Proceedings of
INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND ENERGY SYSTEMS
(ICCCES-16)
In Association with IET, UK & Sponsored by TEQIP-II
29th -30th, Jan. 2016

Paper ID:CSEIT30

IMPLEMENTATION OF ELASTIC AES

Swati P. More
Dr.V.R.Ghorpade
Department of Computer Science and Engineering,
D.Y. Patil College of Engineering & Technology, Kolhapur

ABSTRACT: Elastic block cipher, allows to "stretching" the supported block size of block cipher up to a length double the original block size, while increasing the computational workload proportionally to the block size. We opt for the first method for creating an elastic block cipher from an existing block cipher. Our intent is not to design a newad-hoc cipher. But to systematically build upon existing block ciphers. Our method uses the round function from an existing block cipher. Allowing us to treat the round function of the original cipher as a black box and reuse its properties. This results in the security of the elastic version of a cipher being directly related to that of the original cipher. Our method is designed to enable us to form a reduction between the elastic and the original versions of the cipher. Using this reduction, we prove that the elastic version of a cipher is secure against a key-recovery attack if the original cipher is secure against such attacks.

Keyword: - variable-length block ciphers, elastic block ciphers

I.INTRODUCTION

In cryptography a block cipher is a symmetric key cipher operating on fixed length group of bits termed blocks with an unvarying transformation. A block cipher encryption algorithm might take (for example)a 128-bit block of plaintext as input and output a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input-the secret key. Decryption is similar: the decryption algorithm takes .in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bits block of plaintext. To encrypt messages longer than the block size, a mode of operations e.g. CBC, OFB, CFB, CTR is used.Which allow block ciphers are designed around one or a small number of block sizes with most supporting 128-bit blocks.

As discussed earlier, standard block ciphers are designed around one or a smallnumber of block sizes, with most supporting 128-bit blocks. In applications, the length of the data to be encrypted is often not a multiple of the supported block size. This results in the use of plaintext-padding schemes that imposecomputational and space overheads by appending bits to thedata. When the data being encrypted is relatively small, thepadding can become a significant portion of the encrypteddata. For example, encrypting a database at the field or rowlevel to allow for efficient querying can easily result in a substantial amount of padding. While elastic block cipher, allows us to provide supported block size of a block cipher up to a length double the original block size, this together with modes of operation, permits block sizes to be set based on an application's requirements.

While elastic block cipher, allows us to provide supported block size of a block cipher up to a length double the original block size. While increasing the computational workload proportionally to the block size this together with modes of operation, permits block sizes to be set based on an applications requirements.

II.PREVIOUS WORK

A proposal by Bellare and Rogaway[7] uses any existing block cipher as a black box to create a variable-length block cipher patel et al.[8],proposed a modification to their method.Bellare and Rogaway do not modify the original block cipher, but instead add operations around it.they treat the original block cipher as ablack box and analyse the construction independently of the specific block cipher.

Difference between our approach and proposals by Bellare and Rogaway is that they use unbalanced Fiestelnetwork [3] compared to the elastic network we will use. One of the differences that the round function maps b bits to b bits in the elastic network and maps b bits to y bits in the unbalanced Fiestelnetwork. This alone does not prevent an unbalanced Fiestel network from being used with the round function of an existing block cipher that maps b bits to b bits can be chosen from the output of the round function when $y<b$.

III.PROPOSED METHOD

Our method converts the encryption and decryptionfunctions of existing block ciphers to accept blocks of sizeb to 2b bits, where b is the block size of the original blockcipher. Our method uses a network structure, the elasticnetwork shown in Figure 1, into which the round function of the original block cipher is inserted. This allows the properties ofthe original block cipher's round function to be reused. Theelastic network creates a permutation on b + y bits from around function that processes b bits, where $0 \leq y \leq b$.

• It provides a permutation on b + y bits for any $0 \leq y \leq b$ where b is the block size of the fixed-length block cipher. • It is a single, generic, construction that can be used with any block cipher.

• The cycle of any existing b-bit block cipher becomes a Component of the structure without any modification to it.

• The number of rounds is not set by the structure, but rather the round function can be applied as many Times as needed by a specific cipher. • The rate of diffusion for b+y bits is defined in terms of the rate of diffusion for b bits in the fixed-length block cipher.

• The operations involved in the structure allow for efficient implementations in terms of time and memory Requirements.

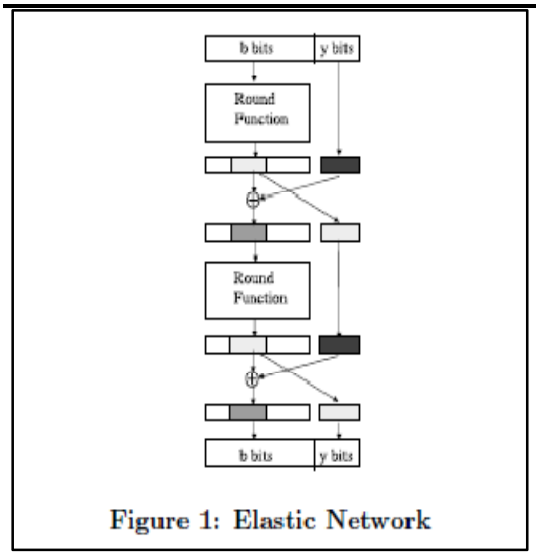

Figure 1: Elastic Network

.

Our process of converting a fixed-length block cipher intoan elastic block cipher involves inserting the cycle of thefixed-length block cipher into the elastic network, addinginitial and final key-dependent permutations, adding or expanding initial and end-of-round whitening, and determining the number of rounds required. The general structureof the method is shown in Fig.2

The following steps convert G with a fixed, b-bit, block Size into its elastic version, G′, that can process b + y bits,for $0 \leq y \leq b$.

1. Set the number of rounds, r′, such that each of theb+y bits is input to and active in the same number ofcycles in G′ as each of the b bits is in G. $r' = r+\lceil ryb \rceil$.

2. Apply initial and end-of-round whitening (XORing withexpanded-key bits) to all b+y bits. If G includes thesewhitening steps, the steps are modified to include allb + y bits. If G does not have this whitening step,the steps are added when creating G′.

3. Prior to the first round and after the last round, applya key-dependent mixing step that permutes or mixesthe bits in a manner that any individual bit is notguaranteed to be in the rightmost y bits with a probability of 1. The leftmost b bits that are output fromthe initial mixing step are the input to the first roundfunction. The initialmixing step is between the initialwhitening and first round function. The final mixingstep is after the last round function and prior to thefinal whitening.4. Alternate which y bits are left out of the round function by XORing the y bits left out of the previousround function with y bits from the round function'soutput, and then swap the result with the y bits left out ofthe previous round? This step is performed after theend of round whitening. Specifically:

(a) Let Y denote the y bits that were left out of theRound functions

(b) Let X denotes some subset of y bits from the round Function's output of b bits. A different set of

An X bit (in terms of position) is selected in eachround.

(c) Set $Y \leftarrow X \oplus Y$.

(d) Swap X and Y to form the input to the nextRound

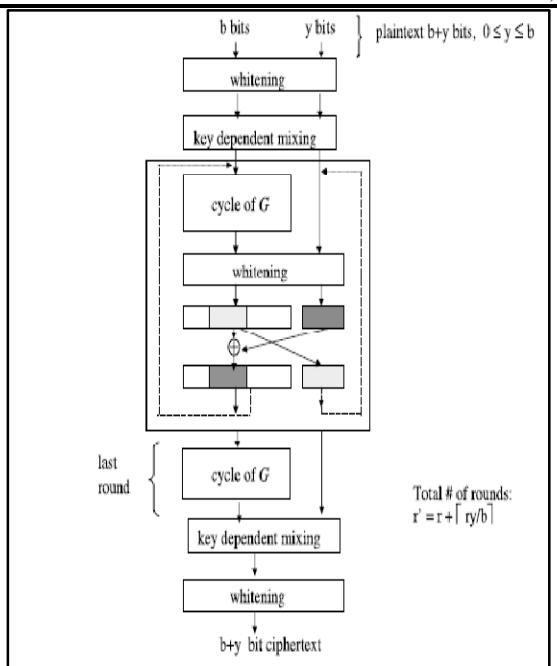

Figure 2: Elastic Block Cipher Structure

Key dependent permutation is a mixing step that permutes or mixes the bits in a manner that any individual bit is not guaranteed to be in the rightmost y bits with a probability of 1.

Whitening is a useful heuristic against attacks that relate the output of a round to the input of the next round. The whitening step assist in letting rounds work in isolation from each other in that the input to a round is unknown even when given the output of the previous round.

Swap Step involves XOR operation on one subset of y bits and another subset in order to increase the rate of diffusion.

IV. RESULTS OR OUTLINE OF THE PROPOSED WORK:

1) Implement a 128 bit AES block cipher algorithm. Round functions from this will be used as a black box in further phase.

2) Implement an elastic block cipher algorithm out of previously implemented AES algorithm. Using its round functions as black box i.e. without disturbing it core functionality.

3) Implement an application that will take plain text as input and give cipher text as output, using elastic version of cipher algorithm.

4) Measure performance of an elastic AES vs. Standard AES

5) Perform differentialcryptanalysis on elastic AES which confirms that the cipher does not introduce potential differential attacks, proving it to be secure at par with standard AES.

V.CONCLUSION

We developed a secure and robust elastic block cipher algorithm over existing fixed length AES block cipher

algorithm.The elastic algorithm proposed should act like a wrapper and can be used over any standard fixed length block cipher algorithm regardless of its implementation.There is minimal efficiency overhead in newly implemented elastic block cipher algorithm.Security of newly implemented elastic block cipher algorithm is at par with that of exiting fixed length block AES algorithm.

REFERENCES

[1] Advanced Encryption Standard (AES) NIST: FIPS 197 (2001)

[2] Aoki, k., Ichikawa, T., Kanda, M., Matsui., S., Nakajima, J., Tokita, T. Camellia: "A 128 bit block cipher suitable for multiple platforms-design and analysis." In: Proceeding of selected Area in Cryptography. LNCS, vol. 2012, 00. 39-56, 2000

[3] Bruce Schneier and John Kelsey "Unbalanced Feistel Networks-cipher design"

[4] Black, J., Rogaway, P. "CBC MACs for arbitary-length : the three key constructions." In Proceeding of Advances in Cryptology-Crypto.LNCS, vol. 1880. Springer, Heideberg (2000)

[5]Schroeppel, R. Hasty Pudding Cipher (1998) http://www.cs.arizona.edu/rcs/hpc

[6] Hall, C., Wagner, D., Kelsey, J., Schneier, B. "Building PRFs from PRPs" In: Proceeding of Advances in Cryptology- Crypto. LNCS, vol. 1462, pp. 370-389. Springer, Heidelberg (1999)

[7]Bellare. M., Rogaway. P. "On the construction of variable length input ciphers" In: Proceeding of Fast Software Encryption. LNCS.Vol. 1636. pp. 231-244. Springer, Heidelberg (1999)

[8] Patel, S., Ramzan, Z., Sundaram G. "Efficient constructions of variable-input-length block ciphers." In: Proceedings of Selected Areas in Cryptography 2004. LNCS.Vol. 3357. Springer, Heidelberg (2004)