An Extensive Survey on Anti Collision Enhancements using Encryption Techniques

Sourabh N. Prasad[1] , Prof. Sanjit Kumar[2]

[1]*M.tech Scholor,* [2]*Reseach guide*

National Institute of Technical Teacher Training and Research, Bhopal

Abstract-These days with an ever increasing number of innovative progressions in the field of communication there is significantly more consistently expanding danger to information which is being uncovered in the earth of cryptographic assaults. With greater progression in web applications there is a considerable measure of basic information which is shared by the client and that must be shielded from unlawful use by the programmers. As the development of innovation, communication through web and remote techniques has turned into a progressive headway recently. The advanced Encryption Standard (AES) are a standout amongst the most critical calculations utilized in symmetric key cryptography In this Study, different finalist applicants of AES algorithms have been dissected, commenting its fundamental points of interest and restrictions, memory utilization of various algorithms and furthermore the determination criteria of AES finalist algorithms assessed on different assessment criteria.

Keyword-AES, SHA-1, hash Functions, labview.

I. INTRODUCTION

In this developing 21st Century, computer has become the important channel for people to communicate each other, by sending, receiving, writing, editing, uploading and downloading through web. However, the security issue may arise with this internet communication. They may worry whether the files and data will be sent in a secure way or not? Thus, it has to be the compulsory which all the files and data sent through the web need to be secured and protected because everybody is concerned about the sensitive data to the web and most organizations believe that web is not as safe as their own data centres. Imagine that how much it data or information might be worth going? So others more professional person was already knew this kind of problem will be bringing in web so they had investigative kind of encryption algorithm to solve this problem.

Cryptographic hash functions, processing a little settled size hash an incentive for a given message of discretionary length, are a significant cryptographic crude that are utilized to anchor incalculable frameworks and applications. A key cryptographic prerequisite is that it ought to be computationally infeasible to discover impacts: two unmistakable messages with a similar hash esteem. Industry's past true decisions MD5 and SHA-1 are both in view of the Merkle-Damgard development that emphasizes a pressure function that updates a settled size inner state called the chinning value (CV) with settled size bits of the info message.

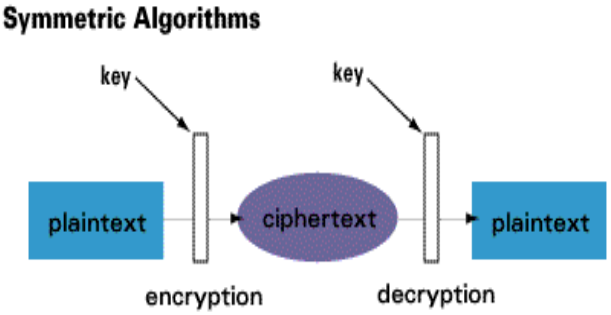

Fig. 1.1 Symmetrical algorithm encryption and decryption process.

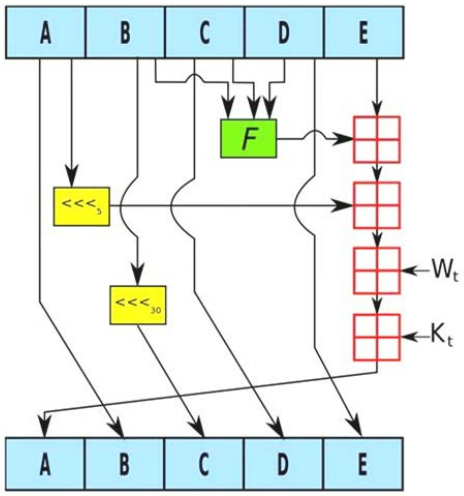

Fig. 1.2 Basic Structure Design of SHA-1

SHA-1, composed by NSA and institutionalized by NIST, is likewise feeble and was hypothetically broken in 2005 with a crash assault with an expected complex¬ity of 269 SHA-1 calls exhibited by Wang et al. With genuine crashes for full SHA-1 distant up until this point, there have been endeavors at delivering impacts for re¬duced adaptations of SHA-1: 64 stages , 70 stages , 73 stages, the last being 75 stages from 2011. The cost of impacts for SHA-1 was enhanced to 261 SHA-1 calls at

EUROCRYPT 2013, together with a close crash assault with cost 257'5 and a picked prefix crash assault with cost 277'1 SHA-1 calls, that remaining parts the present best in class. Other ongoing endeavors concentrated on discovering free start impacts for SHA-1, i.e., crashes for its pressure function, with a 76-step free start crash and all the more as of late a frees tart impact for full SHA-1

SHA-1 is a cryptographic hash function that was composed by the National Security Agency (NSA) and distributed in 1995 [SHA, 1995] as a follow-up to its defective ancestor SHA-0 from 1993. It has a settled hash size of 160 bits and depends on the Merkle-Damgard development. The Merkle-Damgard development is an approach to build a crash safe hash function of self-assertive information estimate from an impact safe pressure function with a settled info measure.

SHA-1 has a pressure function that takes a 160-piece hash esteem and a 512-piece some portion of the message and yields another 160-piece hash esteem. The principal hash esteem is known as the initialisation vector and is a consistent. The last hash esteem is utilized as the last yield of the hash function.

Hash Functions

A hash function is a scientific function that takes a message of self-assertive length as information and produces a yield of settled (littler) length, which is regularly called a unique mark or message process. They are crucial segments of numerous cryptographic applications, for example, computerized marks, secret phrase insurance, message confirmation, irregular number age, etc.A hash function is a numerical function that takes a message of self-assertive length as information and produces a yield of settled (littler) length, which is regularly called as unique mark or message process, see Fig. 1.2. All the more formally, it very well may be characterized as:

Definition . A hash function H : D ^ R is a function that maps variable-length input bit strings M G {0,1}* to settled length yield bit strings H(M) G {0, 1}" for a positive whole number n.Since |D| > |R|, this function is constantly many-to-one. Therefore, there are dependably somewhere around two messages that have a similar unique mark, which is known as an impact.

Despite the fact that it isn't conceivable to maintain a strategic distance from impacts, discovering them effortlessly can be dodged if each yield esteem is seen around similarly likely. For a cryptographic hash function H, it is normal that it ought not be computationally attainable to discover crashes.

Hash functions are principal segments of numerous cryptographic applications. In computerized marks, the marking algorithm is connected to the hash an incentive rather than the message expanding the execution (by handling less information) and security (by recognizing fraud/altering). Without question the security of the plan relies upon the security of the hash function: if the assailant can create two messages with a similar hash, and persuade a gathering to sign one of them, at that point he will have a substantial mark for the other message.

II. THE ADVANCED ENCRYPTION STANDARD (AES)

AES is a square figure with a square length of 128 bits. It takes into account three diverse key lengths: 128, 192, or 256 bits. AES Encryption comprises of 10 rounds of preparing for 128-piece keys, 12 rounds for 192-piece keys, and 14 rounds for 256-piece keys. With the exception of the last round for each situation, every single other round are indistinguishable. Each round of handling incorporates one single-byte based substitution step, a line savvy stage step, a segment shrewd blending step, and the expansion of the round key. The request in which these four stages are executed is distinctive for encryption and Decryption.

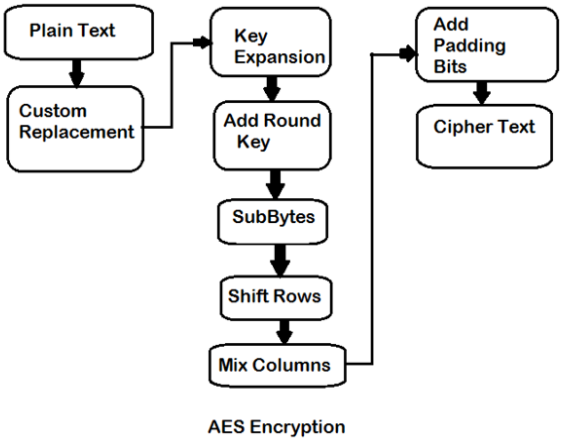

Fig. 2.1 Flow chart of AES encryption.

Therefore, the initial four bytes of a 128-piece input square involve the first* section in the 4 framework of bytes. The following four bytes involve the second section, et cetera. The*4 4 lattice of bytes is alluded to as the state exhibit. Each round of handling takes a shot at the information state cluster and creates a yield state exhibit. The yield state cluster delivered by the last round is revamped into a 128-piece yield square. Not at all like DES, the decoding algorithm contrasts significantly from the encryption algorithm. Albeit, by and large, similar advances are utilized in encryption and decoding, the request in which the means are done is unique. While AES requires the square size to be 128 bits, the first Rijndael figure works with any square size (and any key size) that is a various of 32 as long as it surpasses 128. The state exhibit for the

distinctive square sizes still has just four columns in the Rijndael figure. Notwithstanding, the quantity of segments relies upon size of the square. For instance, when the square size is 192, the Rijndael figure requires a state cluster to comprise of 4 lines and 6 culumns.

AES utilizes a substitution-change arrange in a more broad sense. Each round of preparing in AES includes byte-level substitutions taken after by word-level stages. The idea of substitutions and stages in AES considers a quick programming execution of the algorithm.

As far as security no assault has been found for AES, utilizing the full number of rounds, which is more productive than 296 for AES-192. Of particular note in this setting is the way that AES, because of a vast torrential slide impact, is viewed as invulnerable to related content assaults. The torrential slide impact in this setting alluding to the property that a little contrasts in-put prompts huge contrasts in the yield. Anyway some side-channel assaults, assaults on usage that hole data somehow, has been found for a few executions of AES, however the greater part of them have been immediately fixed when the assault wound up known.

III. LITERATURE SURVEY

Sr. no.	Author	Title	Year	Methodology
1	Anti-collision enhancement of a SHA-1 digest using AES encryption by LABVIEW	R. K. Ibraheem, R. A. J. Kadhim and A. S. H. Alkhalid	2015	A series of latest papers have pretended collision attacks on publicly used hash functions, including the widely published SHA-1 algorithm.
2	An EPC class-1 generation-2 anti-collision protocol for RFID tag identification in augmented systems	L. Sanchez and V. Ramos	2015	n this paper, authors review an augmented RFID system to evaluate its performance and study its advantages and limitations.
3	Simplified computation in memoryless anti-collision RFID identification protocols	H. Landaluce, A. Perallos, L. Bengtsson and I. J. G. Zuazola	2014	A memoryless-based Collision window Tree plus (CwT+) protocol for simplified computation in anti-collision radio frequency identification (RFID) is proposed and presented.
4	Maestro: A high performance AES encryption/decryption system,	M. Biglari, E. Qasemi and B. Pourmohseni	2013	This article presents a high performance yet cost efficient AES system. Maestro can be used in a wide range of embedded applications with various requirements and limitations.
5	Research of enhancement algorithm based on Fibonacci Number for anti-collision in RFID system	Zhaoyang Zhou and Yanju He	2011	Aiming at the problem of tag-collision in RFID system, this paper analyses Aloha algorithm and its improvement algorithm.
6	An Efficient MAC Protocol for Throughput Enhancement in Dense RFID System	G. P. Joshi and S. W. Kim	2009	In this paper author propose a distributed multi-channel reader anti-collision MAC (ACMAC) protocol to mitigate the reader collision problem.
7	A Divide-and-Conquer Technique for Throughput Enhancement of RFID Anti-collision Protocol	J. G. Kim	2008	A novel anti-collision technique is proposed to maximize identification performance in slotted Aloha based radio frequency identification (RFID) systems.

R. K. Ibraheem, R. A. J. Kadhim and A. S. H. Alkhalid [1] A series of latest papers have pretended collision attacks on publicly used hash functions, including the widely published SHA-1 algorithm. To estimate this threat, the natural response has been to strengthening the system to overcoming the weakness that make the system apt to collision. The SHA-1 hash function used in many fields of security system such as digital signature, tamper detection, password protection and so on. SHA-1 is very important algorithm for integrity and authentication realization,

SHA-1 is a one way algorithm to produce hash code of any message with 160 random hash bits, which cannot be reversible. AES with SHA-1 algorithm produce encrypted code that can be reversible to achieve confidentiality. From the implementation and simulation results of AES based on SHA-1 algorithm obtained in Lab VIEW project show simplicity in modelling hash function algorithm generating hash codes encrypted by AES method.

L. Sanchez and V. Ramos [2] RFID is one of the most pervasive technologies in contemporary societies. Modern RFID applications require efficient tag identification mechanisms to improve performance. Recently, a new approach has arisen to enhance the identification process in an RFID network. This new approach considers the inclusion of an additional device in the RFID network, which leads to an augmented RFID system. Up to date, the are only few proposals taking such approach into account, being the most interesting those that extend the interrogation zone of an RFID reader. However, the performance of such proposals has not been evaluated yet. In this paper, authors review an augmented RFID system to evaluate its performance and study its advantages and limitations. Moreover, authors design an anti-collision protocol for such system taking advantage of such features. Our proposed protocol is EPC Class-1 Generation-2 standard compliant. authors evaluate an augmented RFID system along with our proposal in terms of identification delay to find that it is able to highly reduce such parameter, with gains of up to 40% when compared with a well known multi-reader scheme.

H. Landaluce, A. Perallos, L. Bengtsson and I. J. G. Zuazola [3] A memoryless-based Collision window Tree plus (CwT+) protocol for simplified computation in anti-collision radio frequency identification (RFID) is proposed and presented. The CwT+ makes effective use of a threshold to accurately enhance bit-tracking and in turn lowers the identification time of the communication response. The threshold limits the bitstream of responding tags in an accurate fashion for simplified computation in the interrogation procedure. Simulation results show the outperformance of the CwT+ compared with earlier protocols.

M. Biglari, E. Qasemi and B. Pourmohseni [4] High throughput AES encryption/decryption is a necessity for many of modern embedded systems. This article presents a high performance yet cost efficient AES system. Maestro can be used in a wide range of embedded applications with various requirements and limitations. Maestro is about one million times faster than the pure software implementation. The Maestro architecture is composed of two major components; the soft processor aimed at system initialization and control, and the hardware AES engine for high performance AES encryption/decryption. A ten stage implicit pipelined architecture is considered for the AES engine. Two novel techniques are proposed in design of AES engine which enable it to reach a throughput of 12.8 Gbps. First, tightly coupled encryption and round key generation units in encryption unit, and second, ahead of time round key generation in decryption unit. Altera DE2-115 development and educational FPGA board is used as the platform for Maestro. In the proposed architecture the DMA modules act as interfaces between data sources and data sinks by loading the input data into AES engine and taking encrypted and generated test data to target memories.

Zhaoyang Zhou and Yanju He [5] Aiming at the problem of tag-collision in RFID system, this paper analyses Aloha algorithm and its improvement algorithm. An enhancement dynamic frame slotted Aloha algorithm based on Fibonacci Number was proposed. Furthermore, the strategy of changing the frame length is established. The simulation indicates that the proposed algorithm can improve the throughput and load of RFID system.

G. P. Joshi and S. W. Kim [6] In dense radio frequency identification (RFID) system, reader collision problem is bottleneck of overall system performance. In this paper authors propose a distributed multi-channel reader anti-collision MAC (ACMAC) protocol to mitigate the reader collision problem. The proposed probability based channel selection approach helps selecting channel efficiently and reduces the waiting time and beaconing method solves the hidden and exposed node problem. Also, channel utilization probability based random backoff mitigates the collision possibility in the control channel. Simulation results show our protocol is energy efficient and gives higher network throughputs than the existing MAC layer protocol in RFID.

J. G. Kim, [7] A novel anti-collision technique is proposed to maximize identification performance in slotted Aloha based radio frequency identification (RFID) systems. Authors observe that much higher throughput can be achieved by identifying tags in a divide-and-conquer method, in which the set of tags is partitioned into multiple subsets of roughly equal size and then each subset is identified in sequence. Numerical results show that the throughput performance of our proposal outperforms existing methods by a significant margin.

IV. PROBLEM IDENTIFICATION

Nowadays, web has turned out to be one of the critical part in our lives and it is considered as one of the communication way. Our lives will be unpleased if there is no web. In spite of the fact that the web are generally utilized internationally, it is reasonable a few people may in any case not know the procedure associated with the web communication, and one of the case forms behind the

web is the Advanced Encryption Standard (AES) encryption to encode and decode the record and visit by coding.

Beginning from the presence of PC up to this point, there are bunches of communications by sending or getting the information or records between the sender and receiver. In the interim, the encryption procedure is executed with the communication to ensure the information or record transmission, subsequently, just the receiver can comprehend the substance inside the document and information sent by the sender, which is a two-routes communication in secure way.

V. CONCLUSION

The aim of the this Study is to give a review of the AES encryption algorithm, to build up a model that is actualized for communication reason, and to test the created model as far as exactness reason. The idea of AES algorithm was right off the bat considered, including the definition, verifiable foundation, and a short correlation was made between the AES algorithm with different kinds of algorithm. Here, the reason of picking AES algorithm as the considered was additionally being explained. Efficiency of algorithms was likewise another critical criteria. Two qualities were resolved as basic in the choice of the AES: security and effectiveness. In this examination the assessment and determination criteria of AES finalist algorithms will be researched additionally the correlation between various algorithms will be talked about.

REFERENCES

[1]. R. K. Ibraheem, R. A. J. Kadhim and A. S. H. Alkhalid, "Anti-collision enhancement of a SHA-1 digest using AES encryption by LABVIEW," 2015 World Congress on Information Technology and Computer Applications (WCITCA), Hammamet, 2015, pp. 1-6.

[2]. L. Sanchez and V. Ramos, "An EPC class-1 generation-2 anti-collision protocol for RFID tag identification in augmented systems," 2015 International EURASIP Workshop on RFID Technology (EURFID), Rosenheim, 2015, pp. 36-43.

[3]. H. Landaluce, A. Perallos, L. Bengtsson and I. J. G. Zuazola, "Simplified computation in memoryless anti-collision RFID identification protocols," in Electronics Letters, vol. 50, no. 17, pp. 1250-1252, 14 Aug. 2014.

[4]. M. Biglari, E. Qasemi and B. Pourmohseni, "Maestro: A high performance AES encryption/decryption system," The 17th CSI International Symposium on Computer Architecture & Digital Systems (CADS 2013), Tehran, 2013, pp. 145-148.

[5]. Zhaoyang Zhou and Yanju He, "Research of enhancement algorithm based on Fibonacci Number for anti-collision in RFID system," 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 588-590.

[6]. G. P. Joshi and S. W. Kim, "An Efficient MAC Protocol for Throughput Enhancement in Dense RFID System," 2009 4th International Symposium on Wireless Pervasive Computing, Melbourne, VIC, 2009, pp. 1-5.

[7]. J. G. Kim, "A Divide-and-Conquer Technique for Throughput Enhancement of RFID Anti-collision Protocol," in IEEE Communications Letters, vol. 12, no. 6, pp. 474-476, June 2008.

[8]. Christophe De Canniere, Florian Mendel, and Christian Rechberger, Collisions for 70-Step SHA-1: On the Full Cost of Collision Search, Selected Areas in Cryp¬tography (Carlisle M. Adams, Ali Miri, and Michael J. Wiener, eds.), Lecture Notes in Computer Science, vol. 4876, Springer, 2007, pp. 56-73.

[9]. Christophe De Canniere and Christian Rechberger, Finding SHA-1 Characteris¬tics: General Results and Applications, ASIACRYPT (Xuejia Lai and Kefei Chen, eds.), Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 1-20.

[10]. Florent Chabaud and Antoine Joux, Differential Collisions in SHA-0, CRYPTO (Hugo Krawczyk, ed.), Lecture Notes in Computer Science, vol. 1462, Springer, 1998, pp. 56-71.

[11]. Martin Cochran, Notes on the Wang et al. 263 SHA-1 Differential Path, Cryptol¬ogy ePrint Archive, Report 2007/474, 2007.

[12]. Ivan Damgard, A Design Principle for Hash Functions, CRYPTO (Gilles Bras¬sard, ed.), Lecture Notes in Computer Science, vol. 435, Springer, 1989, pp. 416¬427.