ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

AVK based Cryptosystem and Recent Directions Towards Cryptanalysis☆

Shaligram Prajapat[1*] Ashok Sharma[2] Ramjeevan Singh Thakur[1]

ABSTRACT

Cryptanalysis is very important step for auditing and checking strength of any cryptosystem. Some of these cryptosystem ensures confidentiality and security of large information exchange from source to destination using symmetric key cryptography. The cryptanalyst investigates the strengths and identifies weakness key as well as enciphering algorithm. With increase in key size the time and effort required to guess the correct key increases so trend is increase key size from 8, 16, 24, 32, 56, 64, 128 and 256 bits to strengthen the cryptosystem and thus algorithm continues without compromise on the cost of time and computation. Automatic Variable Key (AVK) approach is an alternative to the approach of fixing up key size and adding security level with key variability adds new dimension in the development of secure cryptosystem. Likewise, whenever any new cryptographic method is invented to replace per-existing vulnerable cryptographic method, its deep analysis from all perspectives (Hacker / Cryptanalyst as well as User) is desirable and proper study and evaluation of its performance is must. This work investigates AVK based cryptic techniques, in future to exploit benefits of advances in computational methods like ANN, GA, SI etc. These techniques for cryptanalysis are changing drastically to reduce cryptographic complexity. In this paper a detailed survey and direction of development work has been conducted. The work compares these new methods with state of art approaches and presents future scope and direction from the cryptic mining perspectives.

☞ keyword : Automatic Variable Key (AVK), cryptanalysis,Hacker, AI, Genetic Algorithm,Swarm Intelligence, cipher, neural network, cryptography,Artificial neural Networks (ANN), Genetic Algorithm (GA),Swarm Intelligence (SI).

1. Introduction

Information Security is definitely not a very new born concept. The people who grew up in internet age generally have a broad experience in information technology, computer science and information assurance, Which enables them to have a richer perspective that empowers them to think outside the information defense black box and look at attack patterns and threat similarities. But the people who were born before the internet age, most of the times find it difficult to view information security in context of bits and bytes. In planning of efficient cryptosystem against attackers, this perspective is very important [1, 2].

Fig. 1. Information Security and possible attacks [1] (a) Attack on Availability (b) Attack on Confidentiality (c) Attack on Integrity and (d) Attack on Authenticity

The framework of information security is presented in Figure 1.It provides broad overview of environment of information security and cryptosystem .The outer layers is concerned user,

[1] Dept. of Computer Application and Mathematics, MANIT Bhopal, India
[2] BU Bhopal, India
* Corresponding author (haligram.prajapat@acm.org)
[Received 9 May 2016, Reviewed 24 May 2016, Accepted 15 June 2016]
☆ A preliminary version of this paper was presented at ICONI 2015 and was selected as an outstanding paper.

organization and physical level of security. The central part focuses on set of algorithms and procedures essential for ensuring (a) availability (b) confidentiality (c) integrity and (d) authenticity of information [1, 2, 3]. There is a strong need and will always be, for efficient and optimum cryptic algorithms to support this structure. This is the reason which motivated us for exploring approaches of cryptosystem and symmetric key based approaches in particular.

Continuous technological advancement influences in the security by cryptosystem and prevention against learning attacks, improving key size, Key generation schemes and exchange using parameters. In the process of improvement of cryptosystem, attackers and security experts several approaches have been presented in Table 1. This Table shows work has been carried out in this direction. Machine learning, ANN based system, Genetic Algorithms etc. over the traditional disciplines of fixed key having longer and longer size to ensure confidentiality, integrity and availability of information .The recent strategy is Automatic Variable Key (AVK approach) where session wise key is used for information exchange. In the subsequent sections of this paper study has been done on this alternative style of information exchange.

Table 1. Possible Domain for cryptanalyst

S.No.	Criteria or tool for securing information
1.	Applied Technique: ANN, KNN, SVM, Decision tree, GA, Fuzzy logic (classification, clustering and association)
2.	Used algorithm: AES,DES, Blowfish,Vigenere ciphers
3.	Nature of Key : Symmetric (Private),Asymmetric (Public), No Key
4.	Mathematical operations :key based multiple Huffman tables, Tree parity machine, Interpolation (Polynomial, fuzzy), Reversible non-XOR operator

This study of AVK based cryptosystem will help researchers to identify the nature of research work that has been done so far and to develop and extend it further in the theoretical as well as possible applied cryptic mining domain. This work will highlight the AVK process and significance of AVK cryptosystem. Self explanatory diagrams and charts will save researcher's time for quick reference. Further, this work can be enhanced and updated with identified AVK based cryptosystem and Cryptic mining directions.

2. BACKGROUND FOR CRYPTANALYSIS

A **cryptosystem** "S" is a 7-tuple: S = (M, C, K_d, K_e, F, and E, D) Where:

M = Set of all possible **plaintext** m i.e. M= {m_1, m_2 .....}. Each message mi is the text to be encrypted (plaintext) and usually written in the lowercase alphabet: M = {a, b, c⋯ x, y, z}.

C = Set of all possible **cipher text** c i.e. C= {c_1, c_2.....}.Each encrypted message (cipher text) c_i is usually written in uppercase alphabet: C = {A, B, C⋯ X, Y, Z}.

K_d= Set of all possible **decryption key k** i.e. K_d= { k_1, k_2,....}

K_e=Set of all possible **encryption key k'** i.e. K_d= { k1 ',k2 ',....}.

F: K_d→Ke is a mapping from decryption key with corresponding encryption key. For Symmetric Cryptosystem **K_d** = K_e and F = I (Enciphering and deciphering keys are same.)

E is the mapping E: K_e→(M→C) that maps encrypting keys K_e into encrypting relations EKe:M→C. Each E_{Ke} must be total and invertible, but need not be a deterministic function or onto.

D: K→(C→M) is the mapping that maps decrypting keys k into decrypting functions d_k:C→M. Each dk must be a deterministic function and onto. E and D are related in that

K_e = F (k)⊂D (k) =d_k = e_{ke}^{-1} = E $(k_e)^{-1}$

m = $D_{[k]}$ (E [F ($k_{j]}$ (M)) Often e_{ke} are one to one and onto.

Cryptogram: A segment (word) of cipher text of length 1...n

Cryptographic Algorithms: The procedure that transforms messages (or plaintext) into cryptograms (or cipher text) and vice-versa.

Key Space: The set of possible keys K is called the key-space.

Key Size: It is the number of bits taken by key to transform the message M into Cipher C. Length of key decides the strength of cryptosystem. As the key length used by cryptosystem is increased the processing time and efforts needed to guess the actual key increases For example 8 bit long key contains 256 possibilities. A systematic attempt for exploring this key is polynomial time feasible, but the number of possible keys increases exponentially with the key size. For a 56-bit key containing 2^{56} possible keys. A cryptanalyst or hacker tries one

million keys per second would take approx 2284 years to try. Similarly for 64 bits with 2^{64} possibilities he would take 5.85x105 years. With the development of multi another approach of advancement in cryptography is Automatic variable key approach, the cipher generated from this approach are through dynamic keys that keeps changing from session to session.

some variety of techniques(such as Fibonacci Q and Sparse Matrix) and it's analysis from hackers and cryptanalyst perspective is available in [8,10,14,16,18].from the perspective of Cryptic mining, The clustering and classification of ciphers is to be investigated from ANN,BBN and its variants.

The special purpose of data mining techniques concerned with extraction of knowledge used by any cryptosystem for exchanging business, scientific and commercial information exchange prepares basis for "Cryptic Mining" domain. *Cryptic Mining* can be defined as a class of mining algorithms used specially for auditing of a cryptosystem for measuring the degree, strength and weakness of constituent algorithms, and to decide the class of algorithm to which it belongs. It includes dedicated and specialized algorithms for mining on binary data, log of cipher text and output of any cryptosystem. For the low level information set, cryptic mining for symmetric key based information exchange with shared, parameterized and session wise keys, increases the security level of cryptosystem. It scrutinizes the system with perception of hackers and cryptanalytic for identification to strengthen the system. The AVK framework and cryptic mining attempts is elucidated in Fig. 2.

Cryptic mining domain can be understood as a collection of techniques the extended traditional mining technique for the extraction of useful patterns and discovery of key size and strength of algorithms. Although, it is assumed that ciphers are 100% random in nature, but in practice it is not so, There may be some patterns generated in cipher-text, input plain-text, keys used to encipher it etc, The patterns stored in stored files or flowing in the network can be used to exploit and harness the weakness in the process using cryptic mining algorithms. For example, using the longest common cipher pattern problem is to find the bit pattern which is common [9]. It is the bit string (or bit strings) of length two or more bits. For given two strings, C_i of length m and C_j of length n, find the longest bit strings which are substrings of both C_i and C_j.For length k-common cipher problem, with two cipher text, C_i of length m and C_j of length n, the cryptanalyst may be interested in finding the common bit sequence or bit strings that are present in both C_i and C_j.

Given the set of cipher texts C={C_1,C2,⋯Ck}, where $|C_i|=n_i$ and $\sum n_i=N$.i.e. they are intended to find for each $2 \le k \le K$, the longest cipher bit-strings which occur as substrings of at least k strings. The lengths and starting positions of the longest common cipher pattern of C_i and C_j can be found in time $\theta(n+m)$ with the suffix-tree and in $\theta(N*K)$ using dynamic programming. For elucidation, consider the cipher text strings C_i = 0 1 0 1 and C_j = 1 0 1 0 .

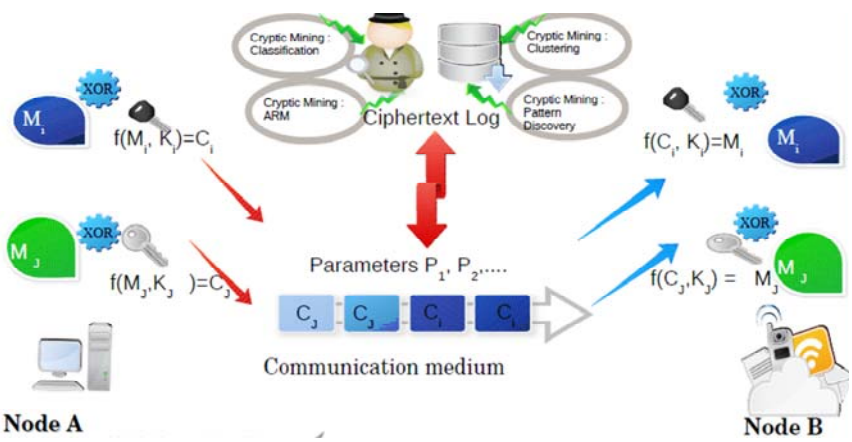
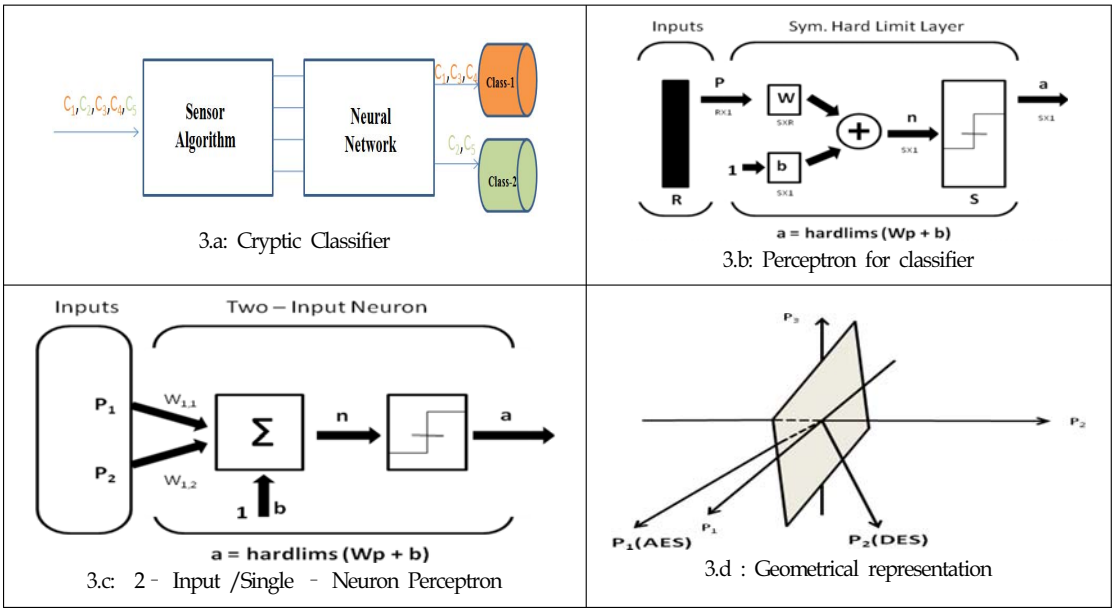


Fig. 2. A framework for AVK Cryptosystem and Cryptic Mining



3.a: Cryptic Classifier

3.b: Perceptron for classifier

3.c: 2 - Input /Single - Neuron Perceptron

3.d : Geometrical representation

Fig. 3. A framework for Cryptic Classification using ANN

Cryptic Classification: A set of algorithms Useful in detecting class of enciphering algorithms, cipher-type, Key size are candidate of this set. Specialized scanners or sensors algorithms will decide the nature and class of algorithm. The easily classified ciphers exhibit weakness of the cryptic algorithm. ANN based classifier (Fig. 3) , Bayesian Belief Network, Decision trees etc may be useful for this task.

Cryptic Clustering: Depending upon similarity among ciphers, plain text-cipher text patterns these set of cryptic mining algorithm groups the ciphered for extracting the knowledge from pattern of the groups and general behavior analysis of input. Agglomerative Clustering, KNN, and vector space clustering tools are beneficial for the task. The work of Oliviera, José and Carlos is useful to demonstrate how clustering of ciphers can help in key size determination and categorization of ciphers [7].

Cryptic Association Rule: Individual cipher blocks or chunks may have association among cipher-cipher, plain text-cipher text, or plain-text, session key. These set of cryptic mining algorithm extracts rule base or association rules for associating certain simple or parameterized cryptosystem based relationships together with (plain-text, cipher-text) paired associations. Cryptic association rule discovery may be useful to find association rules to identify relationships or association among keys (or a part of key as parameters) generated in multiple sessions and dependencies to explore the frequency patterns of key construction using parameters. Normally, one key often goes without other key, but their generation may have a certain association due to some formula or mechanism of key generation. In [25], focus is given on Cryptic Association Rule Mining to analyze the strength of symmetric Cryptosystem.

Pattern Discovery: These set of cryptic mining algorithm works as scanners and input supplied them for probability analysis tools like Markov model, ANN, GA, ACO etc. These cryptic mining techniques finds applications in detecting behavior of malware, ad-ware analysis, classes of attacks using honey-pot and honey-net systems.

2.1 Cryptic Classification using ANN

Enabling Cryptanalyst with ANN for classification of cipher text generated through several cryptic algorithms in polynomial time is desirable aspect of cryptic classifier. He is interested to mine useful guess for detecting full or part of original information or about key. From huge captured log containing variety of ciphers and hash files. Whenever a cipher appears

into this dataset, it may be mixed within other ciphers generated from various other schemes including variations in key size, protocol, type of ciphers generation algorithm, degree of exposures of information about key space and many other information related to plaintext, cipher text, relationship between them. The cryptanalyst may develop a mechanism that will classify/sort/ group according to cipher type. One such method is demonstrated in Fig.3. (a) A scanner algorithm may be developed which measures three properties of ciphers; x, y, and z. If the cipher or key is generated with contribution with parameter-1 then it outputs 1 else -1(if it is not through x).

The sensor algorithm will output 1corresponding to second parameter y if it is through y. Similarly, sensor algorithm will work for parameter z. The three output of sensor will be input to neural network. This neural network (classifier) will decide which kind of cipher is in the database, so that the cipher can be directed to the correct class. Consider a model for classifying minimal two types of class say class-1(For AES: C_1, C3, C4) and class-2(For DES C2,C5). (Fig 3.d)There are only two kinds of ciphers in the captured-database-log. As each cipher passes through the sensor it can be represented by 3-D vector of parameter set P = [x y z]. The output prototype for class-1 is [1 -1 -1] and output for class-2 will be [1 1 -1].

The neural network will receive one 3D input for each cipher from captured log and makes a decision to whether the cipher is from class-1 or of class-2. A simplified single layer perception (Fig. 3.b and 3.c) can be depicted to solve it. The output of perceptron must be 1 when a cipher of class-1 is input and -1 when cipher of class-2 is supplied as input.

$$a = \text{hardlims}([w_{1,1} \quad w_{1,2} \quad w_{1,3}] * [x \quad y \quad z]^t + b)$$

The choice of bias b and the elements of weight matrix is such that the perceptron will be able to correctly distinguish ciphers of class-1 and class-2. Linear separator that can separate ciphers of class-1 and class-2 can be pictorially denoted by XZ-plane and acts as decision boundary with equation Y = 0.

$$[0 \quad 1 \quad 0]*[x \quad y \quad z]^t + 0 = 0$$

The weight matrix w =[0 1 0] and bias will be b=0. w is orthogonal to the decision boundary and points towards the region that contains the prototype patter of class-1 for perceptron o/p of 1.As the decision boundary passes through origin so bias = 0. Y= 0.Thus,

$$[0 \quad 1 \quad 0]*[x \quad y \quad z]^t + 0 = 0$$

Testing of perceptron based classifier can be done as follows. As this classifies ciphers of class-1 and class-2 correctly:

For class-1{C_1,C3,C4}

$$a = \text{hardlims}([0 \quad 1 \quad 0]*[1 \quad 1 \quad -1]^t + 0) = 1$$

For class-2 {C_2,C5}

$$a = \text{hardlims}([0 \quad 1 \quad 0]*[1 \quad -1 \quad -1]^t + 0) = -1$$

if any non distinguishable cipher is supplied as input to the classifier (Cipher with confusing pattern) may be of class-1 or class-2 through the output of sensor with i/p vector = $[-1 \quad -1 \quad -1]^t$

$$a = \text{hardlims} ([0 \quad 1 \quad 0]*[-1 \quad -1 \quad -1]^t + 0) = -1 \text{ (class-2)}$$

Any input cipher that is closer to class-2 with respect to class-1 will be classified as a member of class-2, and vice versa. Thus perceptron based cipher classifier may separate cipher patterns with linear decision boundary. The issues with the approach need deep digging for higher dimension and learning of algorithm. Also complexity will also increase when ciphers cannot be separated by linear boundary. The next section provides detailed survey conducted for finding out alternative approaches like multilayer perception and others. Apart from this perception model numerous other techniques are also in the existence. Next section will illustrate them briefly.

2.2 Extracting association rules in variability concept of key n secured transmission

In AVK approach key or its parameters are to be shared over session to session. These Key may be permutation in received data. If, In 5 applications key k appears 3 times then probability of key =3/5.Let contribution factor of key K_1 (CF) = m/n where m<= n and CF = Contribution Factor .For Example

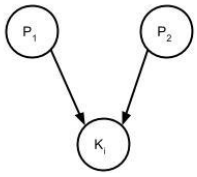
Table 2. Application wise session keys with parameters for AVK

Application	Parameters	Key
A_1	p_1, p_2	K_1, K_2
A_2	p_2, p_3, p_4	K_2, K_3, K_4
A_3	p_1, p_2, p_5	K_1, K_2, K_5
A_4	p_1, p_5	K_1, K_5

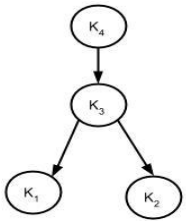
Then K_1=3/5, K2=3/4, K3=1/4, K4=1/4, K_5=2/4=1/2,After having above information sets our aim is to investigate An = ? Since $f(k_1)$,$f(k_2)$> Threshold value 0.5 so these keys K1 and K2 are frequent fuzzy range, due to tendency towards higher crisp value side. Also $f(k_3)$, $f(k_4)$ < Threshold value 0.5 then keys K_3 and K4 are in rare fuzzy range, as they are more nearer towards lower crisp boundary. Variability of key on the basis of above combination, i.e. by applying trend analysis stored in the data bases of Transmitter and Receivers, most probable key can be predicted. Thus weakness of the system can be identified.

2.3 Inference of parameter or key information using BBN

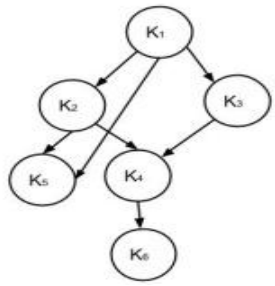
A Bayesian belief network (BBN) pictorially represents probability relationships or directed dependencies on nodes. It is a set of parameters used to construct new key based on past probabilities. Using directed acyclic graph it shows dependency relationships among parameters of key computation, a Table with probability value has been associated with each vertex from its immediate parent nodes. For illustration we Consider 3 random key parameters P_1, P_2 and P_3 corresponding to sessions of symmetric key based cryptosystem, say S_1, S_2 and S_3. In these parameterized key sets P_1 and P_2 are independent parameter variables and each has a direct influence on the key K_i(Due to some common or shared parameters, we will interchangeably use node-label P_i with K_j).The relationship among the parameters can be demonstrated in acyclic graph.



A) Key computation from parameter



B) Acyclic key dependencies (based on parameters)



C) Session keys with parametric dependencies

Fig. 4. A Bayesian belief network for dependencies of session keys

In Fig. 3.a, each parameter in the graph has relationships in the form of directed edge. Since there is a directed edge from P_1 to K_i or P_2 to K_i the P_1 is the parent of K_i and K_i is also child of P_2. In Fig. 3.b, directed acyclic graph key K_1 is descendant of K_4 and K_4 is ancestor of K_2. Conditional Independence Rule: Since a vertex in a Bayesian network is conditionally independent of its non-descendant, if it's parents are known. So, in the Fig. b K_1 is conditionally independent of both K_2 and K_4 for given value of K_3 because vertex K_2 and k_4 are non descendants of node K_1. In Fig. 3.c

The Bayesian-Belief-Network (BBN) representation for uncertain parameter-based dependencies are manifested by observations made earlier (from log of captured information). Considering the key space K = {K_1, K_2, K_3, K_4, K_5, K_6}

Premises are:

K_2, K_3 are derived from K_1 .

K_4 is derived from K_2 and K_3 both.

K_5 is derived from K_1 and K_2 both.

K_6 is derived from K_4.

Using Bayesian Belief Key Network a node represents the keys K_i (where i =1 to 6), connected by dependency arcs influences or parameter dependencies among the keys. The strength of the influencing parameter (parameter) is quantified by conditional probabilities of occurrence of each key. The resultant Joint-probability of the keys will be given by:

$P(K_1,K2,\cdots K_6) = P(K_6 \mid K_4)\, P(K_5 \mid K_2,K_1)\, P(K_4 \mid K_2,K_3) P(K_3 \mid K_1)\, P(K_2 \mid K_1)\, P(K_1)$

Thus decision making process from Bayesian belief network approach will requires two steps verification process. 1. Creating Belief Network or structure and 2. Computation of probability values corresponding to each node.

3. RELATED WORK FOR AVK CRYPTOSYSTEM

In Fig. 3 elucidation of available techniques and literature referring to state of art approaches are available for analysis of cipher-text and mining useful patterns following are some significant work and brief insights of the technology used.

In [1] C.T. Bhunia, The pioneer in AVK based cryptosystem and team have presented schemes of generation and checking of AVK under Various Approaches. They established the fact that AVK is one of the finest approach for achieving the perfect security cryptology.

In [2], some approach towards Generation of AVK to Achieve Perfect Security with simple computation has been presented with exploitation of randomness among the successive two keys.

In [3] AVK with chaos theory has been presented where it is not necessary to exchange the subsequent session key in next sessions (Except the first session). Their conclusion was that the least differential attack was in case of cipher with AVK with chaos theory.

In [4] some protocols of AVK particularly (CSAVK, DSAVK, XOR) have been investigated .They found it to reduced brute force attack, frequency attack and differential frequency attack. They have pointed out the issue that initial key that may be exchanged by any conventional secret mode could be risky.

In [5], some methods towards Optimum data transfer with AVK Techniques have been discussed. They claimed to achieve Perfect Security with Analysis and Comparison. They recommended that instead of sending one key, they proposed to send three keys components. And perform bit-wise logic operation among these three keys components to agree upon to the first key. (RMS of AVK, CSAVK, ASAVK, DSAVK, PROTOCOL-I, PROTOCOL-II and ROTOCOL-III).The new approach of initial key fixation by majority logic provides a confidence of application of AVK cryptology.

In [6] a method of enhancing security level using AVK in case of Vernum Theory on ECB mode of DES and AES have been presented. They have highlighted the advantage of AVK in maintaining security level, if any relation occurs during encryption thereby decreasing security level thereby eliminating any scope of occurrence of diffusion or confusion.

AVK approach is not limited to symmetric key only .For Public key it may be useful also. In [7], RSA- Singular Cubic Curve with AVK has been presented. They found that, it reduces processing time and time complexity (thereby increased speed of encryption).They found it's applicability in high level security application domain where exhaustive set of security parameters may occur.

In [9], Key variability of moving object (sender or receiver) can be archived by using location parameters of object. These location parameters will be used to compute linear, quadratic or cubic key depending upon the requirements.

Key variability can be achieved by using terms of natural Fibonacci sequence [10]. Using a Q-matrix (order 2 X 2) key of decipherment process can be created, that is post multiplied with the message (Converted into ASCII numerical values of size p x 2).The product will generate cipher text ready for transmission. The inverse of Q matrix post multiplied with ciphered matrix will provide plain text information .over the session with different sequence terms f(n-1),f(n),f(n+1) new Q-matrix can be generated by both sender and receiver. In this way AVK process can implemented. The python implementation of [10] has been presented with analysis of Fibonacci-Q algorithm.

In the time variant key work of Prasun [11, 12], numerous curves based cryptic techniques have been presented to demonstrate alternative ways of creating keys. He also proposed the schema of transmitting parameters over the channel for computation of AVK. He wisely presented schemes and analyzed well from hackers perspectives.

Cost of key distribution plays central role in deciding performance of the system. In [13], Pickard and team have present a dynamic set key method of randomized provisioning which can be used to lower the cost of key distribution Cryptography.

AVK approach relies on fixing up key size and varies it over session to session. But choosing the key size is a challenging task, key size less then threshold is risky and higher key size is wastage of resources. In [16], Optimal key Size for AVK based cryptosystem has been discussed and it was concluded that the key length from 6 to 8 byte is sufficient for a session.

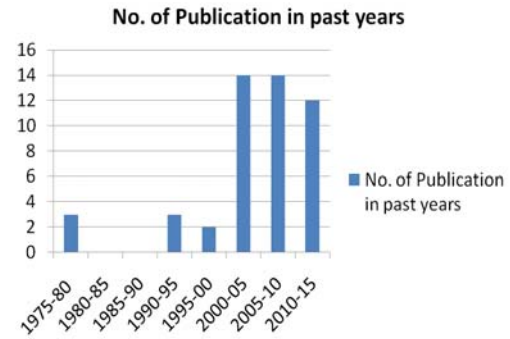
The Success of AVK based cryptosystem is ensured only after its implementation and testing against attacks. In [17] Association rules for variability of key using parameterized approach have been constructed for prediction of future parameters for construction of key from hacker's perspectives. In [18], the cryptic algorithm developed from Fibonacci-Q matrix [10, 14, 15] under various situations say hacker is interested to mine future keys, future key sequences, and probable steady state situation using Markov process. The stochastic analysis and future recommendations for ensuring security is presented in [18, 20].

A number of states of cryptic algorithms are available in the literature for symmetric key approach. To compare, analyze and investigate efficient algorithm various tools and online resources are available. SGcrypter is one online tool in this direction[21].Although it works fine for conventional approaches but SGcrypter tool needs more improvement to compare and analyze the efficiency of AVK based cryptic algorithm other than traditional one.

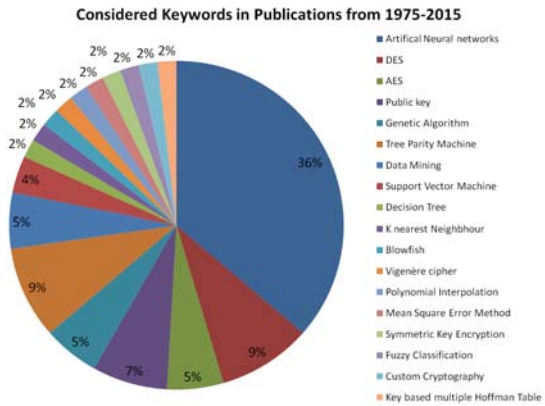
For auditing and testing of effective and efficient cryptosystem, the automated application for cryptanalysis is needed. Traditionally hacker or cryptanalyst applies technique for cipher analysis according to his or her perception and expertise level.

But it is not well organized or disciplined .Cryptic Mining system with advantage of AI and advanced techniques can be developed for testing of cipher generated from such systems. In [19], automated tool based conversion of cipher text into plaintext has been attempted. The implementation has been done successfully for substitution ciphers only. The extension work is required further for incorporating other ciphers. Making such open source tool will enable one to check the strength of cryptosystem.

Apart from AVK based cryptosystem, various approaches towards cryptanalysis can be applied, but it is hard to find out which is better one and heuristics may be needed for efficient solutions. Recent survey of the conventional approaches has been demonstrated in [23]. This paper provides helpful survey and opens new dimension of cryptic mining discipline. The conventional or contemporary cryptography in work of Diffie and Hellman, They have provided a guideline for cryptic literature.



a) Some observed work in past year with count [22]



B) Tools used for cryptic process and analysis [22]

Fig. 4. Some observed work in past year with count and Tools used for cryptic process and analysis

4. FUTURE CRYPTIC MINING DIRECTION

The conceptual and logical models of secure information exchange using automatic variable key has been discussed so far. To sustain this model for satisfying future demands, the possibility of extension for future need is essential, keeping this view the symmetric cryptosystem based on AVK analysis need to be checked for cipher pattern identification, checking the association among plaintext and cipher text analysis. The possibility of learning based parameter prediction may be added as an extension to cryptic tool like Sgcrypter[21]. Fibonacci-Q based cryptic algorithm can be extended for parallel and distributed computing for large input files [10, 24, 18]. The divide and conquer approach and its impact for matrix

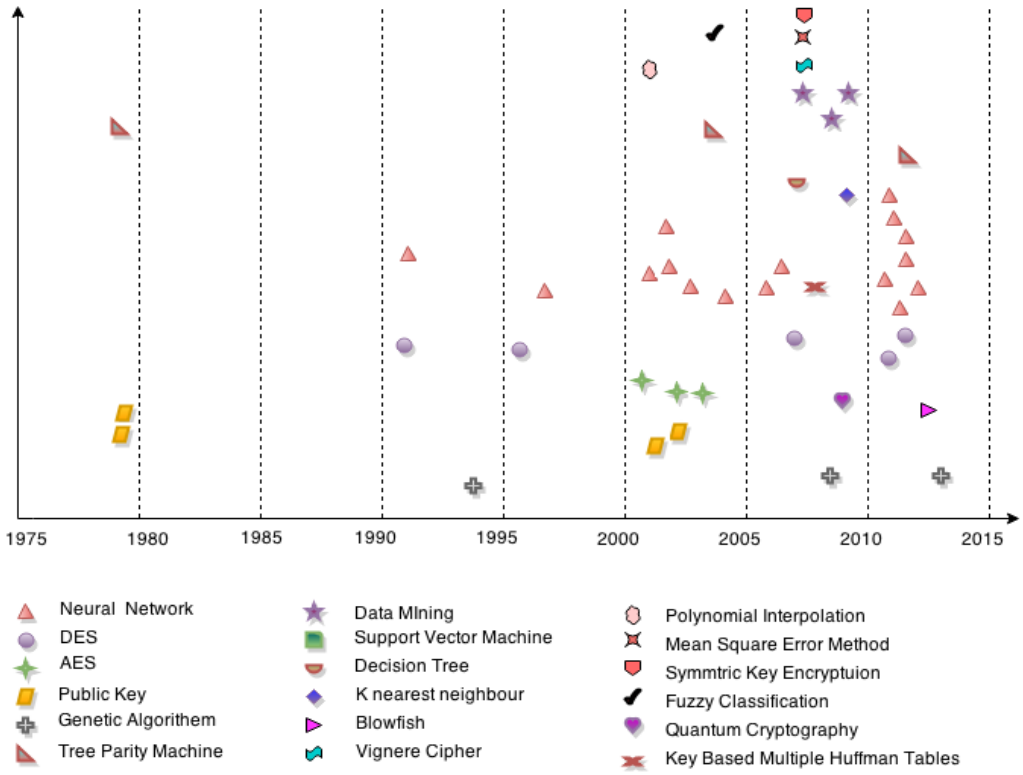


Fig. 5. Publications v/s algorithms in past years [22]

multiplication and gain in the complexity can be tested. The location information based on three dimensional co-ordinate systems can be modeled for real time secure data exchange among moving objects. The security of parametric model for fuzzy parameters and its impact on security of symmetric cryptosystem can be checked. The AVK model for multiple users and multiples keys associated with one single device at one time may be investigated, framed and implemented for analysis to ensure secure information.

The study reveals that before last two decades, the study in the field of cryptanalysis using neural network was very diminishing. But, considering the survey being done the result shows a startled growth in the same field. There are many reasons for this but it certainly shows the presence of research gap and opportunity. Table 3, shows the future scope of different paper being considered for the survey. Section 4.1, 4.2 and 4.3 will throw light from future perspectives and extensions.

4.1 AVK based cryptosystem and IOT

Recently IOT is also gaining pace, here system and Internet is connected to the physical world via “ubiquitous sensors”. The concept of communication between one device with other is not a new concept. Recently, communications among Machines also have been demonstrated with talking machines, for deployment of IOT technologies is demanding more intelligence, more complexity – into the conversation. With the development of Computational Intelligence approach, Intelligent Agent Based System seems to be the backbone and Demand of Future Technology that is capable to provide intelligent Machine to Machine conversations and IOT connectivity solutions for wireless and wired networks, for the benefits of society and Mankind. Since lightweight cryptography algorithms are demand of current and future devices. There are symmetric cryptography namely AES, DES, RC4, Blowfish, Two Fish. For enhancing security one recent

Table 3. Future Scope and research directions for ANN perspectives

No.	Paper Title	Method	Future Direction
1.	Pattern analysis of cipher text: a combined approach	Dictionary and decision tree based approach	Effective cryptanalysis for the AES algorithm
2.	Cryptography and Cryptanalysis Through Computational Intelligence	Artificial neural network	In order to find the effectiveness and efficiency of proposed cryptographic systems EC method can be used
3.	Cryptanalysis of a three rotor machine using a genetic algorithm	Genetic algorithm	Cryptography could be into the cryptanalysis of substitution-permutation systems and possible variations of the rotor machine.
4.	Fuzzy classification based on Fuzzy association rule mining	Fuzzy association rule mining	The framework can deal with not only binary and category attributes but also continuous quantitative attribute.
5.	Multiuser cryptographic techniques	Protective protocol, Public key cryptography, Public key authentication	If sender's keying information is made public then need for secure key distribution is completely eliminated.
6.	Neural Synchronization based Secret Key Exchange over Public Channels: A survey	Neural Network	The study of chaotic maps for transformation of synchronized states of the networks to chaotic encryption keys, with exceptionally low tolerance for decryption error
7.	Quantum Cryptography: A New Generation of Information Technology Security System	Cryptography, Information Security, Security of Data, optical polarization, Quantum Cryptography	Quantum cryptography is headed forwards
8.	Probabilistic attack on neural cryptography	Tree parity machine (a bi layered feed forward artificial neural network	Some experiments may be carried out so the results will be completed and safety of the cryptographic procedure.
9.	Synchronization of neural networks by mutual learning and its application to cryptography	Neural Network	Advanced algorithms for synchronization, which involve different types of chaotic synchronization, seem to be more secure. Such models are subjects of active research
10.	Applying Neural Networks for simplified data encryption standard (SDES) cipher system cryptanalysis	Neural Network	It possible to use this model with the most sophisticated cryptosystems such as public key. as well as to use search for any efficient algorithm to reduce the space search for the keys and use the results as inputs for the neural network to get the correct keys
11.	Design of an efficient neural key generation	Neural Network	The key distribution centre generated the secret key. The key distribution centre will distribute the generated key securely by some method.
12.	Security Of Neural Cryptography	Neural Network	Our understanding for the reason of the majority attack's success implies that we should be looking for algorithms where the Overlap between the attackers would develop much faster than their overlap with the parties. This might be achieved by using larger K values, or some other modifications. These models are still under consideration.
13.	Lessons in Neural Network Training : Over fitting may be harder than expected	Neural Network	Methods for creation of more parsimonious solutions, importance of the MOP/BP bias.
14.	Security of neural cryptography	Neural Network	Our understanding for the reason of the majority attack's success implies that we should be looking for algorithms where the overlap between the attackers would develop much faster than their overlap with the parties. This might be achieved by using larger K values, or some other modifications. These models are still under consideration.

trend is to increase the key length, which has an effect of increasing power and computation time. Still we don't have good candidate in Hash and symmetric key encryption function. This paper highlights the efficient way of enhancing them to be ready for new dimensions of IOT. Our work of Fibonacci-Q, Sparse approach and cryptic-mining are aligned in the extension of AVK concepts, with hacker's and cryptanalyst perspectives. Following research questions are yet to be answered:

(1) what are the scopes of AVK approaches of ensuring efficiency in IOT? Especially when heterogeneity is high like for devices with connectivity at the “edge” of networks in remote and demanding environments, using Ethernet, serial, wireless and USB communication technologies.

(2) How system would maintain reliability on operating with WSN?

(3) How system will control and manage keys in g IoT environments?

(4) How system will be designed to work robustly on deploying intelligence at the network edge? The paper also opens a new direction to think about efficient security mechanism for talking devices in IOT environment using AVK and prepares the basis for AVK based security architectures with the issues of key management scheme, including key provisioning, key updating policy or key agreement.

4.2 AVK Point Estimation based key prediction and maximum likelihood feature

For this assume X is any random key generated by stochastic random variable, and we have following snapshot of key database= {2, 4, 1, 6, 11,}.We have to use any algorithm for pseudo random number generation algorithm, let current number generated is x=8.

1. Let x=8 is random value generated by stochastic generator which is related to key.
2. Let S is the set of all possible key set sensed till now.
3. Compute modulo distance of |x - Ei | for each Ei of S and stored in set T.
4. Let t = min {T} distance of element with subscript i, so use next transmission paring with (± t, i)
5. If computed key is KP with received parameter = KP and matched key is ke Then we generate entropy of C (k_e), Generate enropy of C (k_p) and if Delta=| C (k_e)-C (k_p) | and it is less then threshold then generated key is k.

4.3 Sparse key prediction

In Sparse matrix approach where Encryption technique using sparse matrix is device in [9], the challenge is to correlate nonzero elements with key? The schema is using the position of nonzero elements represents key. It has following advantage:

1. Reduced communication time complexity and computational complexity in terms of encryption
2. The probability of distortion of data is less due to the fact that lower the key size more will be the level of security

4.4 AVK and Compression approach

Using Lossless Compression, one can study all the lossless data compression techniques and calculate the compression in quantitative form, accordingly encrypt the reduced key size and on the basis of graph analyze the estimated encryption time.

5. CONCLUSION

The paper provides research direction to all cryptography beginners who are interested or willing to add contribution in the AVK domain of cryptic mining, extending the idea to develop tools for evaluation of efficiency of a cryptosystem can be developed. Honey pot, honey net for developing offensive mechanism using pattern discovery and behavior analysis of cipher text being propagated in the communication channel. The work also provides highlights of various works going in this direction by considering the paper with survey and statistics, so one can easily identify glimpses of the work done in cryptanalysis using various techniques and algorithms. Further the reader can identify the scope about area for studies that can be carried out to enhance computational efficiency of algorithm and extension of work in that particular field. This paper just not merely list the number of research paper that have been published since decades, but also depicts the summary of those research papers to act as supplement to boost the research work in cryptanalysis. The concept of automatic variable key has been presented and the model is generalized and extended to parametric AVK model to cover broad range of parameters for key construction. The concept of AVK provides vital role in the design of secure information communication with better time efficiency as compared to algorithms that rely on increasing key size to secure information. Apart from stationary communicating parties, moving devices

and objects of wearable computing elements or IOT, location information based key exchange model has been presented. The parametric approach of AVK model can be investigated in the light of association rules.

References

[1] Prajapat Shaligram, D. Rajput, R. S. Thakur, *"Time variant approach towards symmetric key"*, In proceedings of IEEE Science and Information Conference (SAI), pp.398-405, 2013.

[2] R. S. Goswami ,S. K. Chakraborty ,A. Bhunia ,C. T. Bhunia," New Approach towards Generation of Automatic Variable Key to Achieve Perfect Security", in *Proc. of Information Technology: New Generations (ITNG),* pp. 489-491, 2013.

[3] B. Bhuyan, P. Chakrabarti, A. Chowdhuri, F. Masulli, C. T. Bhunia, " Implementation of Automatic Variable Key with Chaos Theory and Studies Thereof", *The IUP Journal of Computer Sciences*, Vol. 5(4), pp. 22-32, 2011.

[4] R.S. Goswami ,S. K. Chakraborty,A. Bhinia ,C. T. Bhunia," Various New Methods of Implementing AVK", in *Proc. of 2nd International Conference on Advances in Computer Science and Engineering*, 2013.

[5] R. S. Goswami, S. K. Chakraborty, A, b. Bhinia, C. T. Bhunia, "Approach towards Optimum Data Transfer with Various Automatic Variable Key (AVK) Techniques to Achieve Perfect Security with Analysis and Comparison", *International Journal of Computer Applications*, Vol. 82(1), 2013.

[6] P. Chakraborty, C.T. Bhunia, B. Bhuyan, "Variable Key: A new investigation in cryptography and results thereof", IJITKM, 2012.

[7] Oliveira C., José A., and Carlos A. C., "Clustering and categorization applied to cryptanalysis", Cryptologia, Vol. 30(3), pp. 266-280, 2006.

[8] H. H. Ngo, X. Wu, P. D. Le, C. Wilson, and B. Srinivasan, "Dynamic Key Cryptography and Applications", In Proc. of International Journal of Network Security, Vol. 10(3), pp. 161–174, 2010.

[9] Prajapat Shaligram, Sharma A., Swami S., Rajput D., Singroli B., R. S. Thakur, "Sparse approach for realizing AVK for Symmetric Key Encryption", *International Journal of Recent Development in Engineering and Technology* (IJRDET), Vol. 2(4), pp. 15-18, 2014.

[10] Prajapat Shaligram, A. Jain and R. S. Thakur, "A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix", *International Journal of Computer & Communication Technology (IJCCT).*

[11] A. p. Singh, S. Kumar, "A new method for generation of variable session keys", *International Journal Of Scientific Research And Education* IJSAE, Vol. 2(8), pp. 1578-1581, 2014.

[12] P. Chakrabarti, B Bhuyan, A. Chowdhuri, C.T.Bhunia, "Novel approach towards realizing optimum data transfer and Automatic Variable Key(AVK) in cryptography", *International Journal of Computer Science and Network Security*, Vol. 8(5), pp. 241-250, 2008.

[13] G. E. Pickard, R. I. Khazan, B. W. Fuller, J. A. Cooley,"DSKE: Dynamic Set Key Encryption analyze the performance of DSKE", MIT Lincoln Laboratory,244 Wood St Lexington MA, 02451,pp. 1-7, 2012.

[14] Prajapat Shaligram, Saxena S., Jain A. and Sharma P.," Implementation of Information Security with Fibonacci Q-Matrix", in proceedings of ICICS-2012 and Special Issue of IJECCE, pp. 118-124, 2012.

[15] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, "Generation of Automatic Variable Key under Various Approaches in Cryptography System", *Journal of the Institution of Engineers* (India): Series B, Vol. 94(4), pp. 215-220, 2013. http://dx.doi.org/10.1007/s40031-013-0066-8

[16] Prajapat Shaligram, R. S. Thakur, "Optimal Key Size of the AVK for Symmetric Key Encryption." In *Covenant Journal of Information & Communication Technology* , Vol.3(2), pp. 71-81, 2015 .

[17] Prajapat Shaligram, R. S. Thakur "Cryptic-Mining: Association Rules Extractions Using Session Log", In proceedings of Computational Science and Its Applications ICCSA 2015, pp. 699-711, 2015. http://dx.doi.org/10.1007/978-3-319-21410-8_53

[18] Prajapat Shaligram, R. S. Thakur. "Markov Analysis of AVK Approach of Symmetric Key Based Cryptosystem." *In proceedings of Computational Science and Its*

Applications ICCSA 2015, pp. 164-176, 2015. http://dx.doi.org/10.1007/978-3-319-21413-9_12

[19] Prajapat Shaligram, A. Thakur, K. Maheshwari and R. S.Thakur, "Cryptic Mining in Light of AI", *in proc. of International Conference On Advances In Computing, Control And Networking - ACCN 2015*, Vol. 5(2), pp. 131 – 135, 2015.

[20] Prajapat Shaligram, K. Maheshwari, A.Thakur and R.S.Thakur, "Cryptic Mining in light of Artificial Intelligence", *International Journal of Advanced Computer Science and Applications(IJACSA)*, Vol. 6(8), pp. 62-69, 2015. http://dx.doi.org/10.14569/IJACSA.2015.060808

[21] Prajapat Shaligram, G. Parmar and R. S. Thakur, "Investigation for Efficient Cryptosystem Using SGcrypter", *proc. of ICCP 2015 and IJAER*, Vol. 79(10), pp. 853-858, 2015. http://dx.doi.org/10.5120/ijca2015906518

[22] Prajapat Shaligram and R.S.Thakur, "Various approaches towards cryptanalysis", *IJCA*, Vol. 127(14),pp.15-24, October 2015.

[23] Prajapat Shaligram, R. S. Thakur, "Cryptic Mining for Automatic Variable Key Based Cryptosystem", *Elsevier Procedia Computer Science,* Vol.78, pp. 199-209, 2016. http://dx.doi.org/10.1016/j.procs.2016.02.034

[24] Prajapat Shaligram, R. S. Thakur, "Realization of information exchange with Fibo-Q based Symmetric Cryptosystem", International Journal of Computer Science and Information Security, IJCSIS, Vol. 14(2), pp. 216-223, 2016.

[25] Prajapat Shaligram, R. S. Thakur, "Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem", International Journal of Computer Science and Information Security, IJCSIS, Vol. 14(2), pp. 233-246, 2016.

[26] Prajapat Shaligram, R.S. Thakur, "Key Diffusion Approach for AVK based Cryptosystem", Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies,(ICTCS -16), 78, 2016. http://dx.doi.org/10.1145/2905055.2905288

◐ Authors ◑

Shaligram Prajapat

has received B.Sc.(Elex), M.Sc.(CS)., UGC.(NET), M.Tech.(CS), M.Phil.(CS) from Devi Ahilya University India. He is associate professor at IIPS Devi A.z University Indore. With over 15 years of teaching experience of UG and PG courses, He has reviewed five international books of Pearson education, 10 papers in reputed conferences, international journals including Springer, and Atlantis press. He has also presented paper in international and national, conferences. He is member of various professional bodies like IEEE, ISTE, ACM, CSI, CSTA, IAENG, IEEE(Computer Society),IRED.

Ashok Sharma

is Associate Professor and head, in post graduate department of computer application MIET, Jammu India. He is Educationist, Researcher and Consultant in Computer Science Information Technology. He earned M.Sc, MCA, M.Phil (Comp.Sc.). His areas of interest include Data Mining, Data Warehousing, Web Mining, and Cloud Computing.

Dr. R. S. Thakur

is Associate Professor in MANIT, India. He is Educationist, Researcher and Consultant in Computer Science and Information Technology. He earned MCA, M.Tech, Ph.D. (Comp.Sc.). He has published more than 75 Research Paper in National, International, Journals and Conferences. He has visited several Universities in USA, Hong Kong, Iran, China, Thailand, Malaysia, and Singapore. His areas of interest include Data Mining, Data Warehousing, Web Mining, Text Mining, and Natural Language Processing. He has received DST Young Scientist Award-2011 in Engineering under Fast Track Scheme, Department of Science & Technology, New Delhi, India.i