International Journal of Engineering & Technology, 7 (2.7) (2018) 502-506

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

HS1-RIV: Improved Efficiency for Authenticated Encryption

Abhishek Bhardwaj[1]*, Subhranil Som[2], S. K. Muttoo[3]

[1,2]Amity institute of Information Technology, Amity University Uttar Pradesh, Noida, India
[3] Department of Computer Science, Delhi University, Delhi, India
** Corresponding author E-mail: abhi14.amity@gmail.com*

Abstract

Encryption was "need of the hour" when it was invented but with the progress of time researchers have shown that it is not very effective when implemented alone. Many attacks are present in the present time, which can break any simple encryption in no time. Therefore, researchers have proposed and proved various techniques, which can work along encryption and can increase security by many folds. This paper aims at bringing essence of this evolution and benefits that tag along with it in one document. Various researchers have different point of view regarding the use of techniques and their benefits along with it, some of those point of views and their reasons are given in this paper

Keywords: *Authenticated Encryption, Subtle Authenticated Encryption, Robust Authenticated Encryption, Initialization vector, Hash Stream 1 (HS1), SIV, RIV*

1. Introduction

Evolution of cryptography is not an eye opening invention, because it is continuously adapting itself and modifying itself from the time of its existence. However, in recent times it is proved by various researchers that cryptography on its own is not secure and possibly open for attacks [1,6], which mostly can prove to be successful. In the counterattack of this loophole various additive techniques are proposed, some of which proved to be of great advantage in respect of security. One of the most primal and easily implemented technique is to add authentication to encryption and makes it- authenticated encryption; another could be to add steganography to cryptography, and so are others. The scope of this will aim at elaborating the branch in which authentication is added to cryptography. Authenticated encryption (hereafter AE) is a symmetric key encryption scheme that provides authenticity and integrity in addition to confidentiality, which is provided by simple encryption. It was used for key wrapping, i.e. protecting the transportations of cryptographic keys. Some basic sub categories of authentication encryption are Hash-then-Encrypt (HtE), MAC-then-Encrypt (MtE), Encrypt-the-MAC (EtM) and Encrypt-and-MAC (E&M). Decryption and authentication is straightforward in all these approaches at the receiver's end, where either authentication is done prior to decryption or visa-versa. All these techniques have security vulnerabilities if not executed properly. However, if properly executed, they all can provide higher level of security. One of the working applications of HtE is WEP (wireless equivalent protocol) for protecting Wi-Fi networks, which had some fundamental weaknesses and led to its replacement.

Another advantage of AE is that, it gives security against chosen plain text attack (here after CPA) and chosen cipher text attack (here after CCA). When checking for any attack, it is assumed that attacker knows the encryption algorithm and still if encryption technique prevents adversary from getting information, then it is considered secure algorithm. There are many examples of CPA, in some cases adversary can send a cipher text that he acquired during eavesdropping, to the decryption server and get plain text in return. In other (and most) cases adversary can learn partial information about the message and not the complete plain text. In the case of AE, even if an assumption is taken that the adversary can obtain encryption of an arbitrary message of his choice (CPA) or he can decrypt any cipher text of his choice (CCA) and his goal is to break semantic security; then also he cannot do it [6].

Many researchers have worked on AE and provided varies schemes that provide better structural design of AE. Rogaway and shrimpton proposed nonce bases MRAE (misuse resistant AE) and introduced synthetic initialization vector scheme (SIV). In the terms of cryptography, a number, which cannot be repeated, is termed as nonce. It helps in providing security against replay attack where every communication has an issued random and unique number called nonce. SIV is a block cipher mode of operation, which takes three inputs, a key, plain text, and multiple variable length octet string, this string is not encrypted but is used for authentication [5]. SIV gives a cipher text as output which has same length as that of the plain text. SIV can be used to achieve two goals, either it will provide deterministic AE or nonce based MRAE.

2. Related work

Various techniques are proposed by researchers in recent times to make communication secure and authentic. In [1] RIV (Random Initialization Vector) is merged with robust authenticated encryption to increase efficiency of robust authenticated encryption. Tjuawinata, I., Huang, T., & Wu, H performed cryptanalysis of authenticated encryption COFFE [4] and proposed ways by which security can be improved in it. AES is one of the most widely accepted encryption algorithm, and thus used as a base in many methodologies such as SIV [5] and RIV. Some academicians have

worked on attacks on cipher texts, and explained how various attacks will work. Ways by which security can be increased by prevention from those attacks is also explained [6]. Some researchers have even proved that merging two cryptographic techniques can result in better security [9]. Another technique, which is used for security increment, is steganography. Steganography is an art of hiding something in plain sight. Many variations of steganography are in existence; such as hiding a message in images [12] or performing a multi-layer embedding using a reverse local histogram shifting [11]. Some review work is also present which teaches techniques for data hiding [10] for improvement in security. With the improvement of technology, need for increased security arose; resulting in techniques such as visual cryptography [14]. Even after all improvements, there are many threats on security, which are explained in [17]. Thinking out of the box, techniques such as discrete logarithms are used with digital signatures and public key cryptosystem to improve system efficiency in the field of security. Biometric systems are considered the highest level of security, but even this technology faces some challenges and issues [21] and need some further improvements.

Cryptography has always been the base of this security but as explained above, need of a counterpart is need of the hour. AE with proper implementation has proved its worth on various grounds [1, 4, 5], but the main part has always been its proper implementation. To implement it properly various modifications and upgradations are done on the basic AE technique [1, 2, and 5]. The need for authenticated encryption arose when only integrity (authenticity) security of a message was not sufficient and the need of confidentiality started to grow. On the base level only four sub classes of authenticated encryption was present, namely: hash then encrypt, MAC then encrypt, encrypt then MAC and encrypt and MAC. Theoretically all four seemed easy to implement with straightforward decryption and authentication but without proper implementation all four started to fail by the hands of cryptanalysts. This does not mean that they were not used; some of the most basic techniques in Wi-Fi security, i.e. WEP was based on hash then encrypt. The next stage in the modification of authenticated encryption was subtle authenticated encryption, which mostly used nonce based authenticated encryption. Nonce is a random generated number, which cannot repeat. Nonce was the base of subtle authenticated encryption but it somehow proved to be the reason of its failure, because if nonce is repeated due to any reason: it be either human error or chosen cipher text attack by attacker; the technique fails [6]. Subtle authenticated encryption uses synthetic initialization vector, which uses static initialization numeric values. However, the next stages perform two level modifications in SAE. In the first modification, SIV was replaced by random initialization vector (RIV), which removed the static shortcomings of the prior technique. Second modification was in the basic structure of the technique, where basic AES was replaced by ChaCha structure. ChaCha structure is a block cipher based technique that proved its worth at various levels of security and it widely used in various applications [3]. Another methodology that came onto bright light was HS1, which when added with basic SIV and followed the basic structure of ChaCha 20, proved to increase security of data transmission by many folds [22]. Crypt-analysis on many techniques even showed that the need of modifications in the existing algorithms is the need of the hour [6, 7, and 17]. Various techniques proposed by researchers for modifications in current technology used for data transmission .Some of the methodologies whose base is AE are explained below with more details.

2.1 Subtle Authenticated Encryption

Various attacks proved that when data is only privacy protected, it fails to give security and needs additional authentication to increase the level of security. Until date, many combined modes of encryption and authentication have developed ([RFC5116], [RFC3610], [GCM], [JUTLA], and [OCB], etc.) which comes under the category of AE [5], that works with nonce. Another category of AE is deterministic and uses nonce less technique. Key wrapping is an excellent application of this category, which is used for protecting transportation of cryptographic keys.

Phillip Rogaway and Thomas Shrimpton proposed SIV that became the next step in the category of basic AE. It provides both nonce based AE and nonce less, deterministic key wrapping. SIV contains two constructions, which are S2V, CTR. S2V contains a pseudo random function (PRF), and CTR contains an encryption/decryption construction. They both uses AES block cipher technique with a key length of 128,192 or 256 bits.

2.2 ChaCha

ChaCha stream cipher is defined as a stand by cipher, which comes from a family of algorithms in which software only (even C language) implementations can give fast and secure results comparable to AES algorithm, which is considered as gold standard in encryption, but is accelerated by hardware implementation. Not only security, AES also provides speed that varies from three times to ten times from many other encryption algorithms such as 3DES [22]. In [22], need of a standby cipher is also explained. In present times many current security algorithms are based on AES because of its speed and hardware implementations, but if in near future AES fails then security of many applications will be at a stake. Its only possible replacement will be 3DES which is many folds slower than it; and thus there is a need of a standby technique which can replace AES with same efficiency and without doing and compromises with security. ChaCha20 is a software based cipher, which is three times faster than AES in systems where software only implementation is present.

Explanation of complete ChaCha algorithm is out of the scope of this paper, but some key points are worth mentioning, such as –

i) Basic operation of ChaCha algorithm is done in a quarter round where the operation is done on four 32 bits unsigned integers.
ii) ChaCha20 means there will be 20 rounds of processing (or 80 quarter rounds)
iii) Other variations of ChaCha stream cipher are ChaCha8 (32 quarter rounds) and ChaCha12(48 quarter rounds)

Assuming four 32 bits signed integers to be a, b, c and d; the actual operation in one quarter round is this

1. a += b; d ^= a; d <<<= 16;
2. c += d; b ^= c; b <<<= 12;
3. a += b; d ^= a; d <<<= 8;
4. c += d; b ^= c; b <<<= 7;

“Where "+" denotes integer addition modulo 2^32, "^" denotes a bitwise Exclusive OR (XOR), and "<<< n" denotes an n-bit left rotation (towards the high bits)”.

Actual operation of quarter rounds are not explained here but just showing output of one quarter round is explained below:

Assuming

- a = 0x11111111
- b = 0x01020304
- c = 0x9b8d6f43
- d = 0x01234567

After one quarter round on these four numbers, using formulas given above, the output will be

- a = 0xea2a92f4
- b = 0xcb1cf8ce
- c = 0x4581472e
- d = 0x5881c4bb

Applying four-quarter rounds will complete a round. Application of ChaCha20 consists of 20 rounds and 80-quarter rounds. Increase in number of rounds will surely result in better security.

3. HS1-SIV

HS1 (Hash-Stream 1) is a pseudo random function (here after PRF) which is used to provide AE through SIV proposed by Rogaway and Shrimpteon. It is designed to provide high software speed on systems like Intel SSE, ARM Neon, etc. HS1 takes an arbitrary input string and an initialization vector (here after IV) and gives a pseudo random string of any desired length as output. For every different pair of input and IV that is provided to HS1, it has a high probability of giving an independent pseudo random string.
SIV, as explained earlier, uses a block cipher based PRF with an input of associated data and plain text to create an SIV. This SIV is used to perform encryption on plain text using a "block cipher encryption scheme". In case of HS1-SIV, HS1 is used to instantiate SIV mode. When HS1 is provided with an "input, IV" pair, it hashes the input using the hash function. Then it XOR's this hash result with the key of stream cipher and uses the HS1 IV as the stream cipher's IV. The primary advantage of it is that this stream cipher will produce as many bytes as desired. It's second advantage is that the stream cipher will produce independent pseudo random output streams for as long as "hash result, IV" pair is never repeated and with an assumption that stream cipher is secured against related key attacks.
HS1-SIV can work on various interfaces but ChaCha stream cipher is the one best suited for it. As explained earlier various version of ChaCha stream cipher such as ChaCha8, ChaCha12, ChaCha20. HS1-SIV as explained by [2] uses ChaCha20 that takes four inputs- A 32 byte key, A 12 byte IV, A plain text and an initial counter value. The resultant will be a cipher text with same length as of the plain text and is a pseudo random.
HS1-SIV as explained in [2] works on various parameters and notations with an aim to achieve the security goals. In every variation of HS1-SIV, probability of adversaries' success is very low, as explained in figure 1

Name	Key Search	SIV Collision
hs1-siv-lo	$n/2^{256}$	$n^2/2^{56} + n^2/2^{64}$
hs1-siv	$n/2^{256}$	$n^2/2^{112} + n^2/2^{128}$
hs1-siv-hi	$n/2^{256}$	$n^2/2^{168} + n^2/2^{256}$

Fig. 1: Adversary's probability of success over n encryptions, each of no more than 2^{32} bytes, or n key guesses

HS1-SIV is designed to achieve some features such as competitive speed on multiple architectures, provable security (with an assumption that ChaCha stream cipher is secured against related key attacks and is a good pseudo random generator), and nonce misuse resistant, scalable and produces a general purpose PRF.

4. Robust Authenticated Encryption

It comes from the family of AE that aims to overcome the drawbacks present in subtle AE. Previously various robust AE schemes are proposed but most of them failed in CAESAR submissions (only four proved robust against leakage of invalid plain text out of total 57 CAESAR submissions) [1]. The work proposed in [1] works on modular framework and is called robust IV, which provides SAE security that is provable. RIV is a successor of SIV that inherits features such as simplicity and strong security from SIV and in addition to this provides robustness against leakage of invalid plain text.

4.1 Modifications in Robust Authenticated Encryption

Robust AE (here after RAE) was a modification to subtle AE (SAE) that aims at increasing the security provided by it. The advantage of RAE is that it provides security even in the case when unverified plaintext is released; and in addition, it inherits all the advantages of SAE. In earlier proposals of RAE, SIV was used which either achieves the goal of nonce based-misuse resistant authenticated encryption or deterministic authenticated encryption. However, [1] proposed Random IV (hereafter RIV) based RAE, which was AES based instantiation of RIV. It was proved that RIV based robust authentication encryption is more secure when compared to SIV based robust authentication encryption, with an only assumption that "AES is secure".

5. Proposed Work

In consent to the above discussion, it is proved that when SIV is replaced by RIV in RAE it proved to be more secure. However, if SIV is an essential structural base for some algorithm it can be merged with "HS1", with a base of "ChaCha" steam cipher, to improve its efficiency.
This paper proposes replacement of SIV with RIV in the structure of HS1-SIV. HS1-SIV proved its efficiency that it is humanly impossible to decipher data secured by it, even with various combinations and several possibilities of key guessing
The only assumption HS1-SIV takes is that AES is secure. By taking this "only" assumption, HS1-RIV is proposed. HS1-RIV will use a pseudo-random function called HS1 (or Hash – Stream 1) and will provide authenticated encryption through RIV. HS1 is designed for high software speed on systems with good processing, without SIMD support. HS1 takes an arbitrary input string and an initialization vector and produces a pseudo random string of any desired length. This feature of HS1 makes it compatible to be used with SIV and RIV. The proposal includes replacement of simple pseudo random function with HS1 for initialization in RIV. A simple replacement of initialization vector will increase the efficiency and security of the proposed algorithm. Final step of proposal includes replacement of RIV with HS1-RIV in [1] to further improve its security. HS1-SIV can provide variable input length and variable output length pseudo random function. The proposal aims at exploiting the advantage that is also provided by HS1-RIV with an addition of better security against chosen plaintext attack. RIV takes the complete structure of SIV, with an additional call to internal PRF for security, against chosen plaintext attack.
Encryption and Decryption process of HS1-RIV is given as follows with the help of a flow chart. In the process of encryption, as explained in figure 2, many parameters are used, such as nonce value, authenticator and other parameters, which can affect performance and security. Decryption process is explained as follows:

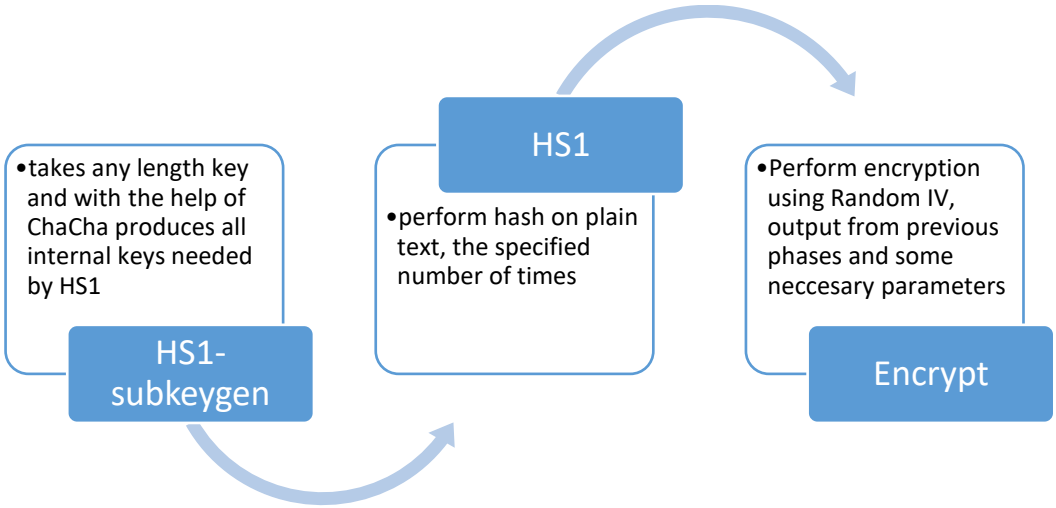

Fig. 2: Encryption process of HS1-RIV

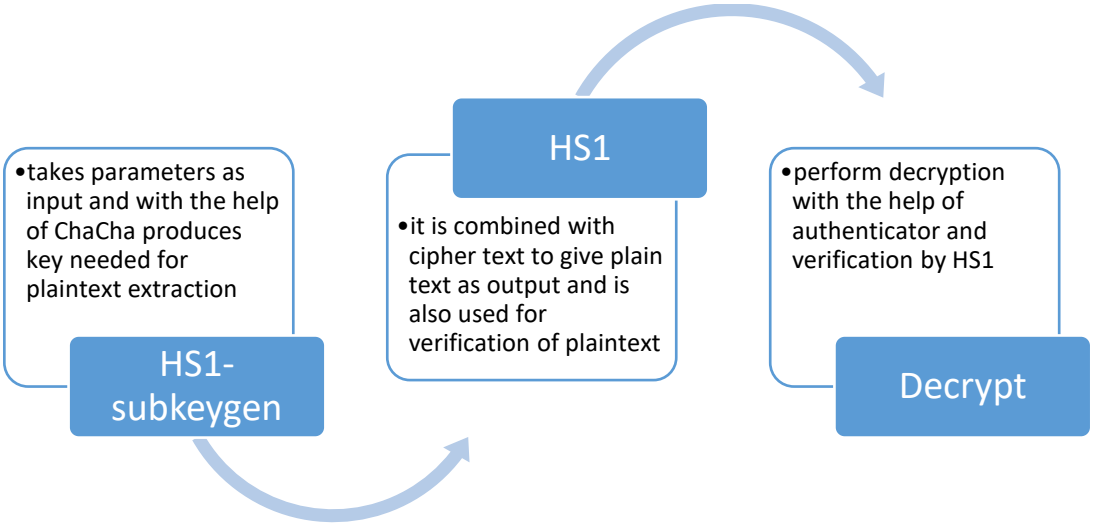

Fig 3: Decryption Process of HS1-RIV

In the process of decryption, as explained in figure 3, authenticator is also used as initialization vector. Decryption is also dependent on various parameters for security and performance. Detailed proposal, results and security proofs will follow in next paper.

6. Conclusion

As a conclusion, it is witnessed, that there are various ways by which efficiency and security of encryption is increased. Be it improvement in encryption, by adding authentication to encryption in cipher techniques such as subtle authenticated encryption, robust authenticated encryption, or merging encryption with steganography. This paper proposes that to improve security of encryption further "hash stream 1"and random initialization vector are merged with basic AES encryption or ChaCha cipher structure. The resultant methodology will provide security against unverified plaintext in addition to all the advantages of HS1-SIV. However, it is just a proposal whereas proofs and results will follow in next paper

References

[1] Abed, F., Forler, C., List, E., Lucks, S., & Wenzel, J. (2016). RIV for Robust Authenticated Encryption. *Fast Software Encryption Lecture Notes in Computer Science*,23-42. doi:10.1007/978-3-662-52993-5_2

[2] Geltink, G., & Volokitin, S. (2016). FPGA Implementation of HS1-SIV. *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications*. doi:10.5220/0005950100410048

[3] Nir, Y., & Langley, A. (2015). ChaCha20 and Poly1305 for IETF Protocols. *Network working group, Internet-Draft*. doi:10.17487/rfc7539

[4] Tjuawinata, I., Huang, T., & Wu, H. (2016). Cryptanalysis of the Authenticated Encryption Algorithm COFFE. *Lecture Notes in Computer Science Selected Areas in Cryptography – SAC 2015*,510-526. doi:10.1007/978-3-319-31301-6_29

[5] Harkins, D. (2008). Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). *Network Working Group*. doi:10.17487/rfc5297

[6] I. (2016, August 19). Cryptography chosen ciphertext attacks (authenticated encryption). Retrieved December 21, 2017, from https://www.youtube.com/watch?v=l3U-povLQp0

[7] A. Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, Noida, 2016, pp. 208-212.

[8] Spammimiccom, *"Spam mimic Explanation"*, http://www.spammimic.com/explain.shtml, July 21, 2017.

[9] Som S., Banerjee M., (2013) "Cryptographic Technique by Square Matrix and Single Point Crossover on Binary Field", 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA'13), IEEE Explorer, Print ISBN: 978-1-4673-2820-3, February 12 – 14, 2013

[10] Sabu M Thampi , " Information Hiding Techniques: A Tutorial Review", ISTE-STTP on Network Security & Cryptography, LBSCE , 2004

[11] Zhibin Pan, Sen Hu , Xiaoxiao Ma , Lingfei Wang.,(May 2015)" Reversible data hiding based on local histogram shifting with multilayer embedding", Journal of Visual Communication and Image Representation Volume 31, August 2015, Pages 64–74

[12] Tzu-Chuen Lu , Jhih-HueiWu,Chun-ChihHuang," Dual-image-based reversible data hiding method using center folding strategy", Signal Processing Volume 115, October 2015, Pages 195–213
[13] Dr. Preeti Mehta,Ms. Monika Bansal , Ms. Akanksha Upadhyaya," Stream Cipher and Block Cipher Based Performance Analysis of Symmetric Cryptography Algorithms: AES and DES", International journal of modern trends in engineering and research ,Volume 2,issue 7 , 2015
[14] Ritesh Mukherjee, Nabin Ghoshal," A Novel Technique for Digital Signature using Steganography Based Visual Cryptography (DSSBVC)"ICRITO,Amity university, 2015
[15] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and steganography-A survey" Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630, 2015
[16] Diffie, W., Hellman, M.E. : New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654, 1976
[17] Seema Nath, Subhranil Som , "Security and Privacy Challenges: Internet of Things", Indian Journal of Science and Technology, Scopus Indexed, Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110642, ISSN (Print): 0974-6846 ISSN (Online): 0974-5645, January 2017.
[18] Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270–299
[19] Rivest, R.L., Shamir, A., Adleman, L.M. (1983): A method for obtaining digital signatures and public-key cryptosystems (reprint). Commun. ACM 26(1), 96–99, 1984
[20] El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18, 1985
[21] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management), vol. 92, no. 6, pp. 948–960, June 2004.
[22] Cryptographic competitions. (n.d.). Retrieved December 26, 2017, from https://competitions.cr.yp.to/round2/hs1sivv2.pdf