivious Transfer to be a cryptographic protocol, a synchronous multiparty program that allows computations and transfer of messages by each party at each point in time. The protocol uses two issue verdicts "accept" or "reject" depending on the satisfactory conditions of the parties. When no party has any message to transfer or compute, the protocol terminates. In 2006, Jiangtao Li and Ninghui Li [11] proposed Oblivious Attribute Certificates (OACerts) which allows a certificate holder to select which attribute to use and how to use. They had also proposed a new cryptographic primitive known as Oblivious Commitment-Based Envelope (OCBE). An attribute value in OACerts can be used by running a protocol or by opening a commitment and then revealing the attribute value, etc. The security of OCBE protocols is based on Discrete Logarithmic Assumptions, Computational Diffie-Hellman Assumption and Random Oracle Method. The OBCE scheme must be oblivious, semantically secure and sound against receiver.

W. Susilo and R. Safavi-Naini [12] proved that a group-oriented encryption scheme is insecure and can be decrypted by two participants only. The method, in which each group member can decrypt an encrypted message, can publicly certify the public keys of the users. They proved that any two conspirators of the group can either break the system or discover the plain text.

Reto Kohlas and Ueli Maurer [13] made a step towards basing public-key infrastructures and public-key certification on strong theoretical key. They proposed certification of public keys that binds them with the entities. It captures the important aspect of public key certification and helps in authentication purposes better than the BAN logic [14]. Public-key revocation technique was proposed by Moni Naor and Kobbi Nissim [15] to overcome the short comings of the calculus approach [13]. The revocation lists are represented by authenticated dictionaries, supported by efficient updates and verification of certificate in the list. It also provides solution for unrevoked certificates which are frequently issued for short periods. These suggested solutions are compatible with various certificates and are better in terms of update rate, robustness and communication costs.Z.Shao [16] used self-certified public key to propose new cryptographic systems based on discrete logarithms. If an attacker supplies incorrect but valid public key then an encrypted message can be easily decrypted by the imposter. To deal with this problem, it is necessary to implement a self-certified public-key [17]. The system requires less computing time. However, a public-key digital certificate is not itself secure to authenticate user.

This idea was given by Lein Harn and Jian Ren [18]. They proposed the concept of GDC (Generalized Digital Certificate) to provide key agreement and user authentication. They proposed both Integer Factoring (IF)-based and Discrete Logarithm (DL)-based protocols to achieve secret key establishment and authentication. Jikai Teng and Chuankun [19] presented a security model for Certificateless Group Key Agreement protocol and proposed a constant round protocol of the same based on CL-PKC (Certificateless Public Key Cryptography) .It increases the efficiency without involving any signature scheme. It provides better AKE security and can tolerate up to n-2 attackers for weak MA-security. Jan Camenisch et al. [20] proposed the need of Private Credentials in Electronic Identities. It does not involve issuers during authentication. Users can disclose their required attributes without being tracked across their transactions. Various non linking public keys can be generated from a single secret key. This secures E-commerce [21] and various online transactions. However, the public key revocation technique is limited.Carlos Gañán et al. developed an accurate model for revocation by analysing the empirical data from actual Certificate Authorities (CAs). The model is based on ARFIMA (Autoregressive Fractionally Integrated moving Average) process. It can be used as synthetic revocation generator.

Jana Dittmann et al. [22] introduced ways to secure multimedia through cryptographic mechanisms and digital watermarking. The various fields on which it works are confidentiality, data origin authenticity, data integrity entity authenticity and nonrepudiation. Security solutions through E-commerce [21] are necessary to provide access mechanisms to prevent theft and misuse. Cryptographic mechanisms are based on cryptosystems, consisting of a set of keys and sets on which functions operate. The communicating entities in a private key cryptosystem, share a secret keys whereas Trapdoor one-way functions implement public-key cryptosystems. The digital watermarking technique is based on steganographic systems that embed information directly into media data. They also suggests that revocation of certificates is to be done for algorithm compromise, change of key usage, defect or loss of security token, change of security policy, etc. Huijuan Yang and Alex C. Kot [23] proposed a two-layer binary data hiding scheme for authentication and identification of tempering locations respectively. According to this proposal, an image is divided into multiple macro-blocks (MBs) that are classified into eight categories. The flippability of pixel is determined by the connectivity preserving transition criterion. The proposed technique, with embedded Block Identifier (BI), is effective in detecting possible tampering in watermarked image, both in qualified as well as unqualified MBs. In December 2007, Y. -K. Huang et al. [24] proposed an OCDM transmission using both cryptographic and steganographic methods to achieve both data isolation and security. Separate codes for cryptographic code swapping and key distribution had been used. The two data hiding schemes are wrapped so as to avoid cracking of schemes if an imposter knows nothing about the OCDMA codes.

Srdjan Capkun et al. [25] proposed a self-organised management system of public-key that allows the users to use their public and private keys to issue certificates so as to perform authentication without any network partitions. This approach does not rely on system initialization state or any trusted authority. This secures the mobile ad hoc networks as it is applied to open networks which do not require any

centralized control. The users themselves create the private and public keys and chains of public key certificates perform key authentication purposes. They enabled both explicit and implicit certificate revocation mechanisms. Key authentication is possible even if the network is partitioned. In January, 2006, Srdjan Capkun et al. [26] showed that mobility helps in peer-to-peer security. They had shown how mobility can provide security to ad hoc networks by exchanging required cryptographic materials and removes the previous beliefs of difficulties in security [27]. It secures the network through key establishment and authentication, based on two scenarios. The first scenario considers mobile nodes, controlled by central authority and the second scenario considers mobile nodes where each represents a user with its own mobile device. This method can be applied in self-organized networks and networks with offline authority. It works both with symmetric cryptography and with public key and provides related protocols. They applied both public key approach and symmetric key approach to both self-organized and authority control network. A self-organized network layer, called SCAN, was proposed by Hao Yang, James Shu, Xiaoqiao Meng and Songwu Lu [28] to secure mobile ad hoc networks. It protects the forwarding operations in unified framework as well as routing. They exemplified the idea in context of AODV routing protocol. To control SCAN overload, they determined the token lifetime of each node. The design is fully localized, distributed and self-organized. The SCAN executes functions like collaborate monitoring, token renewal and revocation. The detection accuracy of SCAN is sensitive to channel error, parameters in detection algorithm, mobility, etc.

Albert Wasef and Xuemin (Sherman) Shen [78] introduced an Expedite Message Authentication Protocol (EMAP) through an efficient revocation checking process thus replacing the time consuming CRL checking process. It uses a highly secure, fast HMAC function. The protocol is based on bilinear pairing, hash chains and searching algorithms like linear and binary search. Finally a hash function is used to map all possible certificates. The protocol provides high security against forging attacks, Replay attacks, Forward secrecy and Colluding attacks. It has a computational complexity of O (1). Raquel Lacuesta et al. [79] presented a Secure Protocol for Spontaneous Wireless Ad Hoc networks. They applied both asymmetric cryptography and symmetric cryptography for device identification and session keys exchange respectively. The routing protocol determines the fault tolerance of the network. Periodic authentication of user certificate is necessary otherwise the device might be blocked. They implemented Java programming for the development of the protocol. It is a self-configured protocol without any external support.

Lingfang Zeng et al. [81] presented a Self-Destructing Data System to protect data in the Cloud. It ensures data privacy by integrating cryptographic techniques with an active storage framework. The system consists of a metadata server, an application node and a storage node. It decreases the throughput for uploading and downloading by less than 72% and increases the latency by less than 60%. Huaqun Wang et al. [82] presented an Identity-based Remote data possession checking in Public clouds. The protocol consists of a private key generator, a client and a cloud server. The communication and computation overheads of the protocol are very less, with an additional advantage of certificate management and verification.

Prabir Kr. Naskar et al [83] presented a symmetric key encryption algorithm based on linear geometry. 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. Correlation value for both secret and encrypted image is one.

Ankita Baheti et al [84] proposed a symmetric key encryption algorithm based on cyclic elliptic curve, chaotic system and provides authentication using neural networks. It performs the encryption with eight 32-bit registers. Based on piecewise non-linear chaotic map, the method generates pseudorandom bit sequences for various round keys. The method incorporates large key space, faster, good encryption effect and sensitive to small changes.

Wafa Elmannai et al [85] proposed a secure protocol using the property of Quantum Wave Function. 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. It prevents attack on user's password using quantum computing efficiency. It prevents compromising passwords and can replace the drawback of classical encryption algorithms.

IV. Comparison Study

TABLE I. Comparison Table For Different Symmetric Key Cryptography Algorithm

Method-I	
Introduction of chips/cards and their authentication processes	
Features	It provides autonomous data transfer and has various key management functions. The DPA Countermeasure circuit and low power SCA resistant Asynchronous S-Box design prevents the DPA attacks.
Advantages	The chip provides low hardware penalty with high fault coverage and provides a throughput of more than 177 Mbps.
Downsides	The set up design is slightly complex and increases the time complexity [2].
Applications	Commercial data storage and communications like hard disks, high speed network protocols like FDDI or ATM, national administrations.
Method-II	

Oblivious Transfer (OT) and Oblivious Attribute Certificates (OACerts)	
Features	OT is a cryptographic protocol, a synchronous multiparty program that allows computations and transfer of messages by each party at each point in time. OACerts allows a certificate holder to select which attribute to use holder to select which attribute to use and how to use.
Advantages	OT prevents any uncertainty or delay present in the channel [10]. OACerts allows oblivious access control and is highly efficient and secure.
Downsides	OACerts cannot secure anonymous communication channels. Credential distribution and revocation technique handling are not clear.
Applications	Exchanging secrets, coin flipping by the telephone, and sending certified mail.
Method-III	
Public Key Certification and Revocation	
Features	It provides various techniques for checking the validation of public keys based on calculus method, discrete logarithms, integer factoring, etc. The revocation techniques provide solution for unrevoked certificates which are frequently issued for short periods.
Advantages	It helps in authentication purposes better than the BAN logic [14]. The system requires
Downsides	The encryption techniques are based on complex mathematics and increase the computation overheads.
Applications	It helps in reasoning and formalizing in digital economy. It is used in smart cards and mobile phones, etc.
Method-IV	
Watermarking Scheme and Image Authentication	
Features	The digital watermarking technique is based on steganographic systems that embed information directly into media data. The two data hiding schemes are wrapped so as to avoid cracking of schemes if an imposter knows nothing about the OCDMA codes.
Advantages	The Binary Image Authentication scheme is effective in detecting possible tampering in watermarked image, both in qualified as well as unqualified MBs. Watermarking provides an efficient topology for data-origin authenticity and integrity. It ensures security, impartibility, robustness, transparency, and confidentiality.
Downsides	The cryptographic mechanism works with one bit of input. Hence, if the bit changes, the system may fail. Miss detection of tampering is likely to occur to those MBs that do not contain enough flappable pixels.
Applications	Digital imagery, 3D models, audio, certificates, engineering drawings, legal documents, digital books, etc.

Method-V	
Protection of data in the cloud	
Features	The system consists of a metadata server, an application node and a storage node. The Identity-based Remote data possession checking in Public clouds consists of a private key generator, a client and a cloud server.
Advantages	The communication and computation overheads of the protocol are very less, with an additional advantage of certificate management and verification.
Downsides	The process is slight lengthy.
Applications	Mobile internet, cloud computing, etc.
Method-VI	
Symmetric key encryption algorithm based on linear geometry	
Features	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.
Downsides	----------
Applications	Medical, commercial and military systems.
Method-VII	
Symmetric key encryption algorithm based on cyclic elliptic curve and chaotic system	
Features	It provides authentication using neural networks. It performs the encryption with eight 32-bit registers. Based on piecewise non-linear chaotic map, the method generates pseudorandom bit sequences for various round keys.
Advantages	Large key space, faster, good encryption effect and sensitive to small changes.
Downsides	If the change in media data is quite smaller than the adjustable parameter ranging, then the algorithm fails.
Applications	Various business requirements.
Method-VIII	
Secure protocol using the property of Quantum Wave Function	
Features	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.
Downsides	----------
Applications	Various hardware implementations.

V. Future Scope On Symmetric Cryptography

Various mechanisms had been proposed so far, based on symmetric key cryptography. They ensure excellent data security. But there are certain areas that remained open. Strong revocation techniques for Oblivious Attribute Certificates need to be developed. In case of Peer-to-Peer Security, the data recovery should be fast and it should handle large number of computers. SOA can be applicable for high data transfer. Self-certification of public key helps in data security but it requires large storage. So, methods can be developed to reduce the storage and time requirements simultaneously. Digital watermarking has various parameters like robustness, transparency, security, capacity, complexity, etc. But we

cannot achieve them simultaneously. Depending on this condition, an appropriate algorithm can be developed. It can be analyzed, how a large message can be embed, retaining its robustness. Better cryptographic methods improve the system performance and operate efficiently in different scenarios.

VI. Conclusion

Cryptography plays a vital role in ensuring data security through various aspects like authentication, confidentiality, non-repudiation, data integrity, etc. In this paper, we have analyzed various symmetric cryptographic mechanisms developed so far. These encryption and decryption techniques depend upon the type of data and the channel through which the data is being communicated. We have drawn a comparison analysis of the proposed mechanisms based on their basic features, advantages, drawbacks and applications. Among those, the digital watermarking scheme and public key certification and revocations are found to be highly efficient. The watermarking scheme is based on Steganographic systems, where the information is directly embed into media data. The public key certification and revocation techniques ensure the validation of public keys, which is essential for data privacy. They both render robustness, transparency, security, imperceptibility, possibility of verification, flexibility and efficiency.

References

[1] Karlheinz Hafner,Hartmut C. Ritter,Thomas M. Schwair,Stefan Wallstab,Michael Deppermann,Iuergen Gessner,Stefan Koesters,Wolf-Dietrich Moeller,Gerd Sandweg,"Design and Test of an Integrated Crypto chip", IEEE Design & Test Of Computers, December 1991 , pp.6-17 , IEEE.

[2] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner," A 177 Mb/s VLSI Implementation of the International Data Encryption Algorithm"IEEE JOURNAL OF SOLID-STATE CIRCUITS, March 1994,vol.29, no.3,pp.303-307,IEEE.

[3] X. Lai, J. L. Massey, "A proposal for a new block encryption standard", in Advances in Cryptology-EUROCRYPT' 90. Berlin, Germany: Springer-Verlag, 1990, pp. 389-404.

[4] X. Lai, J.L. Massey, and **S.** Murphy, "Markov ciphers and differential cryptanalysis," in Advances in Cryptology-EUROCRYPT*'91.* Berlin, Germany: Springer-Verlag, 1991, pp. 8-13.

[5] H. Bonnenberg, "Secure testing of VLSI cryptographic equipment,"Ph.D. dissertation, ETH Zurich, Switzerland, 1993.

[6] David Naccache, David MRaYhhi,"CRYPTOGRAPHIC SMART CARDS", IEEE Micro, June 1996, pp. 14-24, IEEE

[7] Po-Chun Liu, Hsie-Chia Chang, Chen-Yi Lee, "A True Random-Based Differential Power Analysis

[8] Countermeasure Circuit for an AES Engine", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, February 2012,Vol. 59,No. 2.pp.103-107,IEEE

[9] Gilles Brassard, Claude Crepeau, and Miklos Santha," Oblivious Transfers and Intersecting Codes", IEEE TRANSACTIONS ON INFORMATION THEORY, November 1996,Vol. 42,No. 6,pp. 1769-1780

[10] dm.ing.unibs.it/giuzzi/corsi/Support/papers-cryptography/187.pdf

[11] www.uclouvain.be/.../publications.pdf.abff2911710bcf40.4f542d6469736f726465722e706466.pdf

[12] Jiangtao Li, Ninghui Li," OACerts: Oblivious Attribute Certificates", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, October-December, 2006, Vol.3, No.4, pp.340-352, IEEE

[13] W. Susilo, R. Safavi-Naini," Remark on self-certified group-oriented cryptosystem without combiner", ELECTRONICS LETTERS, September 1999,Vol.35,No.18,pp.1539-1540,IEEE

[14] Reto Kohlas, Ueli Maurer,"Reasoning About Public-Key Certification: On Bindings between Entities and Public Keys", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, April 2000, Vol.18,No.4,pp.551-560,IEEE

[15] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication,"ACM Trans. ComputerSyst., vol. 8, no. 1, pp. 18–36, 1990.

[16] Moni Naor, Kobbi Nissim,"Certificate Revocation and Certificate Update", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, April 2000, Vol.18,No.4,pp.561-570,IEEE

[17] Z.Shao,"Cryptographic systems using a self-certified public key based on discrete logarithms", IEE Proc.-Comput. Digit. Tech., November 2001,Vol.148,No.6, pp.233-237,IEEE

[18] KOHNFELDER, L.M.: 'A method for certificate'. MIT Lab. For Computer Science, Cambridge, Mass. (May, 1978)

[19] Lein Harn, Jian Ren," Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, July 2011,Vol.10,No.7,pp.2372-2379,IEEE

[20] Jikai Teng, Chuankun Wu,"A Provable Authenticated Certificateless Group Key Agreement with Constant Rounds", JOURNAL OF COMMUNICATIONS AND NETWORKS, February 2012, Vol.14, No.1, pp.104-110, IEEE

[21] Jan Camenisch, Anja Lehmann, Gregory Neven," Electronic Identities Need Private Credentials", IEEE Security & Privacy, January/February 2012, pp.80-83, IEEE

[22] Andrew Meye, Peter Taylor," E-commerce-an Introduction", COMPUTING & CONTROL ENGINEERING JOURNAL, June 2000,IEEE

[23] Jana Dittmann, Petra Wohlmacher, Klara Nahrstedt,"Multimedia and Security Using

[24] Cryptographic and Watermarking Algorithms", IEEE MultiMedia, October–December 2001, pp.54-65,IEEE

[25] Huijuan Yang, Alex C. Kot," Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature and Block Identifier", IEEE SIGNAL PROCESSING LETTERS, December 2006, Vol.13, No.12, pp.741-744, IEEE

[26] Y.-K. Huang, B. Wu, I. Glesk, E.E. Narimanov, T.Wang, P.R. Prucnal,"Combining cryptographic and

[27] steganographic security with self-wrapped optical code division multiplexing techniques", ELECTRONICS LETTERS, December 2007, Vol.43, No.25, IEEE

[28] Srdjan Capkun, Levente Buttya´n, Jean-Pierre Hubaux,"Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, January-March 2003, Vol.2, No.1, pp.52-64, IEEE

[29] Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttya´n,"Mobility Helps Peer-to-Peer Security", IEEE TRANSACTIONS ON MOBILE COMPUTING, January 2006, Vol.5, No.1, pp.43-51, IEEE

[30] dl.acm.org/citation.cfm?id=778422

[31] Hao Yang, James Shu, Xiaoqiao Meng, Songwu Lu,"SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, February 2006, Vol.24, No.2, pp.261-273, IEEE

[32] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing," in *Proc. IEEE WMCSA*, 1999, pp. 90–100.

[33] Wenbo He, Ying Huang, Ravishankar Sathyam, Klara Nahrstedt, Whay C. Lee," SMOCK: A Scalable Method of Cryptographic Key Management for Mission-Critical Wireless Ad-Hoc Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, March 2009, Vol.4, No.1, pp.140-150, IEEE

[34] Kevin R.B. Butler, Sunam Ryu, Patrick Traynor, Patrick D. McDaniel,"Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, December 2009, Vol.20, No.12, pp.1803-1815, IEEE courses.cs.washington.edu/courses/csep590/06wi/finalprojects/youngblood_csep590tu_final_paper.pdf

[35] M. -H. Guo, H.-T. Liaw, D. -J. Deng, H. -C. Chao," Cluster-based secure communication mechanism in wireless ad hoc networks", IET Inf. Secur., January 2010, Vol.4, Iss.4, pp.352-360, IEEE

[36] Prashant Dewan, Partha Dasgupta," P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, July 2010, Vol.22, No.7, pp.1000-1013, IEEE

[37] MICHELE NOGUEIRA, ALDRI SANTOS, LUIZ CARLOS P. ALBINI," SURVIVABLE KEY MANAGEMENT ON WANETS", IEEE Wireless Communications, December 2011, pp.82-88, IEEE

[38] Xixiang Lv, Hui Li," Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks", IET Inf. Secur., April 2012, Vol.7, Iss.2, pp.61-66, IEEE

[39] Lo-Yao Yeh, Yu-Lun Huang, Anthony D. Joseph, Shiuhpyng Winston Shieh, Woei-Jiunn Tsaur," A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, May 2012, Vol.61, No.4, pp.1907-1924, IEEE

[40] Jun Li, Peter L. Reiher, Gerald J. Popek, "Resilient Self-Organizing Overlay Networks for Security Update Delivery", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, January 2004, Vol.22, No.1, pp.189-202, IEEE

[41] Xiaojian Tian, Duncan S. Wong, Robert W. Zhu,"Analysis and Improvement of an Authenticated Key Exchange Protocol for Sensor Networks", IEEE COMMUNICATIONS LETTERS, November 2005,Vol.9, No.11, pp.970-972, IEEE

[42] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks,"in Proc. of the Second ACM International Conference on Wireless Sensor Networks and Applications. ACM Press, 2003, pp. 141–150.

[43] Mohamad Badra, Ibrahim Hajjeh,"Key-Exchange Authentication Using Shared Secrets", IEEE Computer Society, March 2006, pp.58-66, IEEE

[44] S.H. Jokhio, I.A. Jokhio, A.H. Kemp," Node capture attack detection and defence in wireless sensor networks", IET Wirel. Sens. Syst., August 201, Vol.2, Iss.3, pp.161-169, IEEE

[45] Majid Khabbazian, T. Aaron Gulliver, Vijay K. Bhargava," Double Point Compression with Applications to Speeding Up Random Point Multiplication", IEEE TRANSACTIONS ON COMPUTERS, March 2007, Vol.56, No.3, pp.305-313, IEEE

[46] [44]C. Pedraza, J. Castillo, J.I. Martı´nez, P. Huerta, C.S. de La Lama," Self-reconfigurable secure file system for embedded Linux", IET Comput. Digit. Tech, January 2008, Vol.2, No.6, pp.461-470, IEEE

[47] Youngho Jeong, Soonchoul Kim, Heejeong Kim, Han-Seung Koo, Eunjung Kwon, "A Novel Protocol for Downloadable CAS", IEEE Transactions on Consumer Electronics, August 2008, Vol.54, No.3, pp.1236-1243, IEEE

[48] Yang Zhang, Jun-Liang Chen," A Delegation Solution for Universal Identity Management in SOA", IEEE TRANSACTIONS ON SERVICES COMPUTING, January-March 2011, Vol.4, No.1, pp.70-81, IEEE

[49] Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, Carles Padró," On Codes, Matroids, and Secure Multiparty Computation From Linear Secret-Sharing Schemes", IEEE TRANSACTIONS ON INFORMATION THEORY, June 2008, Vol.54, No.6, pp.2644-2657, IEEE

[50] Aggelos Kiayias, Moti Yung," Cryptographic Hardness Based on the Decoding of Reed–Solomon Codes", IEEE TRANSACTIONS ON INFORMATION THEORY, June 2008, Vol.54, No.6, pp.2752-2769, IEEE

[51] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields.Journal of the Society for Industrial and Applied Mathematics, 8:300–304, 1960.

[52] C. W. Chiou, W. -Y. Liang, H. W. Chang, J. -M. Lin, C. -Y. Lee," Concurrent error detection in semi-systolic dual basis multiplier over GF(2m) using self-checking alternating logic", IET Circuits Devices Syst., February 2010, Vol.4, Iss.5, pp.382-391, IEEE

[53] MACWILLIAMS F.J., SLOANE N.J.A.: 'The theory of error-correcting codes' (North-Holland, Amsterdam, 1977)

[54] LIDL R., NIEDERREITER H.: 'Introduction to finite fields and their applications' (Cambridge University Press, New York, 1994)

[55] M. H¨olbl and T. Welzer, "Two improved two-party identity-based authenticated key agreement protocols," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1056–1060, 2009.

[56] Kyung-Ah Shim," Cryptanalysis of Two Identity-Based Authenticated Key Agreement Protocols", IEEE COMMUNICATIONS LETTERS, April 2012, Vol.16, No.4, pp.554-556, IEEE

[57] Chang-An Zhao, Fangguo Zhang, Dongqing Xie," Faster Computation of Self-Pairings", IEEE TRANSACTIONS ON INFORMATION THEORY, May 2012, Vol.58, No.5, pp.3266-3272, IEEE

[58] Claude Carlet, Philippe Gaborit, Jon-Lark Kim, Patrick Solé," A New Class of Codes for Boolean Masking of Cryptographic Computations", IEEE TRANSACTIONS ON INFORMATION THEORY, September 2012, Vol.58, No.9, pp.6000-6011, IEEE

[59] Jun Wu, Yiyu Shi, Minsu Choi," Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, October 2012, Vol.61, No.10, pp.2765-2775, IEEE

[60] link.springer.com/chapter/10.1007%2F3-540-57332-1_26 smallbusiness.chron.com/disadvantages-public-key-encryption-68149.html

[61] www.ntu.edu.sg/home/eackot/softcopy%20paper/Yang-Kot%20Pattern-Based%20Data%20Hiding%20for%20Binary%20Images%20By%20Connectivity-Preserving_TMM_2007_03.pdf

[62] www.ianswer4u.com/2011/05/peer-to-peer-network-p2p-advantages-and.html#axzz3630uSrVX

[63] sites.google.com/site/computernetworksassignment1/advantages-and-disadvantages-to-peer-to-peer-and-client-server-networks

[64] www.dmst.aueb.gr/dds/pubs/jrnl/2004-CompSec-p2pav/html/VAS04.html

[65] www.birs.ca/workshops/2009/09w5103/report09w5103.pdf

[66] www.usna.edu/Users/math/wdj/_files/documents/reed-sol.htm

[67] www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html

[68] www.exforsys.com/tutorials/soa/soa-disadvantages.html

[69] www.ehow.com/facts_7261271_disadvantages-service-oriented-architecture.html

[70] www.yash.com/service-oriented-architecture/soa-service-oriented-architecture-applications.php

[71] searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[72] www.webopedia.com/TERM/A/AES.html

[73] www.ijcscn.com/Documents/Volumes/vol2issue4/ijcscn2012020405.pdf

[74] www.iusmentis.com/technology/encryption/des/

[75] pocketbrief.net/related/BlowfishEncryption.pdf

[76] www.vocal.com/cryptography/rc4-encryption-algoritm/

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

[78] Carlos Gañán, Jorge Mata-Díaz, Jose L. Muñoz, Juan Hernández-Serrano, Oscar Esparza, Juanjo Alins," A Modeling of Certificate Revocation and Its Application to Synthesis of Revocation Traces", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, December 2012, Vol.7, No.6, pp.1673-1686, IEEE

[79] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", *IEEE*

TRANSACTIONS ON MOBILE COMPUTING, January 2013, Vol. 12, No. 1, pp. 78-89, IEEE

[80] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, April 2013, Vol. 24, No. 4, pp. 629-641, IEEE

[81] Sami Rosenblatt, Srivatsan Chellappa, Alberto Cestero, Norman Robson, Toshiaki Kirihata and Subramanian S. Iyer, "A Self-Authenticating Chip Architecture Using an Intrinsic Fingerprint of Embedded DRAM", *IEEE JOURNAL OF SOLID-STATE CIRCUITS*, November 2013, Vol. 48, No. 11, pp. 2934-2943, IEEE

[82] Lingfang Zeng, Shibin Chen, Qingsong Wei, and Dan Feng, "Se-Das: A Self-Destructing Data System Based on Active Storage Framework", *IEEE TRANSACTIONS ON MAGNETICS*, June 2013, Vol. 49, No. 6, pp. 2548-2554, IEEE

[83] Huaqun Wang, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, "Identity-based remote data possession checking in public clouds", *IET Inf. Secur.*, 2014, Vol. 8, Iss. 2, pp. 114-121, IEEE