ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

HASHED LIGHTWEIGHT AUTHENTICATION IN ENCRYPTION

M. Harini[1], T.Sahana[1], S.Saravanan[2]*, M.Lavanya[2]
[1]B.Tech Information Technology, School of Computing, SASTRA University
[2]Assistant Professor, School of Computing, SASTRA University, Thanjavur, Tamilnadu, India
Email: saran@core.sastra.edu

Received on 26-07-2016 *Accepted on 03-09-2016*

Abstract

Secure Communication of data is a major concern in today's growing world. Cryptography is the mathematical technique of hiding information for ensuring authentication, confidentiality and other aspects of information security. The growing aspect of data transmission needs an exceptional means of security over the network. Cryptanalysis attack has to be difficult for the third party access. These emphasize the demand for light weight concept in encryption. An Authenticated Lightweight Encryption (ALE) is an individual-path nonce-based encryption algorithm which uses associated data. It implements the combination of both AES-128 bit key schedule and their round transformation. ALE provides better security and high performance than other encryption techniques but it leads to Slide attack which occurs when the periodic process illustrates self-similarity and independent of the iterated round function. It is prevented by avoiding the self-similarity of a periodic process by adding iteration counters and random constants which is fixed. It employs all symmetric cryptographic functions, from hashing to authenticated encryption and random number generation. Thus a cryptographic process based on AES technique, implemented with lightweight algorithm and lightweight hash function is proposed for better security.

Keywords: Encryption algorithm, Hash function, Light Weight algorithm

1. Introduction

Security is a key concern while transmitting the data. . As the internet and other forms of communication becomes more frequent, security becomes increasingly important. Cryptography is a method of storing and transmitting data by which data can be kept confidential. It is an art of protecting information by changing it into an unreadable format but sometimes encrypted messages can by broken by cryptanalysis also called as code-breaking. Crypto-system helps to deal with security related problems by encrypting the data in sender and decrypting it in the receiver. The four main objectives of cryptography are Confidentiality, Integrity, Non-Repudiation, and Authentication. An

Authenticated Lightweight encryption is implemented in order to attain better security and high performance than other encryption techniques.

2. Existing Method

Authenticated Lightweight Encryption (ALE) [1] implements the combination of both AES-128 bit key schedule and their round transformation. It is an individual-path nonce-based encryption algorithm which uses associated data.It provides optimized low area implementation in order to attain better security and high performance than other encryption techniques. It also improves area and time efficiency. Leak Extraction (LEX) [2] for block cipher is an idea to provide output key stream by extracting specific position at particular rounds from the internal state. This helps with fast encryption with storing only small state. LEX state does not need to be changed with time and it evolves very slowly. Comprehensive review of state-of-the-art [3] research program in lightweight block cipher's implementation is implemented with basic metrics. This increases the security level of the system with better performance model. In paper [4], to maintain the power of data authenticity and query integrity with data owners and users, data are outsourced to un-trusted clouds. Hence, for multiple version key value data, an authenticated data-outsourcing problem is addressed. This delivers data integrity, data authenticity and freshness. Resultant authentication [5] on data streams over linear algebraic queries is achieved using lightweight scheme. It is extended for many operations like sums, dot products, matrix multiplication, etc. Achieve privacy preservation [6] and data integrity with differential tolerance, a secure data aggregation technique is proposed. System of creating and sharing session keys in a non-interactive way is grasped for AES encryption. Data integrity and authenticity for transmitted data is gained here. Attribute based encryption achieves [7] secured storage, transmission and sharing of data in the distributed environment. But it uses expensive bilinear pairing. A system with elliptic curve cryptography is proposed to overcome issues like security and privacy in such environment like Internet of Things. In paper [8], end-to-end secured connection is risky in IoT due to heterogeneous nature of communication and imbalance in resource capabilities. A novel collaborative approach for key establishment is designed to reduce the requirements of security protocols. Lightweight secure implementation [9] SMS4 is proposed against node confine with white box attack for protecting wireless sensor networks. This is for symmetric algorithms in encryption. This solution fulfills the necessity of sensor nodes. It is a method to overcome slide channel attacks and key compromise in the node. This is a white box type encryption algorithm, which improves both security and complexity. Privacy preserving authentication protocol [10] for Radio Frequency Identification is provided by a lightweight stream cipher. This depends on a single cryptographic component. The ambition is to provide a balance between privacy and safety, resistance against defiance of service attacks and computational efficiency. This is achieved by stream cipher which is chosen arbitrarily with low complexity and also provides security. Lightweight Phrase Search[11] in Cloud storage with Symmetric Searchable Encryption is used for searching document with phrase or consecutive keyword. This provides efficient system with low costs of transmission and storage. Authenticated Permutation [12] based Encryption is the first authenticated encryption scheme based on permutation that is defiant across nonce misuse. In paper [13], protecting data privacy and encrypting specific sensitive data provides efficient database utilization a very interesting task. A lightweight framework for isolate prevention of data queries in cloud computing is designed to maintain the structure of database and supports adequate queries. A cross-layer based lightweight implementation [14] is proposed to provide a channel with better security for transmission. It is robust under various security attacks along with better performance progress. In paper [15], side channel analysis accomplishes the information which leaked through unintended outputs. The least requirements for heuristic based SCA-security is designed to preserve the implementation of AES with any standard mode. Universal forgery [16] is a proposed method to generate the correct tag of any given message. This works even if the attacker changes a single block. It performs one-time pre-processing resulting in faster system. A provable security is achieved to overcome this attack by threshold implementation. In paper [17], one of the attacks in Advance Encryption Standard is first order power analysis attack. A provable security to overcome this attack is achieved by threshold implementation.

3. Proposed System

Study has been done to overcome the major flaws from the existing system. The proposed system uses the Authenticated Lightweight algorithm with lightweight hash function. Keccak, a family of sponge function is a proposed cryptographic hash algorithm providing more security. Keccak has a thick safety margin. The duplex and sponge function used by this technique provides more security against generic attacks. This proposed method proposes this function, implemented with ALE algorithm.

Thus a new algorithm namely hashed lightweight authenticated encryption is developed from the existing systems. This algorithm deploys three layer of security. First layer provides the authenticated encryption for the given input. Second layer is implemented with lightweight cryptographic algorithm and the final layer includes lightweight cryptographic hash function. All together the three layers provide maximum security, authentication, confidentiality and integrity.

The algorithm for proposed HALEX system is as follows:

1. Get the input Plaintext, Key and associated data.

2. Perform Keccak operation for the given plain text by passing it as argument.

2.1. Hexadecimal Big Integer is derived for provided input with different round constant and rotation offset.

2.2. String of arbitrary length is returned by converting the hexadecimal value.

3. Hashed plaintext, key and associated data in byte array is passed into ALE function.

4. ALE function performs two operations namely AES and LEX.

    4.1. Input associated data is first split into block of 16 bytes and encrypted with AES function.

    4.2. AES performs following operations for each block

        4.2.1. Key expansion

        4.2.2 Initial AddRoundKey

        4.2.3. Perform all Four Rounds of AES

        4.2.4 Final round with no MixColumns.

    4.3. Plaintext is then encrypted with AES and LEX operation after splitting as bloc as same as associated data.

        4.3.1. Normal AES operation is performed for given input bloc of 16 bytes.

        4.3.2. Produced output is passed as parameter into the LEX function which performs same AES operations and returns only particular 4 bytes for each round.

    4.4 Each four byte leaked is EXO Red with bloc message to produce cipher text

5. After performing a sequence of encryption for associated data and plaintext bloc, a tag of encrypted bloc is produced as output.

LEX steps were shown below:

```
LeakEX(State, Secret_key)
{
AESKeyExpansion(Secret_Key, Expanded_Key);
State = AESEncrypt(IV, Expanded_Key);
Add_Round_Key(State, Expanded_Key[0]);
for (i=1; i< t; i++){
Rounds(State, i);
```

```
        Outputs[i] = Leak_Extract(State, i mod 2);
        }
        }
        Rounds(State, i)
        {
        Compute four rounds of AES for the given state
        }
KECCAK Function - Func[a](B)
{
 ¥x present in the range 0 to number_of_rounds-1
 B equals to Round[a](B, round_count[x])
return B
}
 For Round[a](B,round_count)
{
Initially at step step0 ,
Array C[p] assigns to xored value of B[p,0] , B[p,1] , B[p,2] , B[p,3] , B[p,4] , until for all p in the range 0…4
Array D[p] assigns to xored value of C[p-1] , rot(C[p+1],1) , until for all x in the range 0…4
Then Array B[p,q] equals to B[p,q] xor with D[p] , until for all (p,q) in the range (0 to 4,0 to 4)
At 1st and 2ndsteps,
Array A[q,2*p+3*q] assigns to rot(B[p,q], r[p,q]), until for all (p,q) in the range (0 to 4,0 to 4)
At 3rd step Array B[p,q] equals to A[p,q] xor with ((not A[p+1,q]) and A[p+2,q]), until for all (p,q) in the range (0 to 4,0 to 4)
Atlast 4th step array B[0,0] equates B[0,0] xored with round_count Finnaly return Array B
}
```

4. Experimental Results

Various Security parameters were analyzed in the following experimental results. They are time, memory usage or utility, Block size, rounds of encryption, Cyber type, Security and various attacks. This is compared with ALE, ALE with Hash function and ALE with LHASH functions. Observation of experimental result shows that ALE with LHASH produces more security than other existing methods.

Parameters	ALE	ALE + HASH	ALE + LHASH
Time	5 ns	9 ns	50 ns
Memory (MB)	2.73	2.72	2.7
Block size (bits)	128	128	128
Rounds	10	10	10
Cipher type	Symmetric	Symmetric	Symmetric
Security	Less secure	Moderate	More secure
Known attacks	Slide attack, Side channel attack	Slide attack, Side channel attack	More complex in attempting side channel attack

5. Conclusion

The proposed design implements a lightweight hashing technique (keccak) in order to realize the data integrity and confidentiality. This Hash function is employed with ALE algorithm which provides high security in terms of complexity. From our experiment results, it is observed that the authentication of a given message is ensured in a lightweight manner and cryptanalysis is made difficult to break by the attackers. Thus the data security is tightened.

References

1. Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen, Elmar Tischhauser, 2014, ALE: AES-Based Lightweight Authenticated Encryption, IEEE Series, Vol8424, 447 - 466.

2. A. Biryukov. 2008, Design of a New Stream Cipher-LEX, eSTREAM Finalists, Vol4986, 48–56.

3. B. J. Mohd, T. Hayajneh, Athanasios V. Vasilakos, 2015, A Survey on Lightweight Block Ciphers fpr Low-Resource Devices: Comparitive Study and Open Issues, Jounal of Network and Computer Applications. 73 – 93.

4. Yuzhe Tang, Ting Wang, Ling Liu, Xin Hu, Jiyong Jang.2014, Lightweight Authentication of Freshness in Outsourced Key-Value Stores, Annual Computer Security Application Conference, 176-185.

5. G. Cormode, A. Deligiannakis, M. Garofalakis, and S. Papadopoulos, 2013, Lightweight authentication of linear algebraic queries on data streams, Special Interest Group on Management of Data.

6. HaiyongBao and Rongxing Lu, 2015, A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerancen, Peer-to-Peer Networking and Applications, 1-16.

7. Xuanxia Yao, Zhi Chen, Ye Tian, 2015, A lightweight attribute based scheme for the internet of things, Future generation Computer Systems, Vol 49, No C, 104-112.

8. Ben Saied, Y., Olivereau, A., Zeghlache, D., & Laurent, M, 2014, Lightweight collaborative key establishment scheme for the Internet of Things. Computer Networks, Vol 64, No 8, 273–295.

9. Yang Shi, Zongjian, 2014, Lightweight white-box symmetric encryption algorithm against node capture for WSNs, Wireless Communication and Networking Conference, 3058-3063.

10. B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, 2010, Scalable RFID Systems: a Privacy-Preserving Protocol with Constant-Time Identification. IEEE International Conference on Dependable Systems and Networks (DSN), 1–10.

11. Mingchu Li; Wei Jia; Cheng Guo; Weifeng Sun; Xing Tan, 2015, LPSSE: Lightweight Phrase Search with Symmetric Searchable Encryption in Cloud Storage, Information Technology - New Generations,174–178.

12. Andreeva, E. Bilgin, B. Bogdanov, A. Luykx, A. Mennink, B. Mouha, N. Yasuda, K, 2013, APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography, Cryptology ePrint Archive.

13. Jin Li, Zheli Liu, Xiaofeng Chen, FatosXhafa, Xiao Tan, Duncan S. Wong, 2015, L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing, Knowledge Based Syst. Vol. 79, 18-26.

14. Abhijan Bhattacharyya, Tulika Bose, Soma Bandyopadhyay, ArijitUkil, Arpan Pal, 2015, LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption, AINA Workshops, 682-687.

15. Mostafa M. I. Taha, Patrick Schaumont, 2015, Key Updating for Leakage Resiliency With Application to AES Modes of Operation, IEEE Trans. Information Forensics and Security Vol. 10 No. 3, 519-528.

16. Orr Dunkelman, Nathan Keller, AdiShamir, 2015, Almost universal forgery attacks on AES-based MAC's, Journal: Des. Codes Cryptography, Vol. 76, No. 3, 431-449.

17. BegülBilgin, BenediktGierlichs, SvetlaNikova, VentzislavNikov, Vincent Rijmen, 2014, A More Efficient AES Threshold Implementation, Annual International Conference on Theory and Application of Cryptology, 267-284.

Corresponding Author:

S.Saravanan*,

Email: saran@core.sastra.edu