Chaos-Based Data Encryption Using Arnold's CAT Map

Atila Bostan[1], Murat Karakaya[2], Gökhan Şengül[3]

[1,2,3] Department of Computer Engineering,
Atılım University, Ankara, TURKEY

{[1]atila.bostan, [2] murat.karakaya, [3]gokhan.sengul}@atilim.edu.tr

ABSTRACT

Continuous Automorphism of the Torus (CAT) is a group of algebraic functions and are typically used in chaos-based encryption applications. Arnold's CAT Map is one of the known CAT calculations. The most charming property of Arnold's CAT Map is a number of repetitions of permutations eventually returns the array into the initial state. The number of repetition to return to the initial state is a function of array dimensions and mapping parameter, unquestionably it is chaotic as well.

Utilization of Arnold's CAT Map in encryption is common especially in image encryption and it is generally preferred for its time efficiency when compared with classical block cipher alternatives. Although substitution and permutation are two essential properties of an encryption algorithm, CAT maps are criticized for conducting permutation only.

In this study an encryption algorithm that makes use of Arnold's CAT Map calculation is proposed and its cryptographic properties are presented.

Keywords –Chaos-based encryption, Arnold's CAT Map, Chaotic maps verification

1. INTRODUCTION

There are considerable number of block encryption algorithms that make use of a symmetric key. The most common ones can be listed as Data Encryption Standard (DES), Triple-DES (TDES or 3DES), Advanced Encryption Standard (AES), Internal Data Encryption Algorithm (IDEA), Rivest Cipher (RC-2,4,5,6), Carlisle Adams Stafford Tavares (CAST) [1]. Core two components of any symmetric encryption algorithm are substitution and permutation functions. Substitution means replacing each byte of the plaintext with some other byte alternative. Whereas permutation means shuffling the bytes in plaintext block. All the symmetric key algorithms are composed of these two functions [2]. In order to increase complexity in encryption these functions are executed in many rounds, typically there are at least one substitution and one permutation in each round. Additionally, a round key which is derived from the initial key is added (typically XOR) to the round operations.

Continuous Automorphism of the Torus (CAT) is a type of mathematical function which returns to the initial state after some number of iterations. Figurative description of such a torus function is given in Figure-1. There are several CAT map functions defined in the field of mathematics. Arnold's, Logistics and Henon CAT maps are the best known ones [3]. CAT maps are generally called chaotic maps.

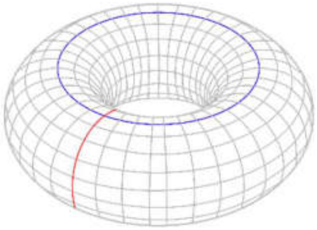


Figure 1. *Schematic description of a continuous automorphism of the torus*

Chaos based encryption studies emerged about 1990s. Chaotic maps and cryptographic algorithms are seen to be similar, since their strong relation to the initial state. The parameters used in the chaotic maps are equivalent to the keys used in the cryptographic algorithms [4]. However, in an abstract view, CAT maps are permuting functions. They don't have any substitution function. CAT map functions only shuffle the initial state order. Nevertheless, the distinguishing characteristics of the CAT maps is their iterated execution guarantees returning back to the initial state anyway [3].

Arnold's CAT map is one of the best known CAT map algorithms and generally studied in image encryption applications. In this study we propose a generic encryption algorithm that is inspired from AES and makes use of Arnold's CAT map (ACM) calculation.

Section two summarizes the literature on CAT map encryption. Following two sections give brief description of ACM and AES respectively. Proposed encryption algorithm is presented in the 5th section. Finally discussion and the conclusions are reported.

2. STUDIES ON CAT MAP ENCRYPTION

Chaos based cryptography has long been studied by the scientists. Different chaotic mapping algorithms were studied. While some of them utilized two or more algorithms, typically one in round-key generation and a different one in encryption, their foremost intention is to increase complexity by using more than one chaotic maps. In Table 1 a matrix that presents the previous studies and their respective mapping algorithms are given [5].

Table 1. *Applied chaotic maps in some proposed image encryption techniques.*

	ACM	**Logistic**	**Henon**	**Lorenz**	**Baker**	**Chen**	**Tent**	**CML**	**Standard map**
Zhu et al. [6]	X	X							
Xu et al. [7]						X			
Zhang and Cao [8]	X			X					
Fu et al. [9]	X								
Zhang et al. [10]	X	X	X						
Ghebleh et al. [11]	X						X		
Elshamy et al. [12]					X				
Ye and Zhou [13]							X	X	
Ye and Zhou [14]							X	X	
Wang et al. [15]					X				
Al-Maadeed et al. [16]		X							
Patidar et al. [17]		X							X
Wong et al. [18]									X
Guanghuia et al. [19]		X							
Zhang et al. [20]		X							
Liu et al. [21]	X	X							

ACM: Arnld's CAT Map, **CML :** Chaotic Map Lattice

It can be seen in Table 1, ACM and Logistic CAT maps are the most common chaotic mapping algorithms studied so far. In parallel with the coverage of this study our focus is on the ACM. Guan et al. [22] studied ACM and Chen map in encrypting the digital images. In their study they used ACM to shuffle the pixels and Chen map to clutter pixel intensity values. Given their study Xiao et al. [23] pointed out the weakness of Guan et al. proposal and further, they proposed a new algorithm to overcome these weaknesses. By the nature of the CAT map algorithms, they are executing permutation only. But, in order to cope with this disadvantage of mapping algorithms Fu et al. [9] proposed a bit shuffling usage in two successive stages and they showed that this approach is more secure than the other ACM applications. In another work Chen et al. [24]

criticized the previous proposals as being weak in chosen plaintext attacks and proposed a hyperbolic mapping for pixel swapping, with the intention to increase the confusion in the algorithm. Keating et al. [25] studied the period problem in ACM and concluded with a mathematical approximation. Finally Soleymani et al. [5] reported a work which uses AMC and Henon map in combination for image encryption.

3. ARNOLD'S CAT MAP ALGORITHM

Arnold's Continuous Aoutomorhism of the Torus Mapping (ACM) algorithm is principally a matrix permutation calculation. In ACM the coordinates of the pixels in an NxN dimension are multiplied with a special 2 x 2 matrix to obtain new X' and Y' coordinates. The distinguishing property of the multiplication is its closed field calculation, which is provided by modulo N operation. No two different indexes ((X_1,Y_1) and (X_2,Y_2)) maps to same (X',Y'), each index maps to a unique new one. So that the index multiplication can successfully shuffle the matrix without any information is lost. Generic formula for ACM calculation and multiplication matrix parameters are given in (1) below.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & P \\ Q & P \times Q + 1 \end{bmatrix} \times \begin{bmatrix} X \\ Y \end{bmatrix} \right\} mod\ N \tag{1}$$

$$\begin{bmatrix} P \times Q + 1 & -P \\ -Q & 1 \end{bmatrix} \tag{2}$$

Where X' and Y' are the new index values calculated from X and Y that are the previous index values. P and Q are integer values of choice and N is the dimension of the data matrix *Data[NxN]*. *Mul[2x2]* is a two dimensional multiplicand matrix with *Mul[1,1]* is always 1 and *Mul[1,1]*=P, *Mul[2,1]*=Q and *Mul[2,2]*=PxQ+1. This definition guaranties the determinant of multiplicand matrix is always 1, so that it has a real Mul^{-1} (2) in all times.

As it is in all the chaotic maps, iterative calculation of the mapping with same parameters eventually returns back to the initial state. The period of a cycle is a factor of P, Q, N and is chaotic. In Figure 2 below the a period (11 rounds of ACM permutation) of picture Lena with size 144x144 is shown for P=1,Q=1.

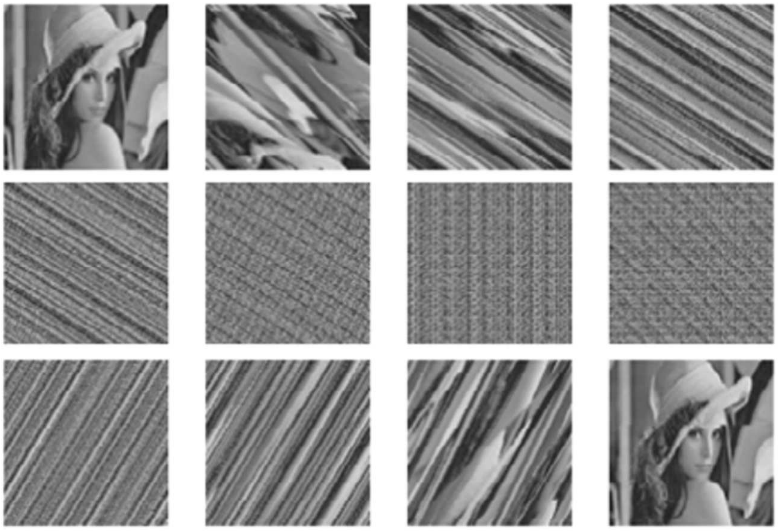


Figure 2. *ACM period of Lena picture (144x144) with P=1,Q=1. Sequence is row vise.*

4. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is a block encryption algorithm that runs on 128, 192 or 256 bits (16, 24 and 32 bytes) key sizes and are called AES-128, AES-192 and AES-256 respectively.

AES algorithm divides the plaintext into 128 bits (16 bytes) blocks and encrypts/decrypt them separately. It has two discrete calculation sequences, namely encryption/decryption and sub-key generation.

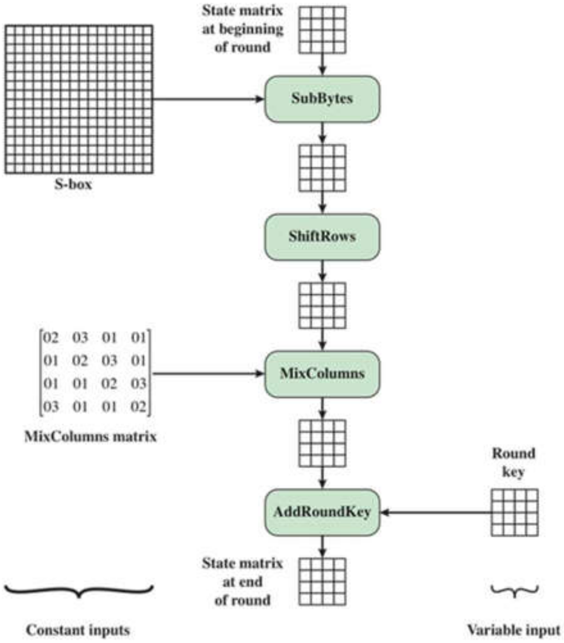
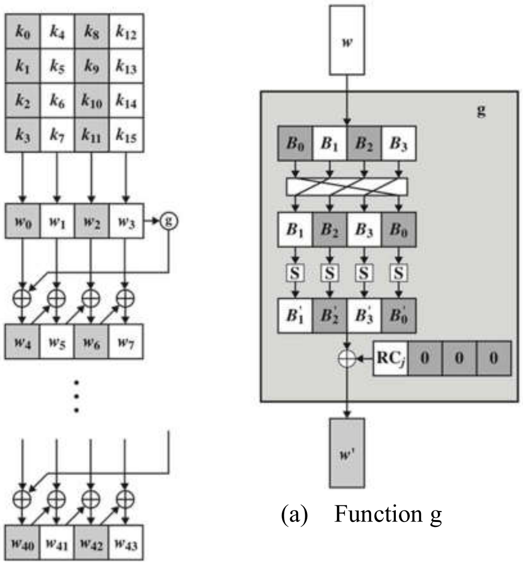


Figure 3. *Four processes in one round of AES encryption.*



(a) Function g

(b) Overall algorithm

Figure 4. *Sub-key generation (a) overall algorithm (b) function g*

In encryption/decryption process there are several rounds executed depending on the key size. The count of rounds is 10 for AES-128, 12 for AES-192 and 14 for AES-256. In each encryption round there are four processes handled. Initially the bytes in 128 bits-block of the plaintext (called as state, handled as 4x4 byte matrix and plaintext is placed as column vise) is replaced with some other byte alternative by using a predefined S-Box. Following the substitution, rows are circular-shifted to the left by row index count (Row index 0 is not shifted, index 1 is shifted 1 byte, index 2 is shifted 2 bytes and index 3 is shifted 3 bytes). After shifting the rows state matrix is multiplied with a MixColumn matrix (see Figure 3). Finally, state matrix is xored with the round key which is derived from the initial key by key generation sequence. The processes in one round of AES encryption is shown in Figure 3. The decryption steps follow the same processes but in reverse order.

Since there are 10 rounds to be executed in the minimum (AES-128) in AES encryption and the key size is not satisfactory for providing a different sub-key to each round, a key expansion process is used. Initial key (16 bytes) is represented as a 4x4 byte matrix. Key bytes are placed in the matrix as column vise and this matrix is the sub-key for the first add-round key operation. But in AES-128 there needs to be 10 sub keys (12 for AES-192, 14 for AES-256) generated from the initial one, given that the there is an additional add-round key operation before the rounds. In order to generate a 128 bits of a sub-key for the following round, initial key matrix is handled column by column. When generating the next four columns the first column (actually the 5th column starting with the initial key columns) is calculated by using a *g* (generator) function which inputs the last column (column 4) in the previous sub-key state. The details for function *g* is shown in Figure 4. The output of the function *g* is xored with the first column of the previous state to obtain the first column of the next sub-key. Generation of following three next-state columns is relatively simple when compared with the first one. Each new column is the xor of the columns just one and three previous ones. This generation steps are repeated 10, 12 and 14 times with respect to AES-128,192 and 256.

5. PROPOSED ENCRYPTION ALGORITHM

Our proposal encryption/decryption algorithm is fundamentally a block encryption algorithm. Since the proposal is based on the fundamentals of AES encryption and makes use of AES key generation process without modification, we call it chaos based AES (CB-AES). The encryption process of AES is modified to include ACM permutation but the key expansion is used as it is in AES.

First two steps (SubBytes and ShiftRows) in AES encryption round are removed while the last two (MixColumns and AddRoundkey) steps are preserved in CB-AES. ACM permutation is inserted as the first operation before the MixColumns and AddRoundKey steps in the encryption round. Hence there are three steps in CB-AES encryption/decryption round. Three steps of CB-AES encryption are shown in Figure 5.

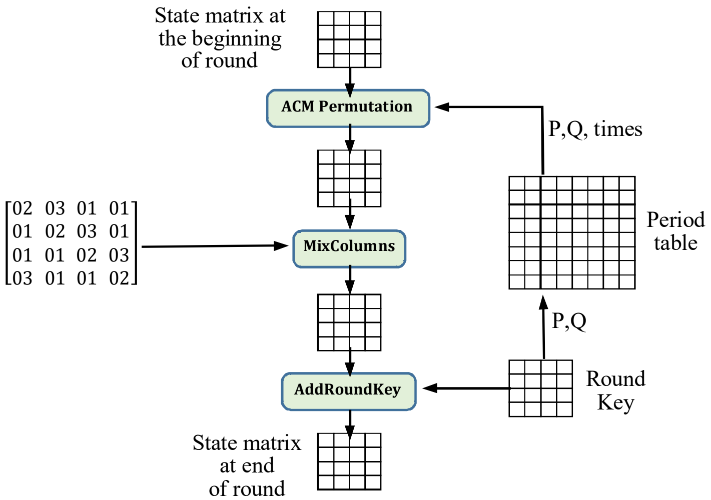


Figure 5. *Three steps in on round of CB-AES*

As it is the case in AES the plaintext block size is 128 bits (16 bytes) and mapped into a 4x4 byte matrix called state. The first step in CB-AES is the ACM permutation. ACM permutation is conducted on bit level in CB-AES. So that N is always 128. In order to conduct an ACM permutation, three parameters need to be identified. These three parameters are P, Q values and the number of iterations to be conducted.

Given that N is fixed as 128 and P, Q can take integer values between 1 and 128, the ACM period for unique values of P and Q can be pre-calculated and stored in a lookup-table which is called Period Table. Thus when P and Q are known the period of ACM permutation can be read from the Period Table.

P and Q values for the multiplicand matrix are derived from the round key. First seven bits of the round key specify P and following seven bits specify Q. When P and Q are specified the ACM period can be read from the Period Table and this period value is used to specify the iteration count (referred as "times" in Figure 5) to be conducted in ACM permutation. Specification of ACM iteration count is shown in (3)

$$times = \lfloor Period/2 \rfloor \text{ where } \lfloor x/y \rfloor = (x - x \bmod y) \,/\, y \tag{3}$$

This simply means that in each encryption round different P and Q values and therefore different times count would be used in ACM permutation, since the round key would be different in each round of encryption.

Following two steps in encryption round is identical with that of in AES.

In decryption phase, all the steps should be conducted in reverse order. AddRoundkey and inverse MixColumn would be conducted as it is in AES decryption. But in inverse ACM permutation there are mathematically two alternatives. Either multiplying the state matrix by "times" round with inverse of multiplicand matrix which is specified by P and Q or executing ACM permutation by complement-times where complement_times is specified by (4). For the re-usage of ACM permutation but with different input values we recommend the later choice.

$$Coplement\_times = times - \lfloor Period/2 \rfloor \text{ where } \lfloor x/y \rfloor = (x - x \bmod y) \,/\, y \tag{4}$$

6. CONCLUSIONS

In this study we presented a chaos based encryption modification to standard AES algorithm. Our intention is to increase complexity and diffusion by having a chaotic calculation to each encryption round. Bit vise permutation characteristic of proposed ACM permutation would meet the byte-substitution step functionality in a more complex manner, since in AES SubBytes step substitution is static for a given byte alternative in each round but in CB-AES identical bytes in two different rounds would be replaced by discrete byte alternatives depending on the round-key.

In the follow-up studies we are to carry out the tests that are given below on the proposed algorithm and the results will be compared that of standard AES and well-known cryptographic algorithms.

- Plaintext bit avalanche effect test
- Key bit avalanche effect test
- Known/selected plaintext attack
- Known/selected ciphertext attack
- Ciphertext only attack

6. REFERENCES

[1] Kocarev, Ljupco, and Shiguo Lian, eds. Chaos-based cryptography: Theory, algorithms and applications. Vol. 354. Springer, 2011.

[2] Stallings, William, and Mohit P. Tahiliani. Cryptography and network security: principles and practice. Vol. 6. London: Pearson, 2014.

[3] Borel, Armand, and Nolan R. Wallach. Continuous cohomology, discrete subgroups, and representations of reductive groups. Vol. 67. American Mathematical Soc., 2013.

[4] L. Shujun, M. Xuanqin, and C. Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in Progress in Cryptology —INDOCRYPT 2001, vol. 2247 of Lecture Notes in Computer Science, pp. 316–329, 2001.

[5] Soleymani, Ali, Md Jan Nordin, and Elankovan Sundararajan. "A chaotic cryptosystem for images based on Henon and Arnold cat map." The Scientific World Journal 2014 (2014).

[6] Z. Zhu, W. Zhang, K. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, vol. 181, no. 6, pp. 1171–1186, 2011.

[7] S.-J. Xu, X.-B. Chen, R. Zhang, Y.-X. Yang, and Y.-C. Guo, "An improved chaotic cryptosystem based on circular bit shift and XOR operations," Physics Letters A, vol. 376, no. 10-11, pp. 1003–1010, 2012.

[8] Z. Zhang and T. Cao, "A chaos-based image encryption scheme with confusion- diffusion architecture," Communications in Computer and Information Science, vol. 152, no. 1, pp. 258–263, 2011.

[9] C. Fu, B. Lin,Y.Miao, X. Liu, and J.Chen, "Anovel chaos-based bit-level permutation scheme for digital image encryption", Optics Communications, vol. 284, no. 23, pp. 5415–5423, 2011.

[10] Y. Zhang, P. Xu, and L. Xiang, "Research of image encryption algorithm based on chaotic magic square," Advances in Intelligent and Soft Computing, vol. 149, no. 2, pp. 103–109, 2012.

[11] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," Signal Processing: Image Communication, vol. 29, no. 5, pp. 618–627, 2014.

[12] A. M. Elshamy, A. N. Z. Rashed, A. E. A. Mohamed et al., "Optical image encryption based on chaotic baker map and double random phase encoding," Journal of Lightwave Technology, vol. 31, no. 15, pp. 2533–2539, 2013.

[13] R. Ye and W. Zhou, "An image encryption scheme based on 2D tent map and coupled map lattice," International Journal of Information and Communication Technology Research, vol. 1, pp. 344–348, 2011.

[14] R. Ye and W. Zhou, "A chaos-based image encryption scheme using 3D skew tent map and coupledmap lattice," International Journal of Computer Network and Information Security, vol. 4, pp. 38–44, 2012.

[15] X. Wang, F. Chen, and T. Wang, "A new compound mode of confusion and diffusion for block encryption of image based on chaos," Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 9, pp. 2479–2485, 2010.

[16] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos based image-encryption and compression algorithm," Journal of Electrical and Computer Engineering, vol. 2012, Article ID 179693, 11 pages, 2012.

[17] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution diffusion based image cipher using chaotic standard and logistic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 14, no. 7, pp. 3056–3075, 2009.

[18] K. Wong, B. S. Kwok, and W. Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters, Section A: General, Atomic and Solid State Physics, vol. 372, no. 15, pp. 2645–2652, 2008.

[19] C. Guanghuia, H. Kai, Z. Yizhi, Z. Jun, and Z. Xing, "Chaotic image encryption based on running-key related to plaintext", The Scientific World Journal, vol. 2014, Article ID 490179, 9 pages, 2014.

[20] Q. Zhang, X. Xue, and X. Wei, "A novel image encryption algorithm based on DNA subsequence operation", The Scientific World Journal, vol. 2012,Article ID 286741, 10 pages, 2012.

[21] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3D chaotic cat map", in Proceedings of the 9th International Conference for Young Computer Scientists (ICYCS '08), pp. 3016–3021, November 2008.

[22] Z.Guan, F. Huang, andW.Guan, "Chaos-based image encryption algorithm", Physics Letters A: General, Atomic and Solid State Physics, vol. 346, no. 1–3, pp. 153–157, 2005.

[23] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," Chaos, Solitons and Fractals, vol. 40, no. 5, pp. 2191–2199, 2009.

[24] J. Chen, Z. Zhu, C. Fu, H. Yu, and L. Zhang, “A fast chaos based image encryption scheme with a dynamic state variables selection mechanism,” Communications in Nonlinear Science and Numerical Simulation, 2014.

[25] J.P. Keating. Asymptotic properties of the periodic orbits of the cat. Nonlinearity, 4:277–307, 1991.