ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics and Information Engineering

Vol. 8, No. 1 (Mar. 2018)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 8, No. 1 (Mar. 1, 2018)

Mobile Ad-Hoc Clustering Using Inclusive Particle Swarm Optimization Algorithm

Anurag Rana, Deepali Sharma
(Corresponding author: Anurag Rana)

Department of Computer Science and Engineering, Arni University, India
(Email: anuragrana.anu@gmail.com)
(Received Mar. 7, 2015; revised and accepted June 22, 2017)

Abstract

Mobile ad-hoc network consists of dynamic nodes that communicate with each without base station. In this paper, we propose an inclusive particles swarm optimization clustering algorithm for mobile ad hoc networks. It has ability to find the optimal or near optimal number of cluster to efficiently manage the resources of network. The cluster heads do the job of routing network packets within the cluster or to the node of other clusters. Proposed IPSOA clustering algorithm takes into consideration the transmission power, ideal degree, mobility of nodes and battery power consumption of the mobile nodes. Weighted clustering algorithm assign a weight to each of this parameter of network and each particle of swarm contain information about the cluster heads and the member of each cluster. We compare the results with Divided Range Particle Swarm Optimization Based Clustering (DRPSO) and result show that proposed technique is efficient and work efficiently than DRPSO.

Keywords: Ad-Hoc Networks; Clustering Cluster Head; Inclusive Particle Swarm Optimization

1 Introduction

Mobile ad-hoc network consists of dynamic nodes that can freely move with different speed. Wireless mobile ad-hoc network (MANET) is a self- organizing network in which no centralized control exists which brings many problems and challenge. Dynamic nodes communicate with each other using wireless links. Nodes have limited ability to collect and process information in term of processing speed and limited size. Due to power limitation, devices typically have limited storage capacity and bandwidth [3, 6, 7, 9].

Weather forecasting, crisis management etc. are application of MANET. Cluster head have high processing speed and battery power than other node on cluster based environment that are responsible for cluster management and network maintenance. Cluster head allocate resources to all the nodes, in addition to controlling and managing it own cluster, it also communicate with others. Cluster-head maintain information about every node within the cluster. To use the network resources effectively and adapt the changing network condition in MANETs is depend on choosing the optimal number of cluster-heads.

Clustering is a method of organizing things into meaningful groups with respect to their similarities objective of clustering is to identify the groups are exclusive so that any instance belongs to a single group. Clustering of nodes in MANETs is one of the biggest challenges. Finding optimal number

of cluster that cover the entire network becomes essential and an active area of research. Clustering allowing the reuse of resources that improve the system performance and it also optimally manages the network topology by dividing the task among specified nodes called cluster-heads, which is very useful for network management and routing.

In this paper, we propose a inclusive particle swarm optimization clustering algorithm to find optimal number of cluster for mobile ad-hoc networks. Particle swarm optimization is a stochastic search technique that has simple parameter that need to be tuned during the execution of the algorithm. It has been an efficient and effective technique to solve complex optimization problems. The algorithm takes a set of parameter of MANETs into consideration such as mobility of nodes transmission power, battery power and moving speed of the nodes.

2 Related Work

Turget *et al.* proposed a genetic algorithm based clustering algorithm [10]. In their approach, the genetic algorithm is used to optimize the number of cluster in an ad hoc network. It is weight based algorithm. Chatterjee *et al.* [2] proposed the weighted clustering algorithm (WCA). It elects cluster-heads according to their weight. Baker *et al.* proposed the lowest-ID, known as identifier based clustering algorithm [1]. It assigns the unique ID to each node and chooses the node with lowest ID as a cluster-head. Gerla *et al.* proposed the highest connectivity clustering algorithm [4]. It is based on the degree of nodes, which is the number of neighbor of a given node.

3 Inclusive Particle Swarm Optimization Algorithm

Particle swarm optimization (PSO) is a stochastic optimization technique develops by Eberhart and kennedy in 1995, inspired by the social behavior of bird flocking or fish schooling. In PSO each single solution is a "bird" in the search space which we call as a "particle". A fitness value is associated with each particle which is evaluated by the fitness function to be optimized and has velocity which directs the flying of the particle [8]. PSO is the potential algorithm to optimize clustering in mobile ad hoc networks because these kinds of networks have limited resources. Particle positions and velocities are generated randomly in the beginning. The algorithms then proceed iteratively and update all velocities and positions of the particles as follows:

$$v_{id} = wv_{id} + c_1 r_1 (P_{id} - X_{id}) + c_2 r_2 (P_{gd} - X_{id}) \quad (1)$$

$$X_{id} = X_{id} + v_{id}. \quad (2)$$

Where

$d(= 1, 2, \cdots, O)$ is the number of dimensions.

$i(= 1, 2, \cdots, N)$ is the size of the population.

w is the inertia weight.

c_1 and c_2 are two positive constants.

r_1 and r_2 are two random values in the range [0, 1].

Equation (1) calculates the new velocity of the ith particle by taking into consideration three terms:

- The particle's previous velocity.

- The distance between the particle's previous best position and current position.
- The distance between the best particles of the swarm.

Equation (2) is used to calculate the new position of a particle.

The basic problem with the PSO is that it restricted the social learning aspect only to the gbest. If gbest is for away from the global optimum then the particles will go to the gbest region and get trapped in a local optimum. Inclusive particle swarm optimization algorithm (IPSOA) has the potential to move the particle in large search space to fly. In IPSOA, pbest position of a particle is updated by using pbest positions of all the particles in a swarm.

The inclusive PSO algorithm uses the following equation form updating velocity of the particle:

$$v_{id} = w \times v_{id} + c + rand_{id} \times (pbest^{df_i(d)} - x_{id}) \tag{3}$$

where $f_i = [f_i(1), f_i(2), \cdots, f_i(d)]$ describes which particles pbest the particle I will use.

Pbest $f_u(d)$ is the dimension of any particle's pbest including its own pbest. The main difference between IPSOA and original PSO is that instead of using particle's own pbest and gbest, all particles pbest can be used to guide the particle's flying direction. This strategy increases the diversity of a swarm when solving complex multidimensional problems. In the strategy the particles can fly in other direction by learning from other particles pbest. This strategy has the ability to jump out of the local optimum by using the co operative behavior of whole swarm.

4 Proposed Technique

In the proposed approach, the IPSOA users for finding the optimum number of clusters are a mobile ad-hoc network for efficiencies routing.

$$W_v = W_1 D_v + W_2 S_v + W_3 M_v + W_4 P_v \tag{4}$$

Where

D is the degree difference.

S_v is the sum of distance of the members of cluster head.

M_v is the average speed of nodes.

P_v is the accumulative time of a nodes being a cluster head.

Sum of weights is $\sum w_i = 1$ and node v with the minimum W_v is chosen as cluster-head. Once a node becomes the cluster-head, neither that node nor its member can participate in the cluster selection procedure further. The cluster head selection algorithm will terminate once all the nodes either becomes cluster-heads or members of cluster-heads. Each node in the search space has unique ID and each particle contains the IDs of all the nodes of the network. These unique ID are used to encode to particles.

The proposed algorithm is list in the following:

Step 1. Initialization:
Initialize the population of particle randomly and initialize the general parameter of IPSOA.

Step2. Fitness Value:
Calculate the fitness value of each particle. Each node is stored according the values of the objective function, which is the sum of all W_v value of cluster heads in particles.

Step 3. Selections:
Select particle neighbor for updating its velocity.

Step 4. Update:
Update the position of gbest and pbest as if Fitness (x_i) > fitness (pbest) then $\text{pbest}_i = X_i$ and if Fitness (x_i) > fitness (gbest) then $\text{gbest}_i = X_i$.

Step 5. Update Velocity and Position:

$$\begin{aligned} V_{id} &= WV_{id} + c_1 r_1 (P_{id} - X_{id}) + c_2 r_2 (P_{gd} - X_{id}) \\ X_{id} &= X_{id} + V_{id}. \end{aligned}$$

Step 6. Check stopping criteria.

Step 7. Report the global best particle as the solution of the problem.

The algorithm iteratively goes through each node in decide whether a node can become a cluster head or not. The Condition is:

- If it is not already a cluster-head.
- If it is not a member of any cluster.
- Number of neighbor of node is less than the predefined maximum allowed number of neighbor of a node.

If node fulfill the above three conditions, it is chosen as a cluster-head. After the cluster head are chosen, the already calculated value of W_v of each node is used to find out the fitness of each particle by taking the summation of all W_v values of all cluster- heads in this particle. This process contain until the maximum number of iterations is reached. When the algorithm converges, the global best particle is reported as the final solution.

5 Experimental Result

We implement the proposed algorithm in Matlab 7.0. We conduct the experiments in a machine with 1.75 GHz dual processors with 1 GB of RAM. We perform experiments of M different nodes on 50×50 and 200×200 grids. All the nodes can move in all possible directions with displacement varying uniformly between o to maximum value (max-disp). The transmission power of each node is set to 30. In our experiments, M is varied between 20 and 80. The maximum number of nodes that n cluster can handle is 10. This restriction will ensure uniform distribution of nodes in each cluster and efficient medium access control (MAC) functioning for an Ad-hoc network.

The parameter of IPSOA is initialized as follows:

1) The population size is set to the number of nodes.
2) The maximum generations are set to 1000.
3) The inertia weight w is set to 0.694.
4) The learning factor c_1 & c_2 are set to 2.

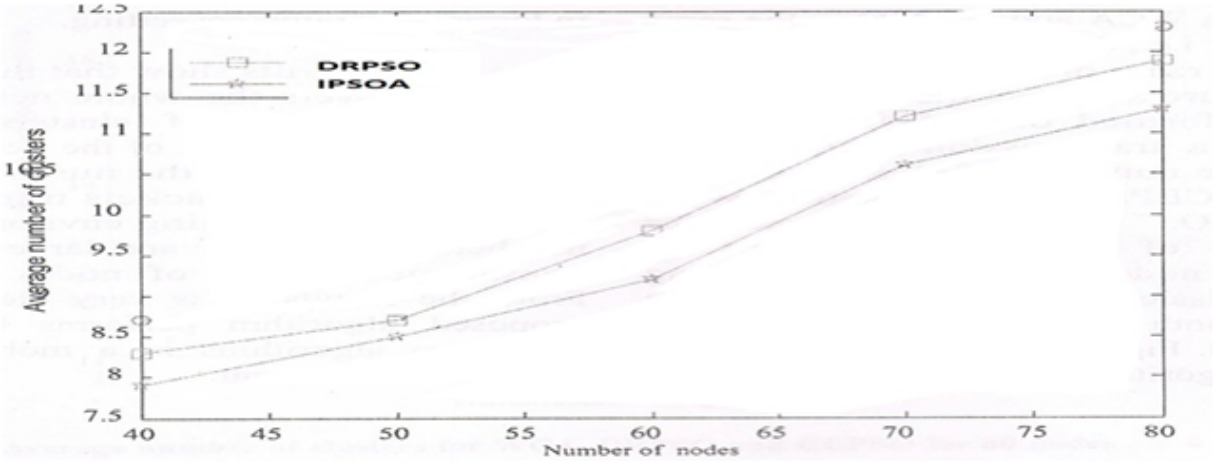

Figure 1: Average number of cluster for DRPSO and IPSOA in 50×50 m2 area with transmission range equal to 35.

We compare the results of the proposed approach with Divided Range Particle Swarm Optimization (DRPSO) based clustering [5]. The same values of all different parameters are used for three algorithms. The results are obtained after performing fifty simulations of each algorithms and then taking their averages. The simulations are performed by varying the number of nodes in the networks and the transmissions range of the mobile nodes.

As can be seen in Figure 1 our proposed algorithm based on IPSOA finds less numbers cluster to cover the whole network then DRPSO in the same environment *i.e.* 50×50 m2 areas with transmission range of 35.

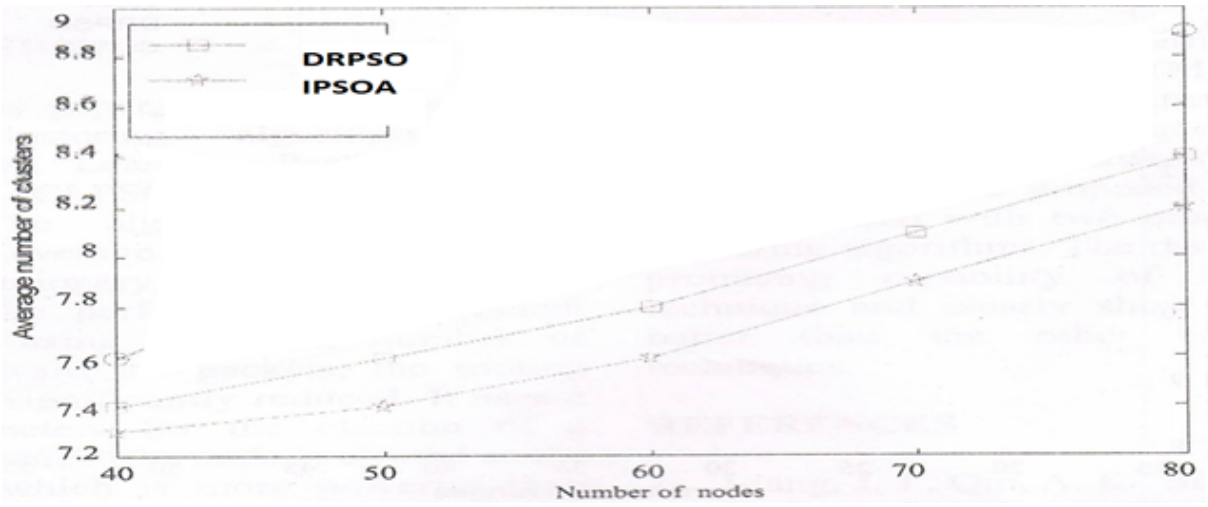

Figure 2: Average number of cluster for DRPSO and IPSOA in 200×200 m2 area with transmission range equal to 35.

Figure 2 shows the experimental results performed on a 200×200 m2 area with a transmission range of 35. The average numbers of cluster are less in case of IPSOA as compared to DRPSO. We also evaluate the performance of the three algorithms by keeping the nodes constant and increasing the transmission ranges of the mobile nodes for both 50×50 m2 and 200×200 m2 areas. Figures 3 and 4 shows that the proposed algorithm works better than the other two algorithms in terms of producing the average number of clusters. The result shows that the proposed approach covers the whole network with minimum number of clusters that can reduce the routing cost of the network. This will help to minimize the number of hops and the delayed the packets transferred in cluster-based routing environment. The numbers of cluster are large, when the transmission ranges of nodes are small from the results, it is very clear that the proposed algorithm performs better than other the algorithms in a mobile ad hoc network environment.

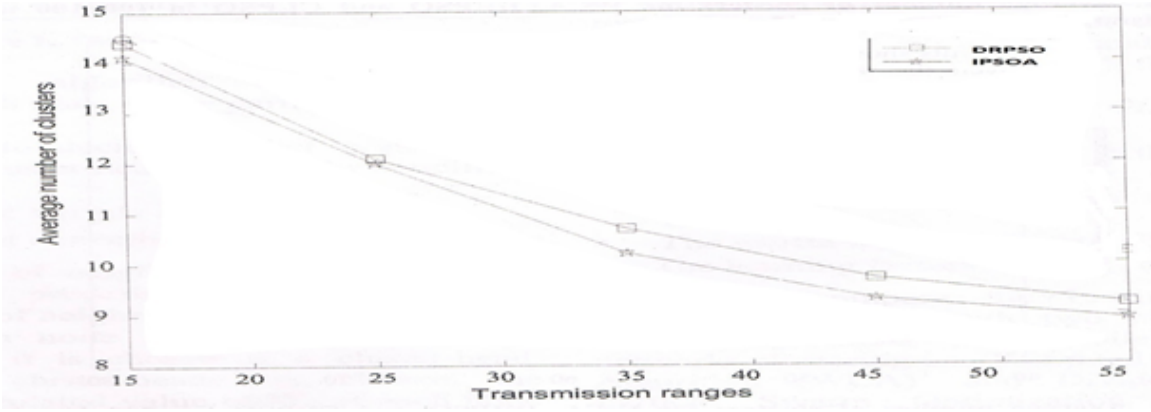

Figure 3: Average number of cluster for DRPSO and IPSOA for 80 on a 50×50 m2 area.

6 Conclusion

In this paper, we have proposed a Mobile Ad Hoc Clustering using Inclusive Particle Swarm Optimization Algorithm (IPSOA). The algorithm attempts to minimize the average number of clusters by using its evolutionary capabilities so that the routing can be performed in an efficient manner. By using minimum number of nodes to forward the packets, the routing delay can be significantly reduced. It uses a set of parameter for the election of a cluster-head hence that node is elector as the cluster-head which is more powerful than the other nodes. It also has a check on the maximum number of nodes that a cluster can handle which leads to the efficient usages of the medium access control (MAC) sub- layer. The simulation result shoe that it is an effective and robust technique for clustering in a mobile ad hoc network environment. The result of the proposed technique is also compared with DRPSO. The result exhibits the promising capabilities of the proposed technique and clearly shows that it works effectively than DRPSO.

References

[1] D. J. Baker, A. Ephremides, "The architectural organization of a mobile radio network via a distributed algorithm," *IEEE Transactions on Communications*, vol. 29, no. 11, pp. 1694-1701,

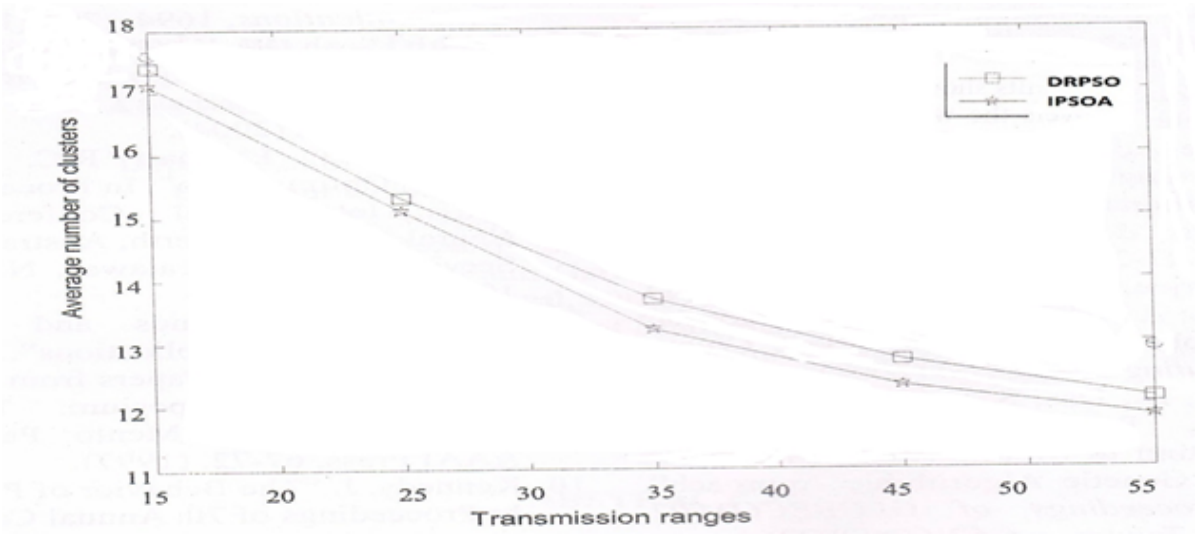

Figure 4: Average number of cluster for DRPSO and IPSOA for 80 on a 200 × 200 m2 area.

1981.

[2] M. Chatterjee, S. K. Das, D. Turgut, "WCA: A weighted clustering algorithm for mobile ad hoc networks," *Cluster Computing*, vol. 5, pp. 193-204, 2004.

[3] I. I. Er, W. K. G. Seah, "Mobility-based D-hop clustering algorithm for mobile ad hoc networks," in *IEEE WCNC'04*, Atlanta, USA, 2004.

[4] M. Gerla, J. T. C. Tsai, "Multicluster, mobile, multimedia radio network," *Wireless Networks*, vol. 1, no. 3, pp. 255-265, 1995.

[5] C. Ji, Y. Zhang, S. Gao, P. Yuan, Z. Li, "Particle swarm optimization for mobile ad hoc networks clustering," in *Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control*, Taipei, Taiwan, Mar. 21-23, 2004.

[6] J. Kennedy, "Minds and cultures: Particle swarm implications," in *Socially Intelligent Agents*, pp. 67-72, 1997.

[7] J. Kennely, R. C. Eberhart, "Particle swarm optimization," in *Proceedings of IEEE International Conference on Neural Networks*, Perth, Australia, IEEE Service Centre, Piscataway, NJ, vol. IV, pp. 1942-1948, 1995.

[8] J. J. Liang, A. K. Qin, P. N. Suganthan, S. Baskar, "Comprehensive learning particle swarm optimizer for global optimization of multimodal functions," *IEEE Transactions on Evolutionary Computation*, vol. 10, no. 3, pp. 281-295, 2006.

[9] V. V. Sunil Kumar, A. Mohammad, "Weighted clustering using comprehensive learning particle swarm optimization for mobile ad hoc networks," *Journal of Computer and Mathematical Sciences*, vol. 4, no. 3, pp. 187-196, 2013.

[10] D. Turgut, S. K. Das, R. Elmasri, B. Turgut, "Optimizing clustering algorithm in mobile ad hoc networks using genetic algorithm approach," in *Proceedings of GLOBRCOM'02*, Taipei, Taiwan, pp. 62-66, 2002.

Biography

Anurag Rana is currently employed as Assistant Professor at Arni University. He acquired M. Tech. Computer Science and Engineering from Arni School of Technology in Arni University (HP). His special interests include Artificial Intelligence, Artificial Neural Network, and Distributed System/Network.

Ruminations on Attribute-based Encryption

Zhengjun Cao[1], Lihua Liu[2], Zhenzhen Guo[2]

(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai University, Shangda Road 99, Shanghai 200444, China[1]

(Email: caozhj@shu.edu.cn)

Department of Mathematics, Shanghai Maritime University, Haigang Ave 1550, Shanghai 201306, China[2]

(Received Oct. 10, 2017; revised and accepted Dec. 5, 2017)

Abstract

Attribute-based encryption (ABE) which allows one to encrypt messages according to intended receivers' attributes is a kind of one-to-many encryption. Unlike the conventional one-to-one encryption which has no intention to exclude any partners of the intended receiver from obtaining the plaintext, an ABE system tries to exclude all unintended recipients from obtaining the plaintext, despite whether they are partners of some intended recipients. We would like to stress that this requirement for ABE is somewhat hard to meet. An ABE system cannot truly exclude some unintended recipients from decryption because some users can exchange their decryption keys in order to maximize their own interests. Due to this observation, we classify confidentialities into two kinds, strong confidentiality and weak confidentiality, corresponding to full obligations and partial obligations for keeping privacy, respectively. These classifications will be helpful to analyze the behaviors of an intended recipient and revisit the security of different encryption models.

Keywords: Attribute-based Encryption; Full Obligations; One-to-Many Encryption; Partial Obligations; Strong Confidentiality; Weak Confidentiality

1 Introduction

The cryptographic primitive of attribute-based encryption was introduced by Sahai and Waters [41]. In the scenario, a user presents an authority with a set of credentials that prove their right to fulfill an attribute. The authority issues a certification for the user to establish that the user fulfills the semantic of the attribute. This process is repeated for all attributes appropriate to each user. As a result, a user's identity is composed of a set, S, of strings which serve as descriptive attributes of the user. Like traditional identity-based encryption, the sender in an ABE system only needs to know the receivers' description in order to determine their public key. For example, a user's identity could consist of attributes describing their university, department, and job function. The sender can specify another set of attributes S' such that a receiver can only decrypt a message if his identity S has at least k attributes in common with the set S', where k is a parameter set by the system.

Attribute-based encryption has attracted much attention. Lewko, Waters, Pirretti, Goyal, and Yamada, *et al.* [1, 16, 22, 24, 25, 26, 39, 46] studied the construction of ABE systems. Ostrovsky, Sahai, and Waters [38] investigated some non-monotonic access structures of ABE. Bethencourt, Sahai, Waters, and Goyal, *et al.* proposed some ciphertext-policy attribute-based encryption schemes [3, 17, 45].

Chase and Chow [7, 8] introduced the setting of multi-authority in ABE. Hohenberger and Waters [19] discussed oline/offline attribute-based encryption. Most of these constructions use bilinear groups and some linear secret-sharing schemes as building blocks.

In 2013, Liu *et al.* [31, 32, 37] studied the white-box traceable CP-ABE problems. Fu *et al.* [12] put forth a blind expressive ciphertext policy ABE scheme for fine grained access control on the encrypted data. In 2015, Li and Zhang [27] designed a fully secure attribute based broadcast encryption scheme. Fu *et al.* [2, 11, 28, 33, 34, 44] paid attention to other variations of ABE. Recently, Yu and Cao [48] have investigated the primitive of attribute-based signcryption with hybrid access policy. Zhang and Yin [49] proposed a recipient anonymous ciphertext-policy attribute-based broadcast encryption scheme.

Unlike a conventional one-to-one encryption, an attribute-based encryption is a kind of one-to-many encryption; that is to say, there could be several intended recipients that are able to decrypt a same ciphertext. Since there are many intended recipients, each recipient undertakes partial obligations to keep privacy of the plaintext. An intended recipient possibly forwards the plaintext to others or shares his decryption key with others. That means the confidentiality level in an ABE system is much lower than that in a conventional one-to-one encryption.

In this paper, we want to stress that the conventional one-to-one encryption has no intention to exclude any partners of the intended recipient from decryption. To the contrary, an ABE scheme tries to exclude all unintended recipients from decryption despite whether they are partners of some intended recipients. We would like to remark that some users in an ABE system can exchange their decryption keys in order to maximize their own interests, which means that an ABE system cannot truly exclude some unintended recipients from decryption. We think the inherent weakness discounts the signification of ABE.

2 Different Confidentiality Levels

Confidentiality is a fundamental information security objective which is a service used to keep the content of information from all but those authorized to have it. An encryption scheme may be used as follows for the purpose of achieving confidentiality. Two parties Alice and Bob first secretly choose or secretly exchange a key pair (e, d), and pick an encryption algorithm $E()$ and its corresponding decryption algorithm $D()$. At a subsequent point in time, if Alice wishes to send a message m to Bob, she computes $c = E(e, m)$ and transmits this to Bob. Upon receiving c, Bob computes $D(d, c) = m$ and hence recovers the original message m.

From the sender's point of view, in a conventional one-to-one encryption the intended recipient undertakes the full obligations to keep privacy of the plaintext. However, the property of receiver's full obligations to keep privacy is too plain to be neglected by researchers and literatures in the past decades.

When one-to-one encryption is generalized to one-to-many encryption, each intended recipient will undertake only partial obligations.

In such a case, the behaviors of an intended recipient should be considered carefully. To facilitate the descriptions of a recipient's behaviors, we will classify confidentialities into two kinds, *strong confidentiality* and *weak confidentiality*, corresponding to *full obligations* and *partial obligations* for keeping privacy, respectively.

It is worth to point out that a recipient undertaking partial obligations for keeping privacy is more prone to leak the recovered message to others, if the betrayal is not traceable.

3 Security Requirement for One-to-one Encryption Revisited

It is well known that the conventional one-to-one encryption requires that the adversary without the valid decryption key cannot recover the plaintext. Note that the adversary here is an uncharacteristic role. The requirement does not imply that some unintended recipients cannot recover or obtain the plaintext. In real life, some partners of the intended recipient can obtain or recover the plaintext by the following two methods.

1) The intended recipient, Bob, forwards the plaintext to his partner, Cindy. We refer to Figure 1 for this case.

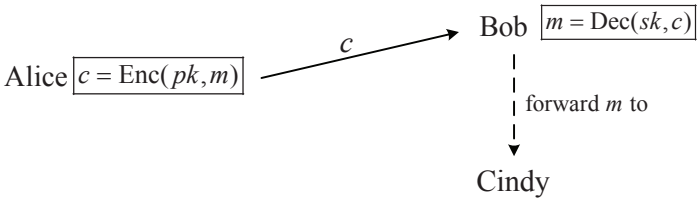

Figure 1: Bob forwards the plaintext m to Cindy

2) The intended recipient, Bob, shares the decryption key with his partner, Cindy. We refer to Figure 2 for this case.

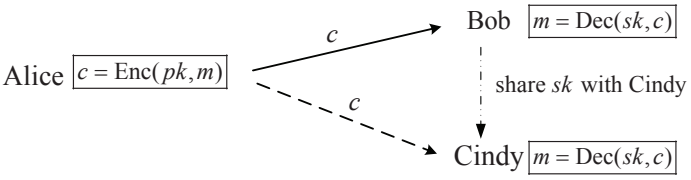

Figure 2: Bob shares his secret key with Cindy

In short, the conventional one-to-one encryption has no intention to exclude some partners of the intended recipient from obtaining the plaintext. *This property is so obvious that it is often neglected.* However, the partnership of recipients must be taken into account when we design a one-to-many encryption system.

4 Attribute-based Encryption Model Revisited

Attribute-based encryption is claimed to be a vision of public key encryption that allows users to encrypt and decrypt messages based on users' attributes. In the scenario, users are represented by the summation of their attributes. An encryptor will associate encrypted data with a set of attributes. An authority will issue users different decryption keys, where a user's decryption key is associated with an access structure over attributes and reflects the access policy ascribed to the user. Notice that attribute-based encryption is a kind of one-to-many encryption.

There are two kind of attribute-based encryptions, ciphertext-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE). In a CP-ABE system, keys are associated with sets of attributes and ciphertexts are associated with access policies. In a KP-ABE system, the situation is reversed: keys are associated with access policies and ciphertexts are associated with sets of attributes. For convenience, we only describe the definition of CP-ABE as follows. We refer to Figure 3 for the essence of the model of ABE.

A ciphertext-policy attribute-based encryption scheme consists of the following four PPT algorithms [40]:

Setup $(1^\lambda) \to (pp, msk)$**:** The algorithm takes the security parameter $\lambda \in \mathbb{N}$ and outputs the public parameters pp and the master secret key msk. Assume that the public parameters contain a description of the attribute universe $\mathcal{U}$.

KeyGen$(1^\lambda, pp, msk, \mathcal{S}) \to sk$**:** The algorithm takes the public parameters pp, the master secret key msk and a set of attributes $\mathcal{S} \subseteq \mathcal{U}$. It generates a secret key corresponding to $\mathcal{S}$.

Encrypt$(1^\lambda, pp, m, A) \to ct$**:** The algorithm takes the public parameters pp, a plaintext message m, and an access structure A on $\mathcal{U}$. It outputs the ciphertext ct.

Decrypt$(1^\lambda, pp, sk, ct) \to m$**:** The algorithm takes the public parameters pp, a secret key sk, and a ciphertext ct. It outputs the plaintext m.

A CP-ABE scheme is correct if the decryption algorithm correctly decrypts a ciphertext of an access structure A with a decryption key on $\mathcal{S}$, when $\mathcal{S}$ is an authorized set of A.

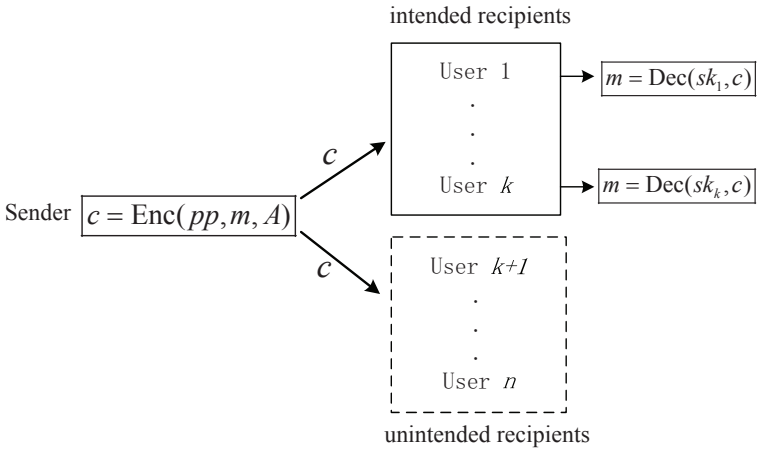

Figure 3: The model of attribute-based encryption

It is easy to find that the attribute-based encryption tries to exclude some unintended recipients from obtaining the plaintext despite whether they are partners of some intended recipients. We shall argue that this purpose cannot be fully achieved.

5 Decryption-key-sharing Attack Against ABE

Most of the existing ABE schemes use bilinear groups and some linear secret-sharing schemes as building blocks. In such an ABE system, there is an authority who is responsible for generating secret keys for

all members. These secret keys are not for one-time use. They can be repeatedly invoked. Concretely, most ABE schemes have the following features:

- *Repudiable key.* The secret key for each member is only used for decryption, not for signing, because it is generated and issued by the authority. Strictly speaking, this key has no the function of non-repudiation from a legal standpoint. Thus, it is better to call it decryption key.
- *Partial obligations.* One intended recipient in a communication undertakes only partial obligations to keep privacy of the plaintext. Apparently, he is more prone to reveal the plaintext to others.
- *Future passerby.* Each member may become one unintended recipient in future communications. In this situation, a member is more prone to reveal his secret key to his partners if these partners are also in the same system.
- *Maximized interest.* In order to maximize the interests (the capability to correctly decrypt future communications), some members can exchange their decryption keys and create alliances with as many different people in the same system as they can. For convenience, we call it decryption-key-sharing attack. We refer to Figure 4 for the essence of this attack.

In short, the attribute-based encryption can not truly exclude some unintended recipients from decryption. The ambitious objective of excluding unintended recipients in ABE model is somewhat hard to fulfill, because an intended recipient could forward the plaintext to some unintended recipients or directly shares his decryption key with his partners.

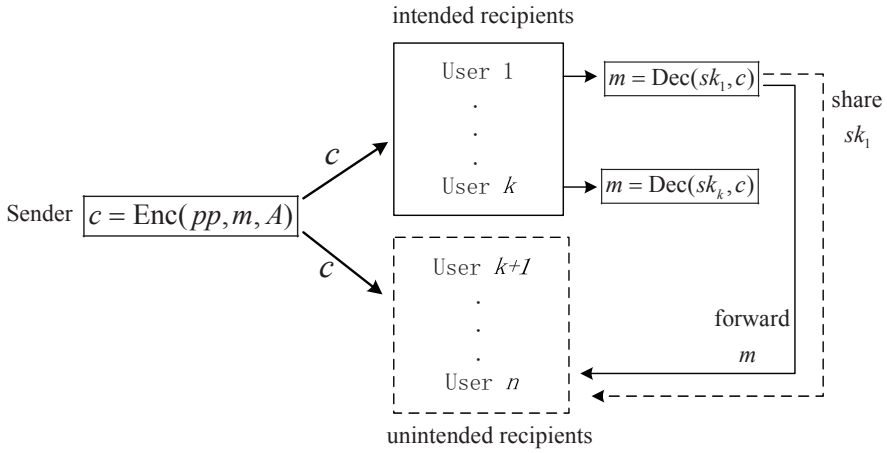

Figure 4: Attacks against attribute-based encryption

6 Analysis of Some Hypothetical Applications of ABE

It claims that attribute-based encryption has enormous potential for providing data security in distributed environments. We shall have a close look at the examples in some literatures. The corresponding schemes take advantage of bilinear property of pairings to insert trapdoors in encryption functions and decryption functions. The heavy pairing computations [6, 29, 30] in these schemes impede their practical implementations. Moreover, we find the necessity of ABE in these examples [3, 19, 24, 38, 39, 41] is indeed overstated.

Example 1. *(see [39]) A user Bob looking for employment in the field of secure systems engineering could place a copy of his resume in publicly accessible web space encrypted with the attributes "secure systems engineering" and "human resources manager". Only potential employers satisfying these attributes would be able to decrypt this information and contact Bob.*

Remark 1. *We believe it is better for Bob to distribute his resume through mass emails as usual.* The privacy exposed in the resume is of far little importance to the job hunter*. The traditional job-hunting method could be more effective than placing the encrypted resume in publicly accessible web space.*

Example 2. *(see [3]) Suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman. The head FBI agent may want to encrypt a sensitive memo so that only personnel that have certain credentials or attributes can access it. For instance, the head agent may specify the following access structure for accessing this information: (("Public Corruption Office" AND ("Knoxville" OR "San Francisco")) OR (management-level > 5) OR "Name: Charlie Eppes"). By this, the head agent could mean that the memo should only be seen by agents who work at the public corruption offices at Knoxville or San Francisco, FBI officials very high up in the management chain, and a consultant named Charlie Eppes.*

Remark 2. *In general,* a bribery allegation concerning a congressman requires strong confidentiality*. We do not think that the primitive of ABE is appropriate for this situation because of its weak confidentiality.*

Example 3. *(see [41]) In a computer science department, the chairperson might want to encrypt a document to all of its systems faculty on a hiring committee. In this case it would encrypt to the identity {"hiring-committee","faculty", "systems"}. Any user who has an identity that contains all of these attributes could decrypt the document.*

Example 4. *(see [24]) Suppose an administrator needs to encrypt a junior faculty member's performance review for all senior members of the computer science department or anyone in the dean's office. The administrator will want to encrypt the review with the access policy ("Computer Science" AND "Tenured") OR "Dean's Office". In this system, only users with attributes (credentials) that match this policy should be able to decrypt the document. The key challenge in building such systems is to realize security against colluding users. For instance, the encrypted records should not be accessible to a pair of unauthorized users, where one has the two credentials of "Tenured" and "Chemistry" and the other one has the credential of "Computer Science". Neither user is actually a tenured faculty member of the Computer Science Department.*

Example 5. *(see [38]) A university is conducting a peer-review evaluation, where each department will be critiqued by a panel of professors from other departments. Bob, who is a member of the panel this year from the Biology department, will need to read (possibly sensitive) comments about other departments and assimilate them for his written review. In an Attribute-Based Encryption system the comments will be labeled with descriptive attributes; for example, a comment on the History department might be encrypted with the attributes: "History", "year=2007", "dept-review". In the Goyal* et al.*'s scheme [39], Bob might receive a private key for the policy "year=2007" AND "dept-review", which would allow him to see all comments from this current year. However, in this setting it is important that Bob should not be able to view comments written about his own department. Therefore, the policy we would actually like to ascribe to Bob's key is "year=2007" AND "dept-review" AND (NOT "Biology").*

Example 6. *(see [19]) In a key-policy ABE (KP-ABE) system, an encrypted message can be tagged with a set of attributes, such as tagging an email with the metadata "from: Alice", "to: IACR board",*

"subject: voting", "date: October 1, 2012", etc. The master authority for the system can issue private decryption keys to users including an access policy, such as giving to Bob a decryption key that enables him to decrypt any ciphertexts that satisfy "to: Bob" OR ("to: IACR board" AND (January 1, 2011 ≤ "date" ≤ December 31, 2012)).

Remark 3. *All the above four examples are contrived. They do not consider the partnership of users. For example, a user with the attributes of "Tenured" and "Chemistry" is very likely to be a close friend of one with the attributes of "Tenured" and "Computer Science". It is a better choice for them to exchange their decryption keys in order to enhance their capabilities to decrypt future communications correctly, if they feel it is necessary. That is to say,* the security of these examples depends on the will of users rather than on any intractable assumptions.

Remark 4. *The strategy of physical access control has been broadly implemented for many years. It was believed to be efficient and robust although it has this or that weaknesses, such as low-level security, inflexibility for selecting users, and lacking of portability. From the perspective of cryptography, physical access control aims to exclude common unauthorized users from decryption, not those powerful adversaries. In nature, it provides only weak confidentiality as ABE. But the sophisticated primitive of ABE is extraordinarily inefficient than physical access control (see the above schemes [19, 24, 41, 38]). Taking into account these shortcomings, we would like to remark that physical access control seems more appropriate for weak confidentiality than ABE.*

7 Another One-to-many Encryption

Broadcast encryption formalized by Fiat and Naor [10], is another primitive of one-to-may encryption. It requires that the broadcaster encrypts a message such that a particular set of users can decrypt the message sent over a broadcast channel. The Fiat-Naor broadcast encryption and the works [13, 14, 20, 42, 43] use a combinatorial approach. This approach has to right the balance between the efficiency and the number of colluders that the system is resistant to. Most of these schemes require that each user's decryption key is for one-time use. They have no intention to exclude some particular recipients from obtaining the plaintext. Therefore, they are immune to decryption-key-sharing attack.

In a revocation system, a broadcaster encrypts a message such that a particular set of revoked users cannot decrypt the message sent over a broadcast channel. In 1998, Kurosawa and Desmedt [21] introduced a method based on polynomial interpolation for constructing revocation systems. The subsequent revocation systems [36, 47] adopt this technique. In 1999, Canetti *et al.* [4, 5] developed a different method for multicast encryption. In 2001, Naor, Naor and Lopspeich [35] proposed a stateless tree-based revocation scheme. Their method was subsequently improved by Halevy and Shamir [18], Goodrich, Sun, and Tamassia [15], and by Dodis and Fazio [9].

At IEEE Symposium on Security and Privacy 2010, Lewko, Sahai and Waters [23] proposed a simple revocation system with very small decryption keys.

In the scheme, the authority generates all users' decryption keys which should be repeatedly used. Like most ABE schemes, the Lewko-Sahai-Waters revocation can not truly revoke some users because it can not resist decryption-key-sharing attack. Note that the Goodrich-Sun-Tamassia tree-based revocation system [15] is immune to this attack. They have stressed that keys should be updated after each insertion or deletion (revocation) of a device. They have also specified the strategy for key update and tree rebalance.

8 Conclusion

The partnership of recipients in an ABE system plays a key role in analyzing the security of the system which has been neglected in the past decade. We find an ABE system can not resist decryption-key-sharing attack.

The flaw renders the primitive impractical. The conventional physical access control has been broadly implemented for many years although it is of low-level security, inflexibility for selecting users and lacking of portability. From the perspective of cryptography, physical access control provides only weak confidentiality as ABE. But ABE is extraordinarily inefficient than physical access control because of the involved heavy pairing computations. Thus physical access control seems more appropriate for weak confidentiality than ABE.

Acknowledgements

We thank the National Natural Science Foundation of China (61303200, 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] N. Attrapadung and et al., "Attribute-based encryption schemes with constant-size ciphertexts," *Theoretical Computer Sciences*, no. 422, pp. 15–38, 2012.

[2] B. Balusamy and et al., "A secured access control technique for cloud computing environment using attribute based hierarchical structure and token granting system," *International Journal of Network Security*, vol. 19, no. 4, pp. 559–572, 2017.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of IEEE Symposium on Security and Privacy (S&P'07)*, pp. 321–334, Oakland, California, USA, May 2007.

[4] R. Canetti and et al., "Multicast security: A taxonomy and some efficient constructions," in *Proceedings of The Conference on Computer Communications, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99)*, pp. 708–716, New York, NY, USA, Mar. 1999.

[5] R. Canetti, T. Malkin, and K. Nissim, "Efficient communication-storage tradeoffs for multicast encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'99)*, pp. 459–474, Prague, Czech Republic, May 1999.

[6] Z. J. Cao, L. H. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifiable outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.

[7] M. Chase, "Multi-authority attribute based encryption," in *Proceedings of 4th Theory of Cryptography Conference (TCC'07)*, pp. 515–534, Amsterdam, Netherlands, Feb. 2007.

[8] M. Chase and S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of ACM Conference on Computer and Communications Security (CCS'09)*, pp. 121–130, Chicago, Illinois, USA, Nov. 2009.

[9] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in *Proceedings of Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop (DRM'02)*, pp. 61–80, Washington, DC, USA, Nov. 2002.

[10] A. Fiat and M. Naor, "Broadcast encryption," in *Proceedings of 13th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'93)*, pp. 480–491, Santa Barbara, California, USA, Aug. 1993.
[11] X. B. Fu, "Unidirectional proxy re-encryption for access structure transformation in attribute-based encryption schemes," *International Journal of Network Security*, vol. 17, no. 2, pp. 142–149, 2015.
[12] X. B. Fu, S. K. Zeng, and F. G. Li, "Blind expressive ciphertext policy attribute based encryption for fine grained access control on the encrypted data," *International Journal of Network Security*, vol. 17, no. 6, pp. 661–671, 2015.
[13] E. Gafni, J. Staddon, and Y.L. Yin, "Efficient methods for integrating traceability and broadcast encryption," in *Proceedings of 19th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'99)*, pp. 372–387, Santa Barbara, California, USA, Aug. 1999.
[14] J. Garay, J. Staddon, and A. Wool, "Long-lived broadcast encryption," in *Proceedings of 20th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'00)*, pp. 333–352, Santa Barbara, California, USA, Aug. 2000.
[15] M. Goodrich, J.Z. Sun, and R. Tamassia, "Efficient tree-based revocation in groups of low-state devices," in *Proceedings of 24th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'04)*, pp. 511–527, Santa Barbara, California, USA, Aug. 2004.
[16] V. Goyal and et al., "Attribute-based encryption for fine grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, pp. 89–98, Alexandria, VA, USA, Nov. 2006.
[17] V. Goyal and et al., "Bounded ciphertext policy attribute based encryption," in *Proceedings of 35th International Colloquium on Automata, Languages and Programming (ICALP'08)*, pp. 579–591, Reykjavik, Iceland, July 2008.
[18] D. Halevy and A. Shamir, "The lsd broadcast encryption scheme," in *Proceedings of 22nd Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'02)*, pp. 47–60, Santa Barbara, California, USA, Aug. 2002.
[19] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proceedings of 17th International Conference on Practice and Theory in Public-Key Cryptography (PKC'14)*, pp. 293–310, Buenos Aires, Argentina, Mar. 2014.
[20] R. Kumar, S. Rajagopalan, and A. Sahai, "Coding constructions for blacklisting problems without computational assumptions," in *Proceedings of 19th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'99)*, pp. 609–623, Santa Barbara, California, USA, Aug. 1999.
[21] K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'98)*, pp. 145–157, Espoo, Finland, May 1998.
[22] A. Lewko and et al., "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'10)*, pp. 62–91, French Riviera, May 2010.
[23] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in *Proceedings of 31st IEEE Symposium on Security and Privacy (S&P'10)*, pp. 273–285, Berleley/Oakland, California, USA, May 2010.
[24] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'11)*, pp. 568–588, Tallinn, Estonia, May 2011.
[25] A. Lewko and B. Waters, "Unbounded hibe and attribute-based encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'11)*, pp. 547–567, Tallinn, Estonia, May 2011.

[26] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Proceedings of 32nd Annual Cryptology Conference, Advances in Cryptology (CRYPTO'12)*, pp. 180–198, Santa Barbara, California, USA, Aug. 2012.
[27] Q. Y. Li and F. L. Zhang, "A fully secure attribute based broadcast encryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 255–263, 2015.
[28] C. W. Liu and et al., "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
[29] L. H. Liu and Z. J. Cao, "A note on 'efficient algorithms for secure outsourcing of bilinear pairings'," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.
[30] L. H. Liu and et al., "On bilinear groups of a large composite order," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 1–9, 2017.
[31] Z. Liu, Z. F. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Transaction on Information Forensics and Security*, vol. 8, no. 1, pp. 76–88, 2013.
[32] Z. Liu, Z. F. Cao, and D. S. Wong, "Traceable cp-abe: How to trace decryption devices found in the wild," *IEEE Transaction on Information Forensics and Security*, vol. 10, no. 1, pp. 55–68, 2015.
[33] H. Ma, T. Peng, and Z. H. Liu, "Directly revocable and verifiable key-policy attribute-based encryption for large universe," *International Journal of Network Security*, vol. 19, no. 2, pp. 272–284, 2017.
[34] J. Modi and et al., "A secure communication model for expressive access control using cp-abe," *International Journal of Network Security*, vol. 19, no. 2, pp. 193–204, 2017.
[35] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proceedings of 21st Annual Cryptology Conference, Advances in Cryptology (CRYPTO'01)*, pp. 41–62, Santa Barbara, California, USA, Aug. 2001.
[36] M. Naor and B. Pinkas, "Efficient trace and revoke schemes," in *Proceedings of 4th International Conference, Financial Cryptography (FC'00)*, pp. 1–20, Anguilla, British West Indies, Feb. 2000.
[37] J. T. Ning and et al., "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transaction on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.
[38] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS'07)*, pp. 195–203, Alexandria, Virginia, USA, Oct. 2007.
[39] M. Pirretti and et al., "Secure attribute-based systems," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS'06)*, pp. 99–112, Alexandria, Virginia, USA, Nov. 2006.
[40] Y. Rouselakis and B. Waters, "New constructions and proof methods for large universe attribute-based encryption," *IACR Cryptology ePrint Archive*, no. 583, 2012.
[41] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'05)*, pp. 457–473, Aarhus, Denmark, May 2005.
[42] D. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," *Design, Codes and Cryptography*, vol. 12, no. 3, pp. 215–243, 1997.
[43] D. Stinson and T. Trung, "Some new results on key distribution patterns and broadcast encryption," *Design, Codes and Cryptography*, vol. 14, no. 3, pp. 261–279, 1998.
[44] C. M. Wang and et al., "A general formal framework of analyzing selective disclosure attribute-based credential systems," *International Journal of Network Security*, vol. 19, no. 5, pp. 794–803, 2017.

[45] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proceedings of International Conference on Practice and Theory in Public-Key Cryptography (PKC'11)*, pp. 53–70, Taormina, Italy, Mar. 2011.
[46] S. Yamada and et al., "A framework and compact constructions for non-monotonic attribute-based encryption," in *Proceedings of International Conference on Practice and Theory in Public-Key Cryptography (PKC'14)*, pp. 275–292, Buenos Aires, Argentina, Mar. 2014.
[47] E. Yoo and et al., "Efficient broadcast encryption using multiple interpolation methods," in *Proceedings of 7th International Conference on Information Security and Cryptology (ICISC'04)*, pp. 87–103, Seoul, Korea, Dec. 2004.
[48] G. Yu and Z. F. Cao, "Attribute-based signcryption with hybrid access policy," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 253–261, 2017.
[49] L. Y. Zhang and H. J. Yin, "Recipient anonymous ciphertext-policy attribute-based broadcast encryption," *International Journal of Network Security*, vol. 20, no. 1, pp. 168–176, 2018.

Biography

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhenzhen Guo is currently pursuing her M.S. degree from Department of Mathematics, Shanghai Maritime university. Her research interests include combinatorics and cryptography.

The Encryption Algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4

Tuychiev Gulom

(Corresponding author: Tuychiev Gulom)

National University of Uzbekistan, Republic of Uzbekistan, Tashkent

(Email: blasterjon@gmail.com)

(Received Mar. 14, 2017; revised and accepted May 25, 2017)

Abstract

In the paper created a new encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 based on networks IDEA8-4 and RFWKIDEA8-4, with the use the round function of the encryption algorithm GOST 28147-89. The block length of created block encryption algorithm is 256 bits, the number of rounds is 8, 12 and 16.

Keywords: GOST 28147-89; Lai-Massey Scheme; Round Function; Round Keys; Output Transformation

1 Introduction

The encryption algorithm GOST 28147-89 [1] is a standard encryption algorithm of the Russian Federation and based on a Feistel network. This encryption algorithm is suitable for hardware and software implementation, meets the necessary cryptographic requirements for resistance and, therefore, does not impose restrictions on the degree of secrecy of the information being protected. The algorithm implements the encryption of 64-bit blocks of data using the 256 bit key. In round functions used eight S-box of size 4x4 and operation of the cyclic shift by 11 bits. To date GOST 28147-89 is resistant to cryptographic attacks. On the basis of structure encryption algorithm IDEA [2] and Lai-Massey scheme developed networks IDEA8-4 [5] and RFWKIDEA8-4 [10], consisting from four round function. In the networks IDEA8-4 and RFWKIDEA8-4, similarly as in the Feistel network, in encryption and decryption process using the same algorithm. In the networks used four round function having one input and output blocks and as the round function can use any transformation.

As the round function networks IDEA4-2 [37], RFWKIDEA4-2 [7], PES4-2 [6], RFWKPES4-2 [18], PES8-4 [38], RFWKPES8-4 [14] using the round function of the encryption algorithm GOST 28147-89 created the encryption algorithm GOST28147-89-IDEA4-2 [15], GOST28147-89-RFWKIDEA4-2 [24], GOST28147-89-PES4-2 [23], GOST28147-89-RFWKPES4-2 [25], GOST28147-89-PES8-4 [30] and GOST28147-89-RFWKPES8-4 [30].

In addition, by using SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations of the encryption algorithm AES [3] as round functions of networks IDEA8-1 [10], RFWKIDEA8-1 [10],

PES8-1 [4], RFWKPES8-1 [14], IDEA16-1 [8], RFWKIDEA16-1 [12], PES16-1 [17], RFWKPES16-1 [19], IDEA32-1 [9], RFWKIDEA32-1 [35], PES32-1 [11], RFWKPES32-1 [13], RFWKIDEA16-2 [12], IDEA16-2 [8], PES16-2 [17], RFWKPES16-2 [19], IDEA32-4 [9], RFWKIDEA32-4 [35], PES32-4 [11], RFWKPES32-4 [13] created encryption algorithms AES-IDEA8-1 [32], AES-RFWKIDEA8-1 [34], AES-PES8-1 [33], AES-RFWKPES8-1 [16], AES-IDEA16-1 [31], AES-RFWKIDEA16-1 [27], AES-PES16-1 [29], AES-RFWKPES16-1 [29], AES-IDEA32-1 [20], AES-RFWKIDEA32-1 [28], AES-PES32-1 [21], AES-RFWKPES32-1 [21], AES-IDEA16-2 [26], AES-RFWKIDEA16-2 [26], AES-PES16-2 [26], AES-RFWKPES16-2 [26], AES-IDEA32-4 [22], AES-RFWKIDEA32-4 [22], AES-RFWKPES32-4 [36], AES-PES32-4 [39].

In this paper, applying the round function of the encryption algorithm GOST 28147-89 as round functions of the networks IDEA8-4 and RFWKIDEA8-4, developed new encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4. In encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 block length is 256 bits, the key length is changed from 256 bits to 1024 bits in increments of 128 bits and number of rounds equal to 8, 12, 16, allowing the user depending on the degree of secrecy of information and speed of encryption to choose the number of rounds and key length.

2 The Encryption Algorithm GOST28147-89-IDEA8-4

2.1 The Structure of the Encryption Algorithm GOST28147-89-IDEA8-4

In the encryption algorithm GOST28147-89-IDEA8-4 length of subblocks X^0, X^1, ..., X^7, length of round keys $K_{12(i-1)}$, $K_{12(i-1)+1}$, ..., $K_{12(i-1)+7}$, $i = \overline{1...n+1}$, $K_{12(i-1)+8}$, $K_{12(i-1)+9}$, ..., $K_{12(i-1)+11}$, $i = \overline{1...n}$ and K_{12n+8}, K_{12n+9}, ..., K_{12n+23} are equal to 32-bits. In this encryption algorithm the round function GOST 28147-89 is applied four time and in each round function used eight S-boxes, *i.e.* the total number of S-boxes is 32. The structure of the encryption algorithm GOST28147-89-IDEA8-4 is shown in Figure 1 and the S-boxes shown in Table 1.

Consider the round function of encryption algorithm GOST28147-89-IDEA8-4. First 32-bit subblocks T^0, T^1, T^2, T^3 are summed round keys $K_{12(i-1)+8}$, $K_{12(i-1)+9}$, $K_{12(i-1)+10}$, $K_{12(i-1)+11}$ *i.e.* $S^0=T^0+K_{12(i-1)+8}$, $S^1=T^1+K_{12(i-1)+9}$, $S^2=T^2+K_{12(i-1)+10}$, $S^3=T^3+K_{12(i-1)+11}$. 32-bit subblocks S^0, S^1, S^2, S^3 divided into eight four-bit subblocks $S^0=s_0^0||s_1^0||...||s_7^0$, $S^1=s_0^1||s_1^1||...||s_7^1$, $S^2=s_0^2||s_1^2||...||s_7^2$, $S^3=s_0^3||s_1^3||...||s_7^3$. Four bit subblocks s_i^0, s_i^1, s_i^2, s_i^3, $i = \overline{0...7}$ transformed into the S-boxes: $R^0 = S_0(s_0^0) \,||\, S_1(s_1^0) \,||\, ... \,||\, S_7(s_7^0)$, $R^1=S_8(s_0^1)||S_9(s_1^1)||...||\ S_{15}(s_7^1)$, $R^2=S_{16}(s_0^2)||S_{17}(s_1^2)||...||\ S_{23}(s_7^2)$, $R^3=S_{24}(s_0^3)||S_{25}(s_1^3)||...||\ S_{31}(s_7^3)$. The resulting 32-bit subblocks R^0, R^1, R^2, R^3 cyclically shifted left by 11 bits and obtain subblocks Y_0, Y_1, Y_2, Y_3: $Y_0=R^0<<11$, $Y_1=R^1<<11$, $Y_2=R^2<<11$, $Y_3=R^3<<11$.

Consider the encryption process of encryption algorithm GOST28147-89-IDEA8-4. Initially the 256-bit plaintext X partitioned into subblocks of 32-bits X_0^0, X_0^1, ..., X_0^7, and performs the following steps:

1) subblocks X_0^0, X_0^1, ..., X_0^7 summed by XOR with round key K_{12n+8}, K_{12n+9}, ..., K_{12n+15}: $X_0^j = X_0^j \oplus K_{12n+8+j}$, $j = \overline{0...7}$.

2) subblocks X_0^0, X_0^1, ..., X_0^7 multiplied and summed with the round keys $K_{12(i-1)}$, $K_{12(i-1)+1}$, ..., $K_{12(i-1)+7}$ and calculated 32-bit subblocks T^0, T^1, T^2, T^3. This step can be represented as follows: $T^0 = (X_{i-1}^0 \cdot K_{12(i-1)}) \oplus (X_{i-1}^4 + K_{12(i-1)+4})$, $T^1 = (X_{i-1}^1 + K_{12(i-1)+1}) \oplus (X_{i-1}^5 \cdot K_{12(i-1)+5})$, $T^2 = (X_{i-1}^2 \cdot K_{12(i-1)+2}) \oplus (X_{i-1}^6 + K_{12(i-1)+6})$, $T^3 = (X_{i-1}^3 + K_{12(i-1)+3}) \oplus (X_{i-1}^7 \cdot K_{12(i-1)+7})$,$i = 1$.

3) to subblocks T^0, T^1, T^2, T^3 applying the round function and get the 32-bit subblocks Y^0, Y^1, Y^2, Y^3.

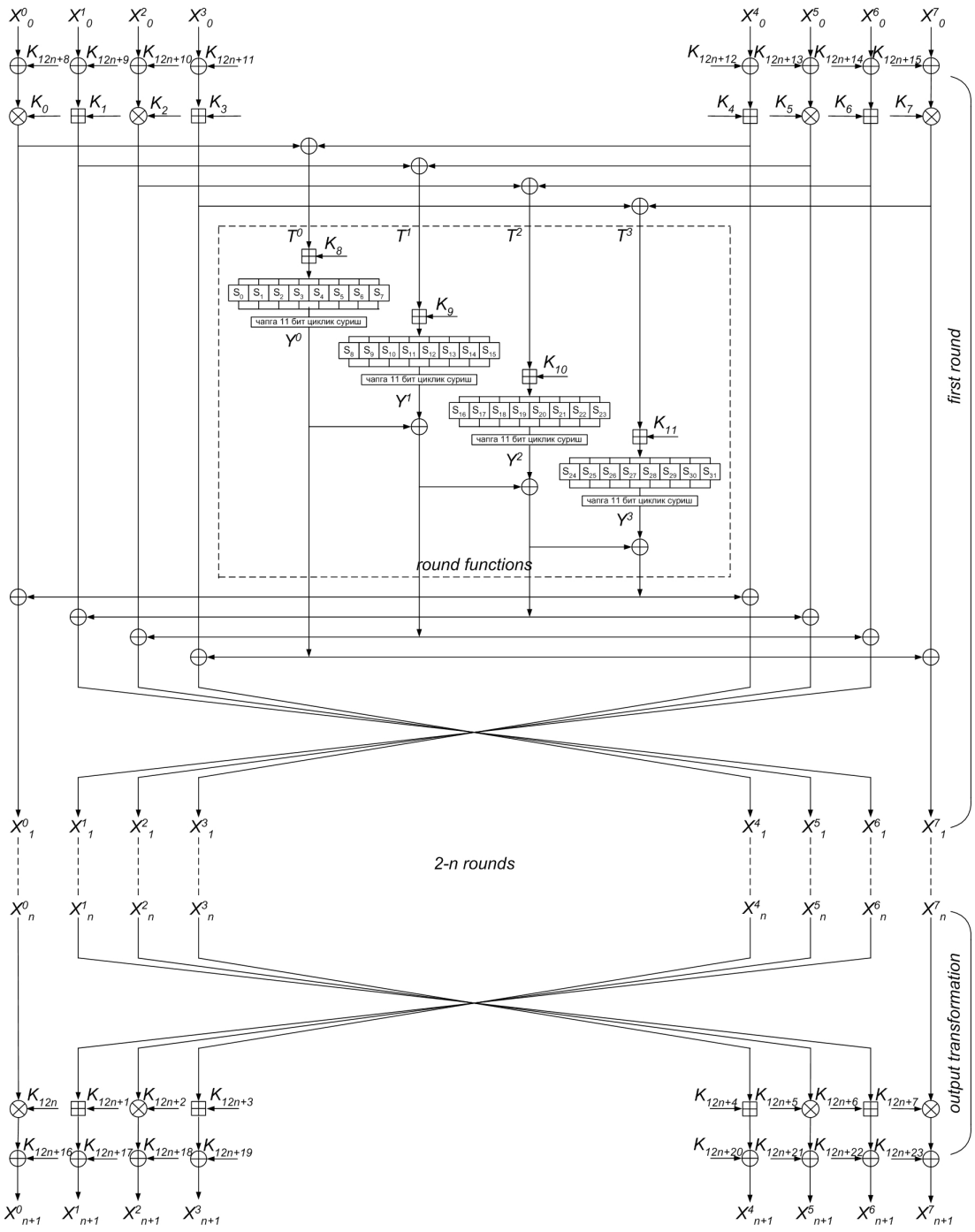

Figure 1: The scheme of encryption algorithm GOST28147-89-IDEA8-4

Table 1: The S-boxes of encryption algorithms

	0x0	**0x1**	**0x2**	**0x3**	**0x4**	**0x5**	**0x6**	**0x7**	**0x8**	**0x9**	**0xA**	**0xB**	**0xC**	**0xD**	**0xE**	**0xF**
S_0	0x4	0x5	0xA	0x8	0xD	0x9	0xE	0x2	0x6	0xF	0xC	0x7	0x0	0x3	0x1	0xB
S_1	0x5	0x4	0xB	0x9	0xC	0x8	0xF	0x3	0x7	0xE	0xD	0x6	0x1	0x2	0x0	0xA
S_2	0x6	0x7	0x8	0xA	0xF	0xB	0xC	0x0	0x4	0xD	0xE	0x5	0x2	0x1	0x3	0x9
S_3	0x7	0x6	0x9	0xB	0xE	0xA	0xD	0x1	0x5	0xC	0xF	0x4	0x3	0x0	0x2	0x8
S_4	0x8	0x9	0x6	0x4	0x1	0x5	0x2	0xE	0xA	0x3	0x0	0xB	0xC	0xF	0xD	0x7
S_5	0x9	0x8	0x7	0x5	0x0	0x4	0x3	0xF	0xB	0x2	0x1	0xA	0xD	0xE	0xC	0x6
S_6	0xA	0xB	0x4	0x6	0x3	0x7	0x0	0xC	0x8	0x1	0x2	0x9	0xE	0xD	0xF	0x5
S_7	0xB	0xA	0x5	0x7	0x2	0x6	0x1	0xD	0x9	0x0	0x3	0x8	0xF	0xC	0xE	0x4
S_8	0xC	0xD	0x2	0x0	0x5	0x1	0x6	0xA	0xE	0x7	0x4	0xF	0x8	0xB	0x9	0x3
S_9	0xE	0xF	0x0	0x2	0x7	0x3	0x4	0x8	0xC	0x5	0x6	0xD	0xA	0x9	0xB	0x1
S_{10}	0xF	0xE	0x1	0x3	0x6	0x2	0x5	0x9	0xD	0x4	0x7	0xC	0xB	0x8	0xA	0x0
S_{11}	0x1	0x8	0x7	0xD	0x0	0x4	0x3	0xF	0xB	0xA	0x9	0x2	0x5	0x6	0xC	0xE
S_{12}	0x2	0xB	0x4	0xE	0x3	0x7	0x0	0xC	0x8	0x9	0xA	0x1	0x6	0x5	0xF	0xD
S_{13}	0x3	0xA	0x5	0xF	0x2	0x6	0x1	0xD	0x9	0x8	0xB	0x0	0x7	0x4	0xE	0xC
S_{14}	0x4	0x5	0xA	0x0	0xD	0x1	0x6	0x2	0xE	0x7	0xC	0xF	0x8	0x3	0x9	0xB
S_{15}	0x5	0x4	0xB	0x1	0xC	0x0	0x7	0x3	0xF	0x6	0xD	0xE	0x9	0x2	0x8	0xA
S_{16}	0x6	0x7	0x8	0x2	0xF	0x3	0x4	0x0	0xC	0x5	0xE	0xD	0xA	0x1	0xB	0x9
S_{17}	0x7	0x6	0x9	0x3	0xE	0x2	0x5	0x1	0xD	0x4	0xF	0xC	0xB	0x0	0xA	0x8
S_{18}	0x8	0x9	0x6	0xC	0x1	0xD	0xA	0xE	0x2	0xB	0x0	0x3	0x4	0xF	0x5	0x7
S_{19}	0x9	0x8	0x7	0xD	0x0	0xC	0xB	0xF	0x3	0xA	0x1	0x2	0x5	0xE	0x4	0x6
S_{20}	0xA	0xB	0x4	0xE	0x3	0xF	0x8	0xC	0x0	0x9	0x2	0x1	0x6	0xD	0x7	0x5
S_{21}	0xB	0xA	0x5	0xF	0x2	0xE	0x9	0xD	0x1	0x8	0x3	0x0	0x7	0xC	0x6	0x4
S_{22}	0xC	0xD	0x2	0x8	0x5	0x9	0xE	0xA	0x6	0xF	0x4	0x7	0x0	0xB	0x1	0x3
S_{23}	0xD	0xC	0x3	0x9	0x4	0x8	0xF	0xB	0x7	0xE	0x5	0x6	0x1	0xA	0x0	0x2
S_{24}	0x1	0x8	0x7	0x5	0x0	0xC	0xB	0xF	0x3	0x2	0x9	0xA	0xD	0x6	0x4	0xE
S_{25}	0x2	0xB	0x4	0x6	0x3	0xF	0x8	0xC	0x0	0x1	0xA	0x9	0xE	0x5	0x7	0xD
S_{26}	0x3	0xA	0x5	0x7	0x2	0xE	0x9	0xD	0x1	0x0	0xB	0x8	0xF	0x4	0x6	0xC
S_{27}	0xF	0xE	0x1	0xB	0x6	0xA	0xD	0x9	0x5	0xC	0x7	0x4	0x3	0x8	0x2	0x0
S_{28}	0xE	0xF	0x0	0xA	0x7	0xB	0xC	0x8	0x4	0xD	0x6	0x5	0x2	0x9	0x3	0x1
S_{29}	0xA	0xB	0xC	0xE	0x3	0xF	0x0	0x4	0x8	0x1	0x2	0x9	0x6	0x5	0x7	0xD
S_{30}	0xB	0xA	0xD	0xF	0x2	0xE	0x1	0x5	0x9	0x0	0x3	0x8	0x7	0x4	0x6	0xC
S_{31}	0xC	0xD	0xA	0x8	0x5	0x9	0x6	0x2	0xE	0x7	0x4	0xF	0x0	0x3	0x1	0xB

4) subblocks Y^0, Y^1, Y^2, Y^3 are summed to XOR with subblocks X^0_{i-1}, X^1_{i-1}, X^2_{i-1}, X^3_{i-1}, i.. $X^0_{i-1} = X^0_{i-1} \oplus Y^3$, $X^1_{i-1} = X^1_{i-1} \oplus Y^2$, $X^2_{i-1} = X^2_{i-1} \oplus Y^1$, $X^3_{i-1} = X^3_{i-1} \oplus Y^0$, $X^4_{i-1} = X^4_{i-1} \oplus Y^3$, $X^5_{i-1} = X^5_{i-1} \oplus Y^2$, $X^6_{i-1} = X^6_{i-1} \oplus Y^1$, $X^7_{i-1} = X^7_{i-1} \oplus Y^0$, $i = 1$.

5) at the end of the round subblocks swapped, i.., $X^0_i = X^0_{i-1}$, $X^7_i = X^7_{i-1}$, $X^1_i = X^6_{i-1}$, $X^2_i = X^5_{i-1}$, $X^3_i = X^4_{i-1}$, $X^4_i = X^3_{i-1}$, $X^5_i = X^2_{i-1}$, $X^6_i = X^1_{i-1}$, $i = 1$.

6) repeating steps 2-5 n times, *i.e.*, $i = \overline{2...n}$ obtain 32-bit subblocks X^0_n, X^1_n, ..., X^7_n.

7) in output transformation round keys K_{12n}, K_{12n+1}, ..., K_{12n+7} are multiplied and summed into subblocks, *i.e.* $X^0_{n+1} = X^j_n \cdot K_{12n}$, $X^1_{n+1} = X^6_n + K_{12n+1}$, $X^2_{n+1} = X^5_n \cdot K_{12n+2}$, $X^3_{n+1} = X^4_n + K_{12n+3}$, $X^4_{n+1} = X^3_n + K_{12n+4}$, $X^5_{n+1} = X^2_n \cdot K_{12n+5}$, $X^6_{n+1} = X^1_n + K_{12n+6}$, $X^7_{n+1} = X^7_n \cdot K_{12n+7}$.

8) subblocks X^0_{n+1}, X^1_{n+1}, ..., X^7_{n+1} are summed to XOR with the round key K_{12n+16}, K_{12n+17}, ..., K_{12n+23}: $X^j_{n+1} = X^j_{n+1} \oplus K_{12n+16+j}$, $j = \overline{0...7}$.

As ciphertext plaintext X receives the combined 32-bit subblocks $X^0_{n+1}||X^1_{n+1}||...||X^7_{n+1}$.

In the encryption algorithm GOST28147-89-IDEA8-4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

2.2 Key Generation of the Encryption Algorithm GOST28147-89-IDEA8-4

In n-round encryption algorithm GOST28147-89-IDEA8-4 in each round used 12 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32-bit round keys is equal to 12n+24. Hence, if n=8 then necessary 120, if n=12 then 168 and if n=16 then 216 to generate round keys. In Figure 2 in encryption used encryption round keys K^c_i instead of K_i, while decryption used decryption round keys K^d_i.

The key encryption algorithm K of length l ($256 \le l \le 1024$) bits is divided into 32-bit round keys K^c_0, K^c_1,..., $K^c_{Lenght-1}$, $Lenght = l/32$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K^c_0 = \{k_0, k_1, ..., k_{31}\}$, $K^c_1 = \{k_{32}, k_{33}, ..., k_{63}\}$,..., $K^c_{Lenght-1} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ and $K = K^c_0||K^c_1||...||K^c_{Lenght-1}$. Then we calculate $K_L = K^c_0 \oplus K^c_1 \oplus ... \oplus K^c_{Lenght-1}$. If $K_L = 0$ then K_L is chosen as 0xC5C31537, *i.e.* $K_L =$ 0xC5C31537. Round keys K^c_i, $i = \overline{Lenght...12n+23}$ calculated as follows: $K^c_i = SBox0(K^c_{i-Lenght}) \oplus SBox1(RotWord32(K^c_{i-Lenght+1})) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit. Here *RotWord32()*-cyclic shift to the left of 1 bit of the 32-bit subblock, *SBox()*convert 32-bit subblock in S-box and $SBox0(A) = S_0(a_0)||\ S_1(a_1)||\ ...||\ S_7(a_7)$, $SBox1(A) = S_9(a_0)||\ S_{10}(a_1)||\ ...||\ S_{15}(a_7)$, $A = a_0||\ a_1||\ ...||\ a_7$ and a_i-four-bit subblock, S_i-i-th S-Box.

Decryption round keys are computed on the basis of encryption round keys and decryption round keys of the first round associate with of encryption round keys as follows:

$$(K^d_0, K^d_1, K^d_2, K^d_3, K^d_4, K^d_5, K^d_6, K^d_7) = ((K^c_{12n})^{-1}, -K^c_{12n+1}, (K^c_{12n+2})^{-1}, -K^c_{12n+3}, -K^c_{12n+4}, (K^c_{12n+5})^{-1}, -K^c_{12n+6}, (K^c_{12n+7})^{-1}, K^c_{12(n-1)+8}, K^c_{12(n-1)+9}, K^c_{12(n-1)+10}, K^c_{12(n-1)+11})$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$(K^d_{12(i-1)}, K^d_{12(i-1)+1}, K^d_{12(i-1)+2}, K^d_{12(i-1)+3}, K^d_{12(i-1)+4}, K^d_{12(i-1)+5}, K^d_{12(i-1)+6}, K^d_{12(i-1)+7}, K^d_{12(i-1)+8}, K^d_{12(i-1)+9}, K^d_{12(i-1)+10}, K^d_{12(i-1)+11}) = ((K^c_{12(n-i+1)})^{-1}, -K^c_{12(n-i+1)+6}, (K^c_{12(n-i+1)+5})^{-1}, -K^c_{12(n-i+1)+4}, -K^c_{12(n-i+1)+3}, (K^c_{12(n-i+1)+2})^{-1}, -K^c_{12(n-i+1)+1}, (K^c_{12(n-i+1)+7})^{-1}, K^c_{12(n-i)+8}, K^c_{12(n-i)+9}, K^c_{12(n-i)+10}, K^c_{12(n-i)+11}), i = \overline{2...n}$

Decryption keys output transformation associated with the encryption keys as follows:

$(K^d_{12n}, K^d_{12n+1}, K^d_{12n+2}, K^d_{12n+3}, K^d_{12n+4}, K^d_{12n+5}, K^d_{12n+6}, K^d_{12n+7}) = ((K^c_0)^{-1}, -K^c_1, (K^c_2)^{-1}, -K^c_3, -K^c_4, (K^c_5)^{-1}, -K^c_6, (K^c_7)^{-1})$.

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K^d_{12n+8+j} = K^c_{12n+16+j}$, $K^d_{12n+16+j} = K^c_{12n+8+j}$, $j = \overline{0...7}$.

3 The Encryption Algorithm GOST28147-89-RFWKIDEA8-4

3.1 The Structure of the Encryption Algorithm GOST28147-89-RFWKIDEA8-4

In the encryption algorithm GOST28147-89-RFWKIDEA8-4 the length of subblocks X^0, X^1, ..., X^7, length of round keys $K_{8(i-1)}$, $K_{8(i-1)+1}$, ..., $K_{8(i-1)+7}$, $i = \overline{1...n+1}$, $K_{8(i-1)+8}$, $K_{8(i-1)+9}$, ..., $K_{8(i-1)+11}$, $i = \overline{1...n}$ and K_{8n+8}, K_{8n+9}, ..., K_{8n+23} are equal to 32-bits. In this encryption algorithm the round function GOST 28147-89 is applied four time and in each round function used eight S-boxes, *i.e.* the total number of S-boxes is 32. The structure of the encryption algorithm GOST28147-89-IDEA8-4 is shown in Figure 2 and the S-boxes shown in Table 1.

Consider the round function of encryption algorithm GOST28147-89-RFWKIDEA8-4. First 32-bit subblocks T^0, T^1, T^2, T^3 divided into eight four-bit sub-blocks, *i.e.*

T^0=t^0_0|| t^0_1|| ...|| t^0_7, T^1=t^1_0|| t^1_1|| ...|| t^1_7, T^2=t^2_0|| t^2_1|| ...|| t^2_7, T^3=t^3_0|| t^3_1|| ...|| t^3_7.

The four bit subblocks t^0_i, t^1_i, t^2_i, t^3_i, $i = \overline{0...7}$ converted into the S-boxes: R^0=$S_0(t^0_0)$|| $S_1(t^0_1)$|| ...|| $S_7(t^0_7)$, R^1=$S_8(t^1_0)$|| $S_9(t^1_1)$|| ...|| $S_{15}(t^1_7)$, R^2=$S_{16}(t^2_0)$|| $S_{17}(t^1_1)$|| ...|| $S_{23}(t^2_7)$, R^3=$S_{24}(t^3_0)$|| $S_{25}(t^3_1)$|| ...|| $S_{31}(t^2_7)$. The resulting 32-bit subblocks R^0, R^1, R^2, R^3 cyclically shifted left by 11 bits and obtain subblocks Y_0, Y_1, Y_2, Y_3: Y_0=R^0<<11, Y_1=R^1<<11, Y_2=R^2<<11, Y_3=R^3<<11.

Consider the encryption process of encryption algorithm GOST28147-89-RFWKIDEA8-4. Initially the 256-bit plaintext X partitioned into subblocks of 32-bits X^0_0, X^1_0, ..., X^7_0, and performs the following steps:

1) Subblocks X^0_0, X^1_0, ..., X^7_0 summed by XOR with round key K_{8n+8}, K_{8n+9}, ..., K_{8n+15}: $X^j_0 = X^j_0 \oplus K_{8n+8+j}$, $j = \overline{0...7}$.

2) Subblocks X^0_0, X^1_0, ..., X^7_0 multiplied and summed with the round keys $K_{8(i-1)}$, $K_{8(i-1)+1}$, ..., $K_{8(i-1)+7}$ and calculated 32-bit subblocks T^0, T^1, T^2, T^3. This step can be represented as follows: $T^0 = (X^0_{i-1} \cdot K_{8(i-1)}) \oplus (X^4_{i-1} + K_{8(i-1)+4})$, $T^1 = (X^1_{i-1} + K_{8(i-1)+1}) \oplus (X^5_{i-1} \cdot K_{8(i-1)+5})$, $T^2 = (X^2_{i-1} \cdot K_{8(i-1)+2}) \oplus (X^6_{i-1} + K_{8(i-1)+6})$, $T^3 = (X^3_{i-1} + K_{8(i-1)+3}) \oplus (X^7_{i-1} \cdot K_{8(i-1)+7})$,$i = 1$.

3) To subblocks T^0, T^1, T^2, T^3 applying the round function and get the 32-bit subblocks Y^0, Y^1, Y^2, Y^3.

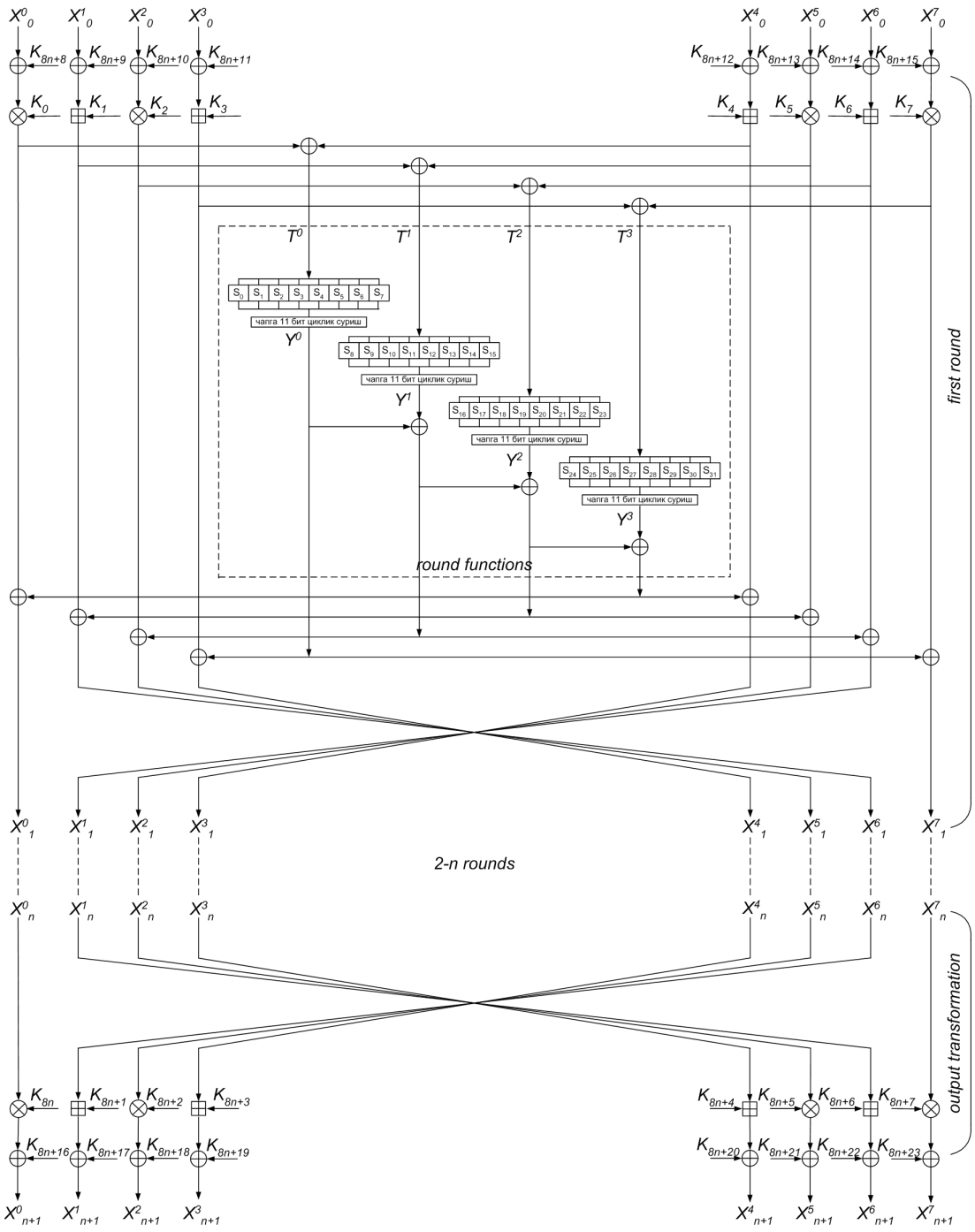

Figure 2: The scheme of encryption algorithm GOST28147-89-RFWKIDEA8-4

4) Subblocks Y^0, Y^1, Y^2, Y^3 are summed to XOR with subblocks X^0_{i-1}, X^1_{i-1}, X^2_{i-1}, X^3_{i-1}, i.. $X^0_{i-1} = X^0_{i-1} \oplus Y^3$, $X^1_{i-1} = X^1_{i-1} \oplus Y^2$, $X^2_{i-1} = X^2_{i-1} \oplus Y^1$, $X^3_{i-1} = X^3_{i-1} \oplus Y^0$, $X^4_{i-1} = X^4_{i-1} \oplus Y^3$, $X^5_{i-1} = X^5_{i-1} \oplus Y^2$, $X^6_{i-1} = X^6_{i-1} \oplus Y^1$, $X^7_{i-1} = X^7_{i-1} \oplus Y^0$, $i = 1$.

5) At the end of the round subblocks swapped, i.., $X^0_i = X^0_{i-1}$, $X^7_i = X^7_{i-1}$, $X^1_i = X^6_{i-1}$, $X^2_i = X^5_{i-1}$, $X^3_i = X^4_{i-1}$, $X^4_i = X^3_{i-1}$, $X^5_i = X^2_{i-1}$, $X^6_i = X^1_{i-1}$, $i = 1$.

6) Repeating steps 2-5 n times, *i.e.*, $i = \overline{2...n}$ obtain 32-bit subblocks X^0_n, X^1_n, ..., X^7_n.

7) In output transformation round keys K_{8n}, K_{8n+1}, ..., K_{8n+7} are multiplied and summed into subblocks, *i.e.* $X^0_{n+1} = X^j_n \cdot K_{8n}$, $X^1_{n+1} = X^6_n + K_{8n+1}$, $X^2_{n+1} = X^5_n \cdot K_{8n+2}$, $X^3_{n+1} = X^4_n + K_{8n+3}$, $X^4_{n+1} = X^3_n + K_{8n+4}$, $X^5_{n+1} = X^2_n \cdot K_{8n+5}$, $X^6_{n+1} = X^1_n + K_{8n+6}$, $X^7_{n+1} = X^7_n \cdot K_{8n+7}$,

8) Subblocks X^0_{n+1}, X^1_{n+1}, ..., X^7_{n+1} are summed to XOR with the round key K_{8n+16}, K_{8n+17}, ..., K_{8n+23}: $X^j_{n+1} = X^j_{n+1} \oplus K_{8n+16+j}$, $j = \overline{0...7}$. As ciphertext plaintext X receives the combined 32-bit subblocks $X^0_{n+1}||X^1_{n+1}||...||X^7_{n+1}$.

In the encryption algorithm GOST28147-89-RFWKIDEA8-4 when encryption and decryption using the same algorithm, only when decryption calculates the inverse of round keys depending on operations and are applied in reverse order. One important goal of encryption is key generation.

3.2 Key Generation of the Encryption Algorithm GOST28147-89-RFWKIDEA8-4

In n-round encryption algorithm GOST28147-89-RFWKIDEA8-4 used in each round 8 round keys of 32 bits and the output transformation of 8 round keys of 32 bits. In addition, prior to the first round and after the output transformation is applied 8 round keys on 32 bits. The total number of 32-bit round keys is equal to 8n+24.

The key encryption algorithm K of length l ($256 \le l \le 1024$) bits is divided into 32-bit round keys K^c_0, K^c_1,..., $K^c_{Lenght-1}$, $Lenght = l/32$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K^c_0 = \{k_0, k_1, ..., k_{31}\}$, $K^c_1 = \{k_{32}, k_{33}, ..., k_{63}\}$,..., $K^c_{Lenght-1} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ and $K = K^c_0||K^c_1||...||K^c_{Lenght-1}$. Then we calculate $K_L = K^c_0 \oplus K^c_1 \oplus ... \oplus K^c_{Lenght-1}$. If $K_L = 0$ then K_L is chosen as 0xC5C31537, *i.e.* $K_L =$ 0xC5C31537. Round keys K^c_i, $i = \overline{Lenght...8n+23}$ calculated as follows: $K^c_i = SBox0(K^c_{i-Lenght}) \oplus SBox1(RotWord32(K^c_{i-Lenght+1})) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit.

Decryption round keys are computed on the basis of encryption round keys and decryption round keys of the first round associate with of encryption round keys as follows:

$$(K^d_0, K^d_1, K^d_2, K^d_3, K^d_4, K^d_5, K^d_6, K^d_7) = ((K^c_{8n)})^{-1}, -K^c_{8n+1}, (K^c_{8n+2)})^{-1}, -K^c_{8n+3}, -K^c_{8n+4}, (K^c_{8n+5)})^{-1}, -K^c_{8n+6}, (K^c_{8n+7)})^{-1})$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$$(K^d_{8(i-1)}, K^d_{8(i-1)+1}, K^d_{8(i-1)+2}, K^d_{8(i-1)+3}, K^d_{8(i-1)+4}, K^d_{8(i-1)+5}, K^d_{8(i-1)+6}, K^d_{8(i-1)+7}) = ((K^c_{8(n-i+1)})^{-1}, -K^c_{8(n-i+1)+6}, (K^c_{8(n-i+1)+5})^{-1}, -K^c_{8(n-i+1)+4}, -K^c_{8(n-i+1)+3}, (K^c_{8(n-i+1)+2})^{-1}, -K^c_{8(n-i+1)+1}, (K^c_{8(n-i+1)+7})^{-1}), \; i = \overline{2...n}$$

Decryption keys output transformation associated with the encryption keys as follows:

$(K_{8n}^d, K_{8n+1}^d, K_{8n+2}^d, K_{8n+3}^d, K_{8n+4}^d, K_{8n+5}^d, K_{8n+6}^d, K_{8n+7}^d) = ((K_0^c)^{-1}, -K_1^c, (K_2^c)^{-1}, -K_3^c, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1})$.

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K_{8n+8+j}^d = K_{8n+16+j}^c$, $K_{8n+16+j}^d = K_{8n+8+j}^c$, $j = \overline{0...7}$.

4 Results

As a result of this study built a new block encryption algorithms called GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4. This algorithm is based on a networks IDEA16-2 and RFWKIDEA16-2 using the round function of GOST 28147-89. Length of block encryption algorithm is 256 bits, the number of rounds and key lengths is variable. Wherein the user depending on the degree of secrecy of the information and speed of encryption can select the number of rounds and key length.

It is known, that the S-box encryption algorithm GOST 28147-89 are secret and used as a long-term key. following Table 2 summarizes options openly declared S-box such as: deg -degree of algebraic nonlinearity; NL -nonlinearity; λ -resistance to linear cryptanalysis; δ-resistance to differential cryptanalysis; SAC-strict avalanche criterion; BIC-bit independence criterion.To S-Box was resistant to cryptanalysis it is necessary that the values deg and NL were large, and the values λ , δ , SAC and BIC small. In block cipher algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 for all S-boxes, the following equation:deg $= 3$, $NL = 4$, $\lambda = 0.5$, $\delta = 3/8$, SAC=2, BIC=4, *i.e.* resistance is not lower than the algorithm GOST28147-89. These S-boxes are created based on Nyberg construction [40].

Table 2: Parameters of the S-boxes encryption algorithm GOST 28147-89

№	Parameters	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
1	deg	2	3	3	2	3	3	2	2
2	NL	4	2	2	2	2	2	2	2
3	λ	0.5	3/4	3/4	3/4	3/4	3/4	3/4	3/4
4	δ	3/8	3/8	3/8	3/8	1/4	3/8	0.5	0.5
5	SAC	2	2	2	4	2	4	2	2
6	BIC	4	2	4	4	4	4	2	4

To the encryption algorithm applied linear cryptanalysis. Attack on 4-round GOST28147-89-IDEA8-4 has a data complexity of 2^{83} chosen plaintexts and on 4-round GOST28147-89-RFWKIDEA8-4 has a data complexity of 2^{75} chosen plaintexts.

5 Conclusions

In this way, built a new block encryption algorithms called GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4 based on networks IDEA8-4 and RFWKIDEA8-4 using the round function of GOST 28147-89. Installed that the resistance offered by the author block cipher algorithm not lower than the resistance of the algorithm GOST 28147-89.

References

[1] GOST, *National Standard of the USSR. Information Processing Systems, Cryptographic Protection. Algorithm Cryptographic Transformation*, GOST 2814789.

[2] J. Massey, X. Lai, "On the design and security of block cipher," *ETH Series in Information Processing*, vol. 1, 1992.

[3] V. Rijmen, J. Daeman, "Aes proposal: Rijndael," *NIST AES Proposal*, 1998. (`http://csrc.nist.gov/`)

[4] G. Tuychiev, "About networks pes8-2 and pes8-1, developed on the basis of network pes8-4," in *Materials of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2014*, vol. 2, pp. 28–32, 2012.

[5] G. Tuychiev, "The network idea8-4, consists from four round functions," *Infocommunications: Networks-Technologies-Solutions*, vol. 26, no. 2, pp. 55–59, 2012.

[6] G. Tuychiev, "The network pes4-2, consists from two round functions," *Uzbek Journal of the Problems of Informatics and Energetics*, no. 5-6, pp. 107–111, 2013.

[7] G. Tuychiev, "The networks rfwkidea4-2, idea4-1 and rfwkidea4-1," *Acta of Turin Polytechnic University in Tashkent*, no. 3, pp. 71–77, 2013.

[8] G. Tuychiev, "About networks idea16-4, idea16-2, idea16-1, created on the basis of network idea16-8," *Compilation of theses and reports republican seminar Information security in the sphere communication and information. Problems and their solutions*, 2014.

[9] G. Tuychiev, "About networks idea32-8, idea32-4, idea32-2, idea32-1, created on the basis of network idea32-16," *Infocommunications: Networks-Technologies-Solutions*, vol. 30, no. 2, pp. 45–50, 2014.

[10] G. Tuychiev, "About networks idea8-2, idea8-1 and rfwkidea8-4, rfwkidea8-2, rfwkidea8-1 developed on the basis of network idea8-4," *Uzbek Mathematical Journal*, vol. 3, pp. 104–118, 2014.

[11] G. Tuychiev, "About networks pes32-8, pes32-4, pes32-2 and pes32-1, created on the basis of network pes32-16," *Ukrainian Scientific Journal of Information Security*, vol. 20, pp. 164–168, 2014.

[12] G. Tuychiev, "About networks rfwkidea16-8, rfwkidea16-4, rfwkidea16-2, rfwkidea16-1, created on the basis network idea16-8," *Ukrainian Scientific Journal of Information Security*, vol. 20, pp. 259–263, 2014.

[13] G. Tuychiev, "About networks rfwkpes32-8, rfwkpes32-4, rfwkpes32-2 and rfwkpes32-1, created on the basis of network pes32-16," *Compilation of theses and reports republican seminar Information security in the sphere communication and information. Problems and their solutions*, 2014.

[14] G. Tuychiev, "About networks rfwkpes8-4, rfwkpes8-2, rfwkpes8-1, developed on the basis of network pes8-4," *Materials of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2014*, vol. 2, pp. 32–36, 2014.

[15] G. Tuychiev, "Creating a data encryption algorithm based on network idea4-2, with the use the round function of the encryption algorithm gost 28147-89," *Infocommunications: Networks-Technologies-Solutions*, vol. 32, no. 4, pp. 49–54, 2014.

[16] G. Tuychiev, "New encryption algorithm based on network rfwkpes8-1 using of the transformations of the encryption algorithm aes," *International Journal of Computer Networks and Communications Security*, vol. 3, no. 6, pp. 31–34, 2014.

[17] G. Tuychiev, "About networks pes16-4, pes16-2 and pes16-1, created on the basis network pes16-8," *Ukrainian Information Security Research Journal*, vol. 17, no. 1, pp. 53–60, 2015.

[18] G. Tuychiev, "About networks pes4-1 and rfwkpes4-2, rfwkpes4-1 developed on the basis of network pes4-2," *Uzbek Journal of the Problems of Informatics and Energetics*, no. 1-2, pp. 100–105, 2015.

[19] G. Tuychiev, "About networks rfwkpes16-8, rfwkpes16-4, rfwkpes16-2 and rfwkpes16-1, created on the basis network pes16-8," *Ukrainian Information Security Research Journal*, vol. 17, no. 4, pp. 163–169, 2015.

[20] G. Tuychiev, "Creating a block encryption algorithm based network idea32-1 using transformation of the encryption algorithm aes," *Acta NUUz*, no. 2/1, pp. 136–142, 2015.
[21] G. Tuychiev, "Creating a block encryption algorithm based networks pes32-1 and rfwkpes32-1 using transformation of the encryption algorithm aes," in *Compilation scientific work scientific and practical conference Current issues of cyber security and information security-CICSIS-2015*, pp. 101–112, 2015.
[22] G. Tuychiev, "Creating a block encryption algorithm on the basis of networks idea32-4 and rfwkidea32-4 using transformation of the encryption algorithm aes," *Ukrainian Scientific Journal of Information Security*, vol. 21, pp. 148–158, 2015.
[23] G. Tuychiev, "Creating a encryption algorithm based on network pes4-2 with the use the round function of the gost 28147-89," *TUIT Bulleten*, vol. 34, no. 4, pp. 132–136, 2015.
[24] G. Tuychiev, "Creating a encryption algorithm based on network rfwkidea4-2 with the use the round function of the gost 28147-89," *International Journal of Advanced Technology in Engineering and Science*, vol. 3, no. 1, pp. 427–432, 2015.
[25] G. Tuychiev, "Creating a encryption algorithm based on network rfwkpes4-2 with the use the round function of the gost 28147-89," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 4, no. 2, pp. 14–17, 2015.
[26] G. Tuychiev, "Development block encryption algorithm based networks idea16-2 and rfwkidea16-2 using the transformation of encryption algorithm aes," in *Information Security in the light of the Strategy Kazakhstan-2050: proceedings III International scientific-practical conference*, pp. 40–60, 2015.
[27] G. Tuychiev, "The encryption algorithm aes-rfwkidea16-1," *Infocommunications: Networks-Technologies-Solutions*, vol. 34, no. 2, pp. 48–54, 2015.
[28] G. Tuychiev, "The encryption algorithm aes-rfwkidea32-1 based on network rfwkidea32-1," *Global Journal of Computer Science and Technology: E Network, Web, Security*, vol. 15, pp. 33–41, 2015.
[29] G. Tuychiev, "The encryption algorithms aes-pes16-1 and aes-rfwkpes16-1 based on networks pes16-1 and rfwkpes16-1," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 53–66, 2015.
[30] G. Tuychiev, "The encryption algorithms gost28147-89-pes8-4 and gost28147-89-rfwkpes8-4," in *Information Security in the light of the Strategy Kazakhstan-2050: Proceedings III International Scientific-Practical Conference*, pp. 355–371, 2015.
[31] G. Tuychiev, "New encryption algorithm based on network idea16-1 using of the transformation of the encryption algorithm aes," *IPASJ International Journal of Information Technology*, vol. 3, pp. 6–12, 2015.
[32] G. Tuychiev, "New encryption algorithm based on network idea8-1 using of the transformation of the encryption algorithm aes," *IPASJ International Journal of Computer Science*, vol. 3, pp. 43–47, 2015.
[33] G. Tuychiev, "New encryption algorithm based on network pes8-1 using of the transformations of the encryption algorithm aes," *International Journal of Computer Networks and Communications Security*, vol. 3, no. 2, pp. 1–5, 2015.
[34] G. Tuychiev, "New encryption algorithm based on network rfwkidea8-1 using transformation of aes encryption algorithm," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 4, no. 1, pp. 1–5, 2015.
[35] G. Tuychiev, "To the networks rfwkidea32-16, rfwkidea32-8, rfwkidea32-4, rfwkidea32-2 and rfwkidea32-1, based on the network idea32-16," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 5, no. 1, pp. 9–20, 2015.
[36] G. Tuychiev, "The encryption algorithm aes-rfwkpes32-4," in *Proceedings International Round Table On the National and Information Security in the Republic of Kazakhstan*, 2016.

[37] G. Tuychiev, M. Aripov, "The network idea4-2, consists from two round functions," *Infocommunications: Networks-Technologies-Solutions*, vol. 24, no. 4, pp. 55–59, 2012.
[38] G. Tuychiev, M. Aripov, "The network pes8-4, consists from four round functions," in *Materials of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2012*, vol. 2, pp. 16–19, 2012.
[39] G. Tuychiev, M. Aripov, "The encryption algorithm aes-pes32-4 based on network pes32-4," in *Materials of the international scientific conference Modern problems of applied mathematics and information technologies-Al-Khorezmiy 2016*, vol. 2, pp. 28–34, 2016.
[40] G. Tuychiev, U. Bakhtiyorov, "About generation resistance s-box and boolean function on the basis of nyberg construction," in *Materials scientific-technical conference Applied mathematics and information security*, pp. 317–324, 2014.

Biography

Tuychiev Gulom candidate technical Sciences (Ph.D.), National University of Uzbekistan.

Ruminations on Fully Homomorphic Encryption in Client-server Computing Scenario

Zhengjun Cao[1], Lihua Liu[2], Yang Li[2]

(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai University[1]

Shangda Road 99, Shanghai, 200444, China[1]

(Email: caozhj@shu.edu.cn)

Department of Mathematics, Shanghai Maritime University, Haigang Ave 1550, Shanghai, 201306, China[2]

(Received Dec. 10, 2017; revised and accepted Feb. 8, 2018)

Abstract

Fully homomorphic encryption (FHE) allows anyone to perform computations on encrypted data, despite not having the secret decryption key. Since the Gentry's work in 2009, FHE has become a hot topic. In this paper, we would like to stress that any computations performed on encrypted data are constrained intrinsically to the underlying domain (finite fields or rings). This restriction makes the primitive useless for the computations involving common arithmetic expressions and relational expressions, because of the incompatibility of numerical computation with underlying encoding transformation over finite domains. We want to reaffirm that cryptography uses modular arithmetic a lot in order to obscure and dissipate redundancies in plaintext, not to perform any numerical calculations. Thus FHE will be of little importance to client-server computing or cloud computing.

Keywords: Client-server Computing; Common Arithmetic; Encryption Domain; Fully Homomorphic Encryption; Modular Arithmetic

1 Introduction

Homomorphic encryption introduced by Rivest, Adleman and Dertouzos [29] in 1978, is a useful cryptographic primitive because it can translate an operation on the ciphertexts into an operation on the corresponding plaintexts. The property is useful for some applications, such as e-voting, watermarking and secret sharing schemes. For example, if an additively homomorphic encryption is used in an e-voting scheme, one can obtain an encryption of the sum of all ballots from their encryption. Consequently, it becomes possible that a single decryption will reveal the result of the election. That is to say, it is unnecessary to decrypt all ciphertexts one by one.

Homomorphic encryption schemes supporting either addition or multiplication operations (but not both) had been intensively studied, *e.g.*, Goldwasser-Micali encryption [20], ElGamal encryption [14], and Paillier encryption [8, 28]. A fully homomorphic encryption (FHE) is defined as a scheme which allows anyone to perform arbitrarily computations on encrypted data, despite not having the secret decryption key. In 2009, Gentry [15] proposed a FHE scheme over ideal lattices, which is capable of evaluating some functions in the encrypted domain. Since then, the primitive has interested many researchers. The Gentry encryption [15] is a fully homomorphic encryption scheme, which makes it possible to evaluate some functions in the encrypted domain. After that, some new FHE schemes appeared.

At Eurocrypt'10, Gentry, Halevi and Vaikuntanathan [19] proposed a FHE scheme based on the Learning With Error (LWE) problem. In 2010, van Dijk, *et al.* [31] constructed a simple FHE scheme using only elementary modular arithmetic. At Crypto'11, a FHE scheme working over integers with shorter public keys and a FHE scheme based on ring-LWE were presented by Coron *et al.* [13], Brakerski and Vaikuntanathan [5], separately. At FOCS'11, a FHE scheme based on standard LWE by Brakerski and Vaikuntanathan [4, 6], and a FHE scheme using depth-3 arithmetic circuits by Gentry and Halevi [16], have interested many audiences. In 2012, Brakerski, Gentry and Vaikuntanathan [3] designed a leveled FHE scheme without bootstrapping. At Eurocrypt'13, Cheon, *et al.* [11] investigated the problem of batching FHE schemes over integers. In 2013, Brakerski, Gentry and Halevi [2] discussed the problem of packing ciphertexts in LWE-based homomorphic encryption.

In 2015, Castagnos and Laguillaumie [10] proposed a linearly homomorphic encryption scheme whose security relies on the hardness of the decisional Diffie-Hellman problem. Recently, Cheon and Kim [12] introduced a hybrid

homomorphic encryption which combines public-key encryption and somewhat homomorphic encryption in order to reduce the storage requirements for some applications.

FHE makes it possible to enable secure storage and computation on the cloud. However, current homomorphic encryption schemes are still inefficient. For example, key generation in Gentry's FHE scheme takes from 2.5 seconds to 2.2 hours [17]. A recent implementation required 36 hours for a homomorphic evaluation of AES [18]. One of the most remarkable things about these implementations is that the computations did not involve common arithmetic expressions and relational expressions. The works [1, 21, 25, 26, 30, 32] discussed the possible applications of FHE. Some outsourcing schemes [7, 9, 22, 23, 24] using homomorphic properties were flawed because of neglecting incompatibility of numerical computations with the arithmetic of underlying finite domains.

In this paper, we want to stress that any computations performed on encrypted data are constrained to the underlying domain (finite fields or rings). This restriction makes the primitive useless for most computations involving common arithmetic expressions, logical expressions and relational expressions, because the incompatibility of numerical computation with underlying encoding transformation over finite domains. It is only applicable to the computations related to modular arithmetic. Some researchers have neglected the differences between common arithmetic and modular arithmetic, and falsely claimed that FHE enables arbitrary computations on encrypted data. We here reaffirm that cryptography uses modular arithmetic a lot in order to obscure and dissipate the redundancies in plaintext, not to perform any numerical calculations.

We revisit Dijk-Gentry-Halevi-Vaikuntanathan FHE scheme [31] and Nuida-Kurosawa FHE scheme [27] under the client-server computing model. The former encrypts bit by bit. The latter works over the underlying domain $\mathbb{Z}_Q$, where Q is a prime. We find that in Dijk-Gentry-Halevi-Vaikuntanathan scheme the server can not decide the carries by the encrypted data, and in Nuida-Kurosawa scheme it is impossible to find an invertible transformation $\mathcal{T}$ from any practical floating point number system to the field $\mathbb{Z}_Q$. Therefore, in both schemes the server can not return right values to the client even though the server is asked to help to evaluate the simple function $f(x, y) = x + y$.

In view of the limitations mentioned above, we believe it might be an overstated claim that FHE is of great importance to cloud computing. To the best of our knowledge, it is the first time to practically discuss the applications of FHE schemes in client-server computing scenario.

2 The Real Goal of Using Modular Arithmetic in Cryptography

Any calculation needs an describing expression, which consists of variables, constants and operators. There are three kinds of expressions: arithmetic expressions, logical expressions and relational expressions. Arithmetic operators include addition $(+)$, substraction $(-)$, multiplication $(*)$, division $(/)$, integer-division $(\backslash)$, modulus (Mod), and so on.

Like common arithmetic, modular arithmetic is commutative, associative, and distributive. Suppose that a, b are in the decryption domain $\mathbb{Z}_p$ where p is a prime, $E(\cdot)$ is a fully homomorphic encryption algorithm, and $D(\cdot)$ is the corresponding decryption algorithm. Then it has the following properties.

$$\begin{aligned} D(E(a) + E(b)) &= D(E(a+b)) = a + b \bmod p \\ D(E(a) \cdot E(b)) &= D(E(ab)) = ab \bmod p. \end{aligned}$$

Generally,

$$\begin{aligned} a + b &\neq (a + b \bmod p), \qquad ab \neq (ab \bmod p) \\ a < b &\not\Longrightarrow E(a) < E(b), \qquad E(a) < E(b) \not\Longrightarrow a < b \end{aligned}$$

We here want to stress that cryptography uses modular arithmetic a lot, because it can obscure the relationship between the plaintext and the ciphertext, and dissipate the redundancy of the plaintext by spreading it out over the ciphertext. It is well known that confusion and diffusion are the two basic techniques for obscuring the redundancies in a plaintext message. They could frustrate attempts to study the ciphertext looking for redundancies and statistical patterns. Practically speaking, the real goal of using modular arithmetic in cryptography is to *obscure and dissipate the redundancies in plaintext, not to perform any numerical calculations.*

To see this, we will have a close look at two typical FHE schemes proposed by Dijk *et al.* [31], Nuida and Kurosawa [27]. The former encrypts bit by bit. The underlying domain for the latter is $\mathbb{Z}_Q$, where Q is a prime.

3 Dijk-Gentry-Halevi-Vaikuntanathan FHE Scheme

3.1 Description

At Eurocrypt 2010, Dijk *et al.* [31] constructed an FHE scheme. For convenience, we here only describe the symmetric version of the Dijk-Gentry-Halevi-Vaikuntanathan FHE scheme as follows.

KeyGen(λ): For a security parameter λ, pick an odd number $p \in [2^{\lambda-1}, 2^{\lambda})$ and set it as the secret key.

Encrypt(p, m): Given a bit $m \in \{0, 1\}$, compute the ciphertext as

$$c = pq + 2r + m$$

where the integers q, r are chosen at random in some other prescribed intervals, such that $2r$ is smaller than $p/2$ in absolute value.

Decrypt(p, c): $m = (c \bmod p) \bmod 2$.

Additively homomorphic property: If $c_1 = pq_1 + 2r_1 + m_1$ and $c_2 = pq_2 + 2r_2 + m_2$, then

$$m_1 + m_2 = (c_1 + c_2 \bmod p) \bmod 2.$$

Multiplicatively homomorphic property: If $c_1 = pq_1 + 2r_1 + m_1$ and $c_2 = pq_2 + 2r_2 + m_2$, then

$$m_1 \cdot m_2 = (c_1 \cdot c_2 \bmod p) \bmod 2.$$

Notice that these homomorphic properties hold only on the condition that computations are constrained to the prescribed modulus $p, 2$. This restriction makes the scheme impossible to deal with any numerical calculations without knowing the modulus p.

3.2 An Example

Suppose that one client sets $p = 7919$ as his secret key. He has two numbers $a = 5$, $b = 3$, and wants a server to help him to compute $c = a + b$. Now, he encrypts two numbers a and b as follows (see Table 1).

Table 1: Ciphertexts of 5 and 3 w.r.t. the secret key 7919

$a = 5$	$\boxed{1}$	$\boxed{0}$	$\boxed{1}$
	$7919 \times 1325 + 2 \times 57 + 1$ $\boxed{10492790}$	$7919 \times 3168 + 2 \times 49 + 0$ $\boxed{25087490}$	$7919 \times 5247 + 2 \times 63 + 1$ $\boxed{41551120}$
$b = 3$		$\boxed{1}$	$\boxed{1}$
		$7919 \times 5538 + 2 \times 85 + 1$ $\boxed{43855593}$	$7919 \times 6214 + 2 \times 74 + 1$ $\boxed{49208815}$

The client sends two ciphertexts

$$\underbrace{\boxed{10492790}, \boxed{25087490}, \boxed{41551120}}_{x} \text{ and } \underbrace{\boxed{43855593}, \boxed{49208815}}_{y}$$

to a server and asks the server to compute the function

$$f(x, y) = x + y.$$

Hence, the server may return the values

$$\boxed{10492790}, \boxed{68943083}, \boxed{90759935}$$

to the client. Thus, the client decrypts the returned values as follows

$$(10492790 \bmod p) \bmod 2 = 1,$$
$$(68943083 \bmod p) \bmod 2 = 1,$$
$$(90759935 \bmod p) \bmod 2 = 0,$$

and obtains the number $(110)_2 = 6$, not the right number 8. See the following Table 2 for the process.

Table 2: An example for Dijk-Gentry-Halevi-Vaikuntanathan FHE scheme

Client		Server
Input: $p = 7919$, $a = 5$, $b = 3$		$f(x, y) = x + y$
Encryption: $3 \to \underbrace{\boxed{43855593}, \boxed{49208815}}_{y}$, $5 \to \underbrace{\boxed{10492790}, \boxed{25087490}, \boxed{41551120}}_{x}$.	$\xrightarrow{x,y}$	
	$\xleftarrow{\hat{c}}$	$f(x, y) = \underbrace{\boxed{10492790}, \boxed{68943083}, \boxed{90759935}}_{\hat{c}}$
Decryption: $\hat{c} \to \underbrace{\boxed{1}, \boxed{1}, \boxed{0}}_{c}$		

3.3 Wrong Output

What's wrong with the above process? *The returned values miss all carries because the server can not decide the carries by the encrypted data.*

One might argue that the client himself can construct a Boolean circuit which contains the carries and send the circuit to the server. For example, Prof. Boaz Tsaban (in personal communications) explained that:

> In adding two k-bit number, any output bit (out of the k+1 bits of the sum) is a concrete, known boolean function of the $2k$ input bits. Thus, the server may apply the $k + 1$ functions to the $2k$ encrypted input bits, and the result can be sent to the client. The decryption will be correct, by the homomorphic property.

The argument is unacceptable because the client is assumed to be of weak computational capability. If the client can construct such a Boolean circuit, then he can directly evaluate the circuit, instead of asking a server to help him to evaluate it.

4 Nuida-Kurosawa FHE Scheme

In Dijk-Gentry-Halevi-Vaikuntanathan FHE scheme, the message space is $\mathbb{Z}_2$. The scheme is very inefficient because it has to generate 256 or more bits in order to mask one bit. At Eurocrypt 2015, Nuida and Kurosawa [27] extended the scheme to the message space $\mathbb{Z}_Q$ where Q is any prime. We here only describe the symmetric version of Nuida-Kurosawa FHE scheme as follows.

4.1 Description

KeyGen(λ): For a security parameter λ, pick an odd number $p \in [2^{\lambda-1}, 2^{\lambda})$ and a prime Q. Set p as the secret key (Q is published).

Encrypt(p, m): Given a message $m \in \mathbb{Z}_Q$, compute the ciphertext as

$$c = pq + Qr + m$$

where the integers q, r are chosen at random in some other prescribed intervals, such that Qr is smaller than $p/2$ in absolute value.

Decrypt(p, c): $m = (c \bmod p) \bmod Q$.

Additively Homomorphic Property: If $c_1 = pq_1 + Qr_1 + m_1$ and $c_2 = pq_2 + Qr_2 + m_2$, then

$$m_1 + m_2 = (c_1 + c_2 \bmod p) \bmod Q.$$

Multiplicatively Homomorphic Property: If $c_1 = pq_1 + Qr_1 + m_1$ and $c_2 = pq_2 + Qr_2 + m_2$, then

$$m_1 \cdot m_2 = (c_1 \cdot c_2 \bmod p) \bmod Q.$$

4.2 An Example

Suppose that one client sets $p = 22801763489$ as his secret key and sets $Q = 15485863$. He has two numbers $a = 0.1$, $b = 2.3$, and wants a server to help him to compute $c = a + b$.

First, he has to transform $a = 0.1$, $b = 2.3$ into integers $\bar{a}, \bar{b}$ such that $\bar{a}, \bar{b} \in \mathbb{Z}_Q$. Denote the transformation by $\mathcal{T}$. Second, he encrypts $\bar{a}, \bar{b}$ and obtains the corresponding ciphertexts $\hat{a}, \hat{b}$. Third, he sends $\hat{a}, \hat{b}$ to a server. The server then takes $\hat{a}, \hat{b}$ as the inputs of the function $f(x, y) = x + y$. Finally, the server returns $\hat{c} = f(\hat{a}, \hat{b})$ to the client. See the following Table 3 for the process.

Table 3: An example for Nuida-Kurosawa FHE scheme

Client		Server
Input: $p = 22801763489$, $Q = 15485863$; $a = 0.1$, $b = 2.3$		$f(x, y) = x + y$
Encoding transformation $\mathcal{T}$: $a \to \bar{a}$, $b \to \bar{b}$ such that $\bar{a}, \bar{b} \in \mathbb{Z}_Q$.		
Encryption: $\bar{a} \to \hat{a}$, $\bar{b} \to \hat{b}$.	$\xrightarrow{\hat{a},\hat{b}}$	
	$\xleftarrow{\hat{c}}$	Computation $f(\hat{a}, \hat{b}) \to \hat{c}$
Decryption: $\hat{c} \to \bar{c}$		
Inverse Transformation $\mathcal{T}^{-1}$: $\bar{c} \to c$.		

4.3 Incompatibility of Numerical Computation with Underlying Encoding Transformation over Finite Domains

What's wrong with the above process? It is impossible to find an invertible encoding transformation from any practical floating point number system to the field $\mathbb{Z}_Q$.

Note that most encryption algorithms must run over some finite domains. One has to transform all inputting characters into integers in the domain. That means *an invertible encoding transformation is necessary for any encryption scheme*. This requirement is so obvious that it is often neglected.

This condition is easily satisfied if all inputting characters are indeed viewed as characters. But when some inputting characters are viewed as floating point numbers and they are used for some arithmetic computations, it is impossible to find such a universal invertible encoding transformation that maps any floating point number to an integer in a prescribed finite domain.

Table 4: A part of ASCII encoding table

character	ASCII code	character	ASCII code
0	48	6	54
1	49	7	55
2	50	8	56
3	51	9	57
4	52	·	250
5	53		

We here describe a possible encryption-decryption process for the floating point numbers 0.1 and 2.3. The ASCII encoding method will map $0.1, 2.3$ to two integers in the field $\mathbb{Z}_{15485863}$.

If a server performs the operator of addition on the encrypted data, $\hat{a}, \hat{b}$, then it gives

$$\hat{c} = \hat{a} + \hat{b} = 7332965072166439 2 + 147988712393689577 = 221318363115353969.$$

The server returns the value to the client. The client will obtain

$$\bar{c} = (221318363115353969 \bmod p) \bmod Q = 6550628.$$

Notice that

$$6550628 = 99 \times 256^2 + 244 \times 256 + 100 \xrightarrow{\mathcal{T}^{-1}} \boxed{99}\boxed{244}\boxed{100}.$$

Table 5: A possible encryption-decryption process for the floating point numbers 0.1 and 2.3

$a = 0.1 \xrightarrow{\text{ASCII}} \boxed{48}\boxed{250}\boxed{49} \xrightarrow{\mathcal{T}} \bar{a} = 48 \times 256^2 + 250 \times 256 + 49 = 3209777 \xrightarrow{q=3215964, r=13}$
$\hat{a} = 73329650721664392 \xrightarrow{\text{mod } p, \text{ mod } Q} \bar{a} = 3209777 \xrightarrow{\mathcal{T}^{-1}} \boxed{48}\boxed{250}\boxed{49} \xrightarrow{\text{ASCII}} 0.1$
$b = 2.3 \xrightarrow{\text{ASCII}} \boxed{50}\boxed{250}\boxed{51} \xrightarrow{\mathcal{T}} \bar{b} = 50 \times 256^2 + 250 \times 256 + 51 = 3340851 \xrightarrow{q=6490231, r=9}$
$\hat{b} = 147988712393689577 \xrightarrow{\text{mod } p, \text{ mod } Q} \bar{b} = 3340851 \xrightarrow{\mathcal{T}^{-1}} \boxed{50}\boxed{250}\boxed{51} \xrightarrow{\text{ASCII}} 2.3$

It does not correspond to the wanted number 2.4 when ASCII encoding method is used.

5 The Inherent Drawback

Cloud computing refers to the practice of transferring computer services such as computation or data storage to other redundant offsite locations available on the Internet, which allows application software to be operated using internet-enabled devices. It benefits one from the existing technologies and paradigms, even though he is short of deep knowledge about or expertise with them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles. Usually, cloud computing adopts the client-server business model.

What computations do you want to outsource privately? Backup your phone's contacts directory to the cloud? Ask the cloud to solve a mathematic problem in your homework? Do a private web search? $\cdots$. It seems obvious that the daily computational tasks are rarely constrained by some prescribed modulus. Moreover, the client-server computing model can not deal with relational expressions which are defined over plain data, not over encrypted data. This is because

$$a < b \not\Longrightarrow E(a) < E(b), \qquad E(a) < E(b) \not\Longrightarrow a < b.$$

In view of this drawback of FHE and the flaws of two typical schemes mentioned above, we think FHE seems inappropriate for cloud computing.

The problem that what computations are worth delegating privately by individuals and companies to untrusted devices or servers remains untouched. We think the cloud computing community has not yet found a good for-profit model convincing individuals to pay for this or that computational service.

6 Conclusion

We reaffirm the role of modular arithmetic in modern cryptography and show that FHE is inappropriate for cloud computing because any FHE scheme does work over some finite domains which leads to the incompatibility of numerical computation with underlying encoding transformation. When two decrypted number are added, one cannot decide the carries without knowing the secret decryption key. Moreover, there is no an invertible transformation from any practical floating point number system to the encryption domain which makes it impossible to tackle numerical calculations. We think the primitive of FHE might be of little importance to client-server computing scenario.

Acknowledgements

We thank the National Natural Science Foundation of China (61303200, 61411146001).

References

[1] B. Balusamy and et al., "A secured access control technique for cloud computing environment using attribute based hierarchical structure and token granting system," *International Journal of Network Security*, vol. 19, no. 4, pp. 559–572, 2017.

[2] Z. Brakerski, C. Gentry, , and S. Halevi, "Packed ciphertexts in lwe-based homomorphic encryption," in *Proceedings of International Conference on Practice and Theory in Public-Key Cryptography (PKC'13)*, pp. 1–13, Nara, Japan, Feb. 2013.

[3] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," in *Proceedings of ACM Conference on Innovations in Theoretical Computer Science (ITCS'12)*, pp. 309–325, Cambridge, MA, USA, Jan. 2012.

[4] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," in *Proceedings of IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS'11)*, pp. 97–106, Palm Springs, CA, USA, Oct. 2011.
[5] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'11)*, pp. 505–524, Santa Barbara, California, USA, Aug. 2011.
[6] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.
[7] Z. J. Cao and L. H. Liu, "Comment on 'harnessing the cloud for securely outsourcing large-scale systems of linear equations'," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1551–1552, 2016.
[8] Z. J. Cao and L. H. Liu, "The paillier's cryptosystem and some variants revisited," *International Journal of Network Security*, vol. 19, no. 1, pp. 89–96, 2017.
[9] Z. J. Cao, L. H. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifible outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.
[10] G. Castagnos and F. Laguillaumie, "Linearly homomorphic encryption from ddh," in *Proceedings of Topics in Cryptology, The Cryptographer's Track at the RSA Conference (CT-RSA'15)*, pp. 487–505, San Francisco, CA, USA, Apr. 2015.
[11] J. Cheon and et al., "Batch fully homomorphic encryption over the integers," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'13)*, pp. 315–335, Athens, Greece, May 2013.
[12] J. H. Cheon and J. Kim, "A hybrid scheme of public-key encryption and somewhat homomorphic encryption," *IEEE Transaction on Information Forensics and Security*, vol. 10, no. 5, pp. 1052–1063, 2015.
[13] J. Coron and et al., "Fully homomorphic encryption over the integers with shorter public keys," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'11)*, pp. 487–504, Santa Barbara, California, USA, Aug. 2011.
[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'84)*, pp. 10–18, Santa Barbara, California, USA, Aug. 1984.
[15] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC'09)*, pp. 169–178, Bethesda, MD, USA, May 2009.
[16] C. Gentry and S. Halevi, "Fully homomorphic encryption without squashing using depth-3 arithmetic circuits," in *Proceedings of IEEE Annual Symposium on Foundations of Computer Science (FOCS'11)*, pp. 107–116, Palm Springs, CA, USA, Oct. 2011.
[17] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'11)*, pp. 129–148, Tallinn, Estonia, May 2011.
[18] C. Gentry, S. Halevi, and N. Smart, "Homomorphic evaluation of the aes circuit," *IACR Cryptology ePrint Archive*, no. 99, 2012.
[19] C. Gentry, S. Halevi, and V. Vaikuntanathan, "A simple bgn-type cryptosystem from lwe," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'10)*, pp. 506–522, French Riviera, May 2010.
[20] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC'82)*, pp. 365–377, San Francisco, California, USA, May 1982.
[21] C.H. Ling, C.C. Lee, C.C. Yang, and M.S. Hwang, "A secure and efficient one-time password authentication scheme for wsn," *International Journal of Network Security*, vol. 19, no. 2, pp. 177–181, 2017.
[22] L. H. Liu and Z. J. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.
[23] L. H. Liu, Z. J. Cao, and O. Markowitch, "A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 79–82, 2016.
[24] L. H. Liu and et al., "Computational error analysis of two schemes for outsourcing matrix computations," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 23–31, 2017.
[25] H. Ma, T. Peng, and Z. H. Liu, "Directly revocable and verifiable key-policy attribute-based encryption for large universe," *International Journal of Network Security*, vol. 19, no. 2, pp. 272–284, 2017.
[26] J. Modi and et al., "A secure communication model for expressive access control using cp-abe," *International Journal of Network Security*, vol. 19, no. 2, pp. 193–204, 2017.

[27] K. Nuida and K. Kurosawa, "(batch) fully homomorphic encryption over integers for non-binary message spaces," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'15)*, pp. 537–555, Sofia, Bulgaria, Apr. 2015.
[28] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'99)*, pp. 223–238, Prague, Czech Republic, May 1999.
[29] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation (R. Demillo and et al. (Eds.))*, pp. 169–180, 1978.
[30] C.Y. Tsai, C.Y. Liu, S.C. Tsaur, and M.S. Hwang, "A publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms," *International Journal of Network Security*, vol. 19, no. 3, pp. 443–448, 2017.
[31] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'10)*, pp. 24–43, French Riviera, May 2010.
[32] C. M. Wang and et al., "A general formal framework of analyzing selective disclosure attribute-based credential systems," *International Journal of Network Security*, vol. 19, no. 5, pp. 794–803, 2017.

Biography

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Yang Li is currently pursuing his M.S. degree from Department of Mathematics, Shanghai Maritime university. His research interests include combinatorics and cryptography.

Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms

Diaa Salama AbdElminaam

(Corresponding author: Diaa Salama AbdElminaam)

Information Systems department, Faculty of Computers and Informatics, Benha University, Egypt
(Email: ds_desert@yahoo.com)

(Received Dec. 10, 2017; revised and accepted Feb. 8, 2018)

Abstract

Cryptography considered from the old science that are human learn it and motivated it through all past years, Cryptography consist of two main items encryption and decryption, encryption mean we take the plain text and convert it a new text can't be read and can't be understood by any one, except the recipient. Through the motivations of technology and using the internet in all human fields, Cryptography was become widely used over many people and transportation data protocols, so encryption using the famous algorithms isolated was considered a high risk and date are not safe or can't away from hackers. So now, in this paper we will introduce a new hybrid technique for Cryptography using two algorithms (AES and Blowfish). This new technique gathering between symmetric and a symmetric encryption. This Combination of using symmetric and a symmetric technique will give us the high security and everyone have his private key that can be used for decryption process by many people at the same time. This technique has also benefit for making hashing for Key by using MD5 hashing function that will make hashing the key in encryption process and make the same process in decryption. This will increase the security of the key plus increasing security using hybrid cryptography. Finally, we will have cipher text cannot be decrypted except by the recipient.

Keywords: AES; Blowfish; Cryptography; Decryption; DES; Encryption; Hybrid Cryptography

1 Introduction

Security was become the main issue that face every body that using internet in their daily work, security can be achieved through five main categories Authentication, Confidentiality and Integrity as illustrated in Figure 1 [5, 9, 16].

- Authentication: mean that unauthorized user cannot access your site or your network.
- Authorization: only authentication user was allowed to access information.
- Integrity: Check that the date was transmit doesn't have any modification in its way to receiver, and this data still valid.
- Audit: is a systematic evaluation of the information security.
- Availability is best ensured by rigorously maintaining information or data.

There are some terms must be introduced about cryptography such as the following and it shown in Figure 2 [24]:

- Plain text: is the text message that someone want to encrypt it and send it to another body, and be sure that no one can read it except the recipient.
- Key: this is the main item that must be known between the sender or receiver message, and if any other one know it all message encrypted by this key will be hacking in very easy way. There are two types of key Public and Private key, public key can make encryption and decryption in some algorithms and in other algorithms there are a privet key that can decrypt message with specific key only.
- Encryption algorithm: the used algorithm to make encryption process, and there are many worked algorithms that are symmetric and a symmetric that user can choose from them.

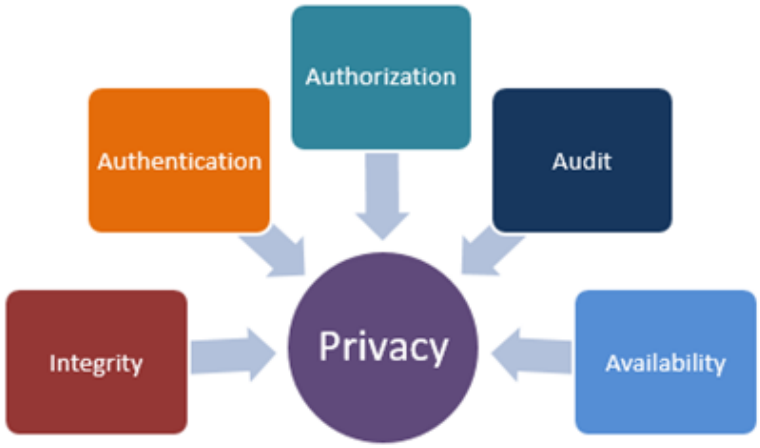

Figure 1: Security factors

- Cipher text: the result of encryption algorithm after applying specific cryptography algorithm for encryption over plain text.
- Decryption: this process concerned with return cipher text to its main form or to the main plain text again.

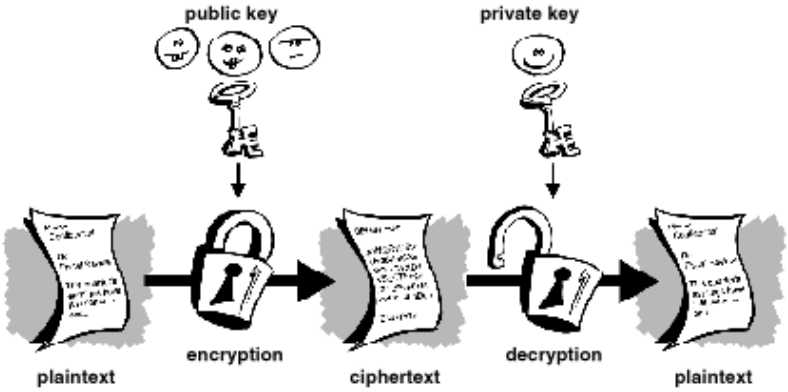

Figure 2: Cryptography process

- Symmetric key: can be named as privet key cryptography, this technique use private key and only one key for cryptography algorithm, in other way encryption and decryption done using one key, and this key must know only by sender and receiver [10, 17]. The main famous algorithms that use this technique Data Encryption Standard (DES) and Advanced Encryption Standard (AES).
- A symmetric key: can be named as public key cryptography, this technique need special keys to doing the cryptography process and there are common algorithms that use this technique as RSA and Elliptic Curve Cryptography (ECC) [1].

There are some advantages and disadvantages for using a symmetric rather than symmetric cipher as following: the main most advantage of asymmetric over symmetric is that no secret channel is necessary for the exchange of the public key. The receiver needs only to be assured of the authenticity of the public key [7]. Symmetric ciphers require a secret channel to send the secret key generated by sender and send to receiver to use it later, Asymmetric ciphers also create lesser key-management problems than symmetric ciphers [15]. Only the second keys are needed for n entities to communicate securely with one another. Disadvantage of asymmetric ciphers over symmetric ciphers is that they tend to be slower than symmetric cryptography. Another disadvantage is that symmetric ciphers can be hacked through a multi trying attack, in which all possible keys are used until one of them succeeded to decrypt the cipher text.

In addition, by motivation in technology and the abilities of server this process will not take a long time until hacker will get the right key, and decrypt the text in easy way.MD5 (technically called MD5 Message-Digest Algorithm) is a cryptographic hash function whose main purpose is to verify that a file has been unaltered [19]. Instead of confirming that two sets of data are identical by comparing the raw data, MD5 does this by producing a checksum on both sets, and then comparing the checksums to verify that they're the same. MD5 has certain flaws and so it isn't useful for advanced encryption applications, but it's perfectly acceptable to use it for standard file verifications [8].

In this paper, we will introduce a new hybrid technique for Cryptography using two algorithms (AES and Blowfish). This new technique gathering between symmetric and a symmetric encryption. This Combination of using symmetric and a symmetric technique will give us the high security and everyone have his private key that can be used for decryption process by many people at the same time. This technique has also benefit for making hashing for Key by using MD5 hashing function that will make hashing the key in encryption process and make the same process in decryption. This will increase the security of the key plus increasing security using hybrid cryptography. Finally, we will have cipher text cannot be decrypted except the recipient.

This paper will be organized as following: first, this paper will be showing the previous or similar worked hybrid cryptography technique, next section will present the new or the proposed hybrid cryptography technique. Next section will present the results of comparison between the following cryptography algorithms DES, AES, Blowfish and presented hybrid technique (AES-Blowfish) and last section will introduce the conclusion of this paper.

2 Related Works

2.1 (Subasree) Cryptography Architecture

As shown in Figure 3, there are a plain text in the above of architecture, it encrypted by ECC, and the result encrypted or cypher text is transmit through secured channel [6]. Simultaneously, MD5 was used to hash the plain text, which already encrypted using ECC. In the same time hash value was encrypted using DUAL RSA, and then transmit it to the destination. When applying this Cryptography Architecture, the plain text cannot been extracted in easy way, as you think, because the Hash value was encrypted with DUAL RSA and calculated with MD5 [4]. However, this technique is complex but if any person has the private key, he can decrypt the cipher text in easy way.

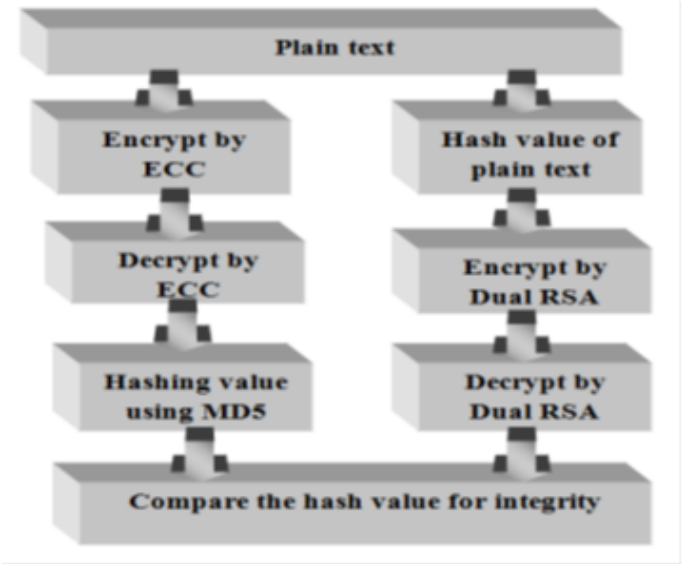

Figure 3: (Subasree) Security architecture

2.2 (Dubal) Cryptography Architecture

As shown in Figure 4, the plain text is encrypted with key by using ECDH [12, 13, 21]. The used algorithm is DUAL RSA, this algorithm takes the main information and also take key to produce the cipher text, and also use the digital signature to increase security and increase authentication that was produced by the following algorithm ECDSA.

In the same time of encryption, MD5 hash value was used for producing the cipher text, then the transmission channel should be used to transmit the new encrypted cipher text. On the other side, decryption will be making

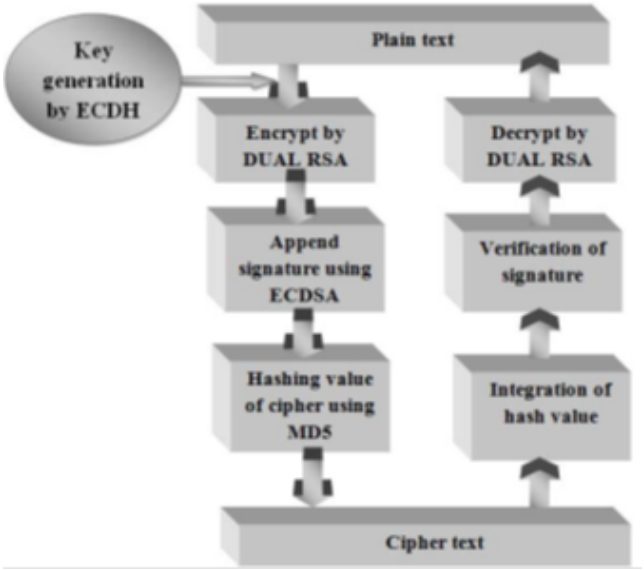

Figure 4: (Dubal) Security architecture

by doing the following steps, hash value should be trusted and checked first and decryption will be making by using DUAL RSA [14]. Hence, the plaintext can be derived. In this protocol, the intruder may be trapped by both the encryption by the DUAL RSA with the key of ECDH algorithm. Although using of the following algorithms DUAL RSA and ECDH the security should be increased but still there are a big problem with the private key [2], if it was hacked.

2.3 Hybrid Cryptography Protocol (HCP)

This algorithm contains from two phases encryption and decryption phase; this paper will present the different steps in every phase with more details as following [18, 20].

2.3.1 Encryption Phase

As Figure 5 shown that the plain text was divided into number of block, each block consists of 128 bits, then every block will be divided for two parts, every part will be encrypted with different algorithm, first block will be encrypted using (AES and ECC) hybrid encryption algorithm, second block will be encrypted using XOR-DUAL RSA algorithm.

ECC used for protection of the secret key, and according to the mathematical problem, ECC can be solved by not making sub exponential but with doing fully exponential, also ECC needs smaller key size and less memory size.

On the other side DUAL RSA are used for making fast encryption and decryption, which DUAL RSA was considered faster four times than standard RSA. Another point must be taken in consideration that XOR Encryption algorithm is one of a symmetric algorithm. This means that the same key is used for both encryption and decryption.

2.3.2 Decryption Phase

As presented below in Figure 6, the encrypted or cipher text will be divided into number of n blocks, each block as encryption phase will be consist of 128 bits. Then each block will be divided to two parts, now we have two cipher text, the hash value of every block will be compared to check if the text is hacked or there are any corruption of data, after check succeeded decryption algorithm will go through as shown in Figure 6 [22].

3 The Proposed Hybrid Cryptography

The proposed hybrid cryptography consist of two phasing one for encryption & the second for decryption, and it will be presented as following:

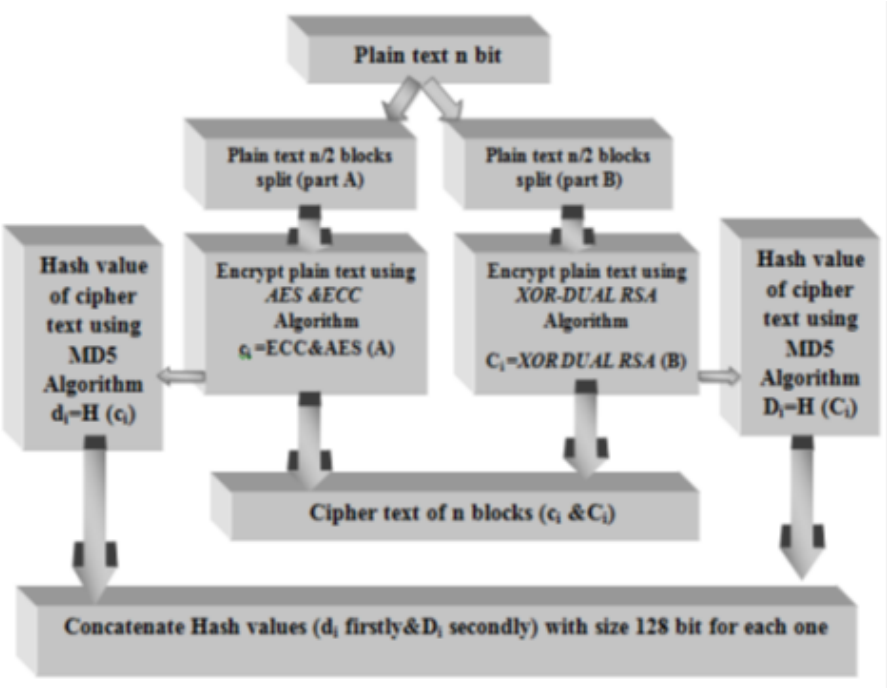

Figure 5: Encryption phase

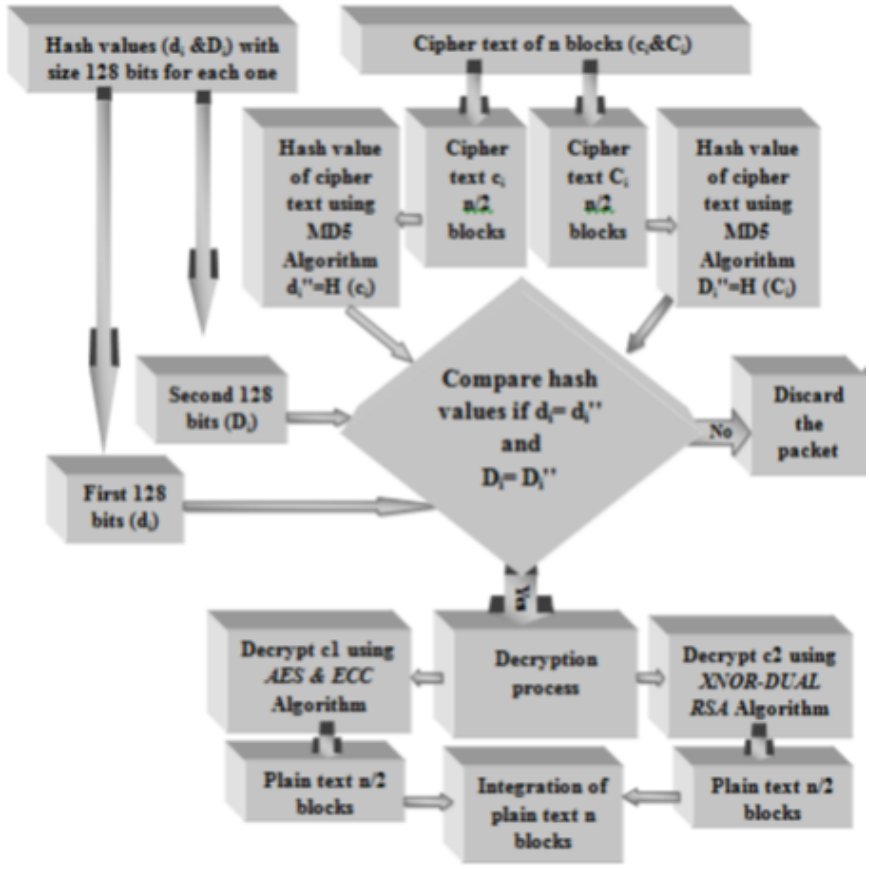

Figure 6: Decryption phase

Encryption Phase: As shown in the below Figure 7, the plain text was divided to n blocks and each block will be divided to two parts one part will be encrypted using (AES) and other by blowfish, next the result of two algorithms will be concatenated and create one text for first block and so on until finished all blocks, in the same time the key used will be hashed using MD5 and used the hash result as key for encryption in AES & Blowfish algorithms.

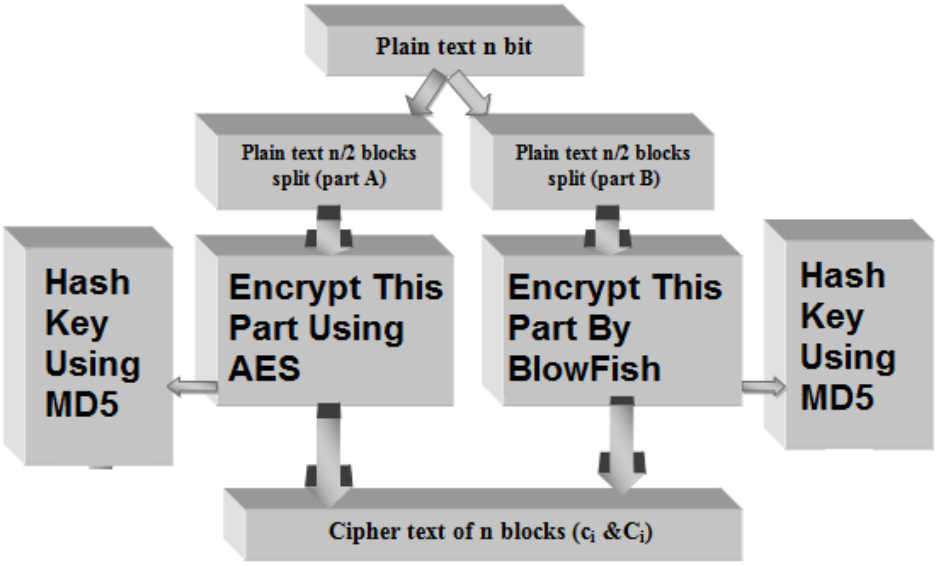

Figure 7: Encryption phase

Decryption Phase: as shown in Figure 8, the cipher text will be dived also to n block and the key will be hashed again to be used in decryption process, after that each block will be dived to two parts, first one will be decrypted using AES with hashed Key, and the second will be decrypted using blowfish algorithm with hashed key.

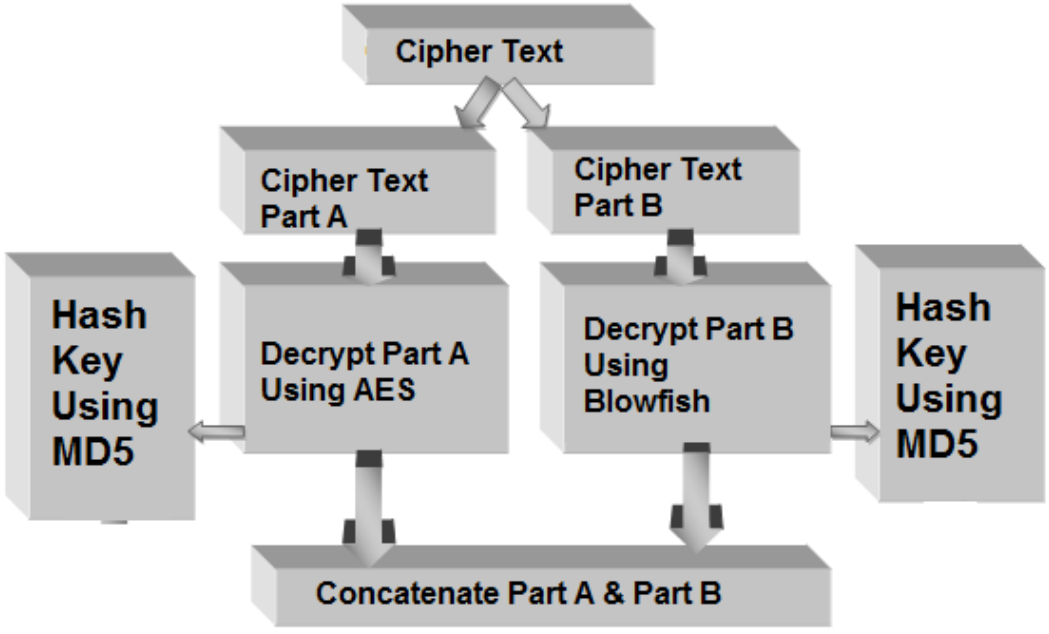

Figure 8: Decryption phase

4 Numerical Results

A. The size of the cipher text As shown below in Table I output of the encryption process. This table shows the size of the encrypted or cipher text in bytes.

B. Time of Encryption and Decryption Processes As shown in Tables 2 & 3 the time for encryption and decryption process for three different techniques.

C. Throughput To calculate the throughput, we used the Encryption time as the following equation: Throughput = size of cipher text / time taken in encryption. Table 4 shows the throughput result of the proposed hybrid cryptography technique compared with the existing algorithms (DES & AES) for different sizes of plain text [3, 11].

Table 1: Size of cipher text (bytes)

Size of plain text (bytes)	DES	AES	AES & Blowfish	AES & RSA
112	141	141	356	378
2305	2654	2630	3007	3790
7894	8301	8505	10147	11103
153422	153783	153845	158607	168302

Table 2: Time of encryption (ms)

Size of plain text (bytes)	DES	AES	AES & Blowfish	AES & RSA
112	2070	2073	4389	4876
2305	3986	3994	5883	5994
7894	14981	15107	33900	34101
153422	106781	106792	194527	201305

Table 3: Time of decryption (ms)

Size of plain text (bytes)	DES	AES	AES & Blowfish	AES & RSA
112	1034	1034	3278	3497
2305	1675	1675	2634	3012
7894	1534	1534	12641	13501
153422	2246	2246	103314	103987

Table 4: Throughput

Size of plain text (bytes)	DES	AES	AES & Blowfish	AES & RSA
112	68.115	68.017	81.111	77.522
2305	665.830	658.487	511.133	632.298
7894	554.101	562.984	299.321	325.591
153422	1478.085	1440.604	815.346	836.054

5 Conclusion

In this paper, we introduced a new hybrid technique for Cryptography using two algorithms (AES and Blowfish). This new technique gathering between symmetric and a symmetric encryption. This Combination of using symmetric and a symmetric technique will give us the high security and everyone have his private key that can be used for decryption process by many people at the same time. This technique has also benefit for making hashing for Key by using MD5 hashing function that will make hashing the key in encryption process and make the same process in decryption. This will increase the security of the key plus increasing security using hybrid cryptography. Finally we will have cipher text cannot be decrypted except by the recipient.

References

[1] L. Abusalah, A. Khokhar, M. Guizan, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78-93, 2008.

[2] M. Akhlaq, M. N. Jafri, *Addressing Security Concerns of Data Exchange in AODV Protocol*, World Academy of Science, Engineering and Technology, 2006.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[4] G. Anastasi, M. Conti, A. Falchi, E. Gregori, A. Passarella, "Performance measurements of mote sensor networks," in *MSWiM'04*, Venezia, Italy, Oct. 4-6, 2004.

[5] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Networks*, vol. 8, no. 5, pp. 481-494, 2002.

[6] Chipcon, *SmartRF CC1000 Preliminary Datasheet (rev. 2.1)*, 2202-04-19, Chipcon AS.

[7] Y. ChunHu, A. Perrig, D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *ACM WiSe*, San Diego, California, USA, 2003.

[8] Crossbow, MPR - Mote Processor Radio Board MIB-Mote Interface/Programming Board User's Manual, Rev A. Document 7430-0021-05, Crossbow Technology Inc, San Jose, California, Dec. 2003.

[9] R. Gupta, "Mobile adhoc network (MANETS): Proposed solution to security related issues," *Indian Journal of Computer Science and Engineering*, vol. 2. no. 5, pp. 748-46, 2011.

[10] S. Haykin and M. Moher, *Modern Wireless Communication*, Prentice Hall, 2005.

[11] X. Hou, D. Tipper, D. Yupho and J. Kabara, "GSP: Gossip-based sleep protocol for energy efficient routing in wireless sensor networks," in *The 16th International Conference on Wireless Communications*, Calgary, Alberta, Canada, 2004.

[12] M. A. Matin, M/ M. Hossain, M. F. I. Hossain, "Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN," in *International Conference for Technical Postgraduates (TECHPOS'09)*, 2009.

[13] G. Padmavathi, "CCMP-AES model with DSR routing protocol tosecure link layer and network layer in mobile adhoc networks," *International Journal of Computer Science and Engineering*, vol. 2, no. 5, pp. 1524-1531, 2010.

[14] E. A. Panaousis, G. Drew, G. P. Millar, T. A. Ramrekha, "A test-bed implementation for securing olsr in mobile ad-hoc networks," *International Journal of Network Security & Its Applications*, vol. 2, no. 4, pp. 2412-2413, 2010.

[15] P. Papadimitratos, Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02)*, San Antonio, TX, 2002.

[16] P. Papadimitratos, H. Zhou, "Secure routing for mobile ad hoc networks," in *Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02)*, San Antonio, 2002.

[17] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, pp. 51-58, 2000.

[18] E. Ramaraj, S. Karthikeyan, M. A. Hemalatha, "A design of security protocol using hybrid encryption technique (AES - Rijndael and RSA)," *International Journal of The Computer, the Internet and Management*, vol. 17. no. 1, pp. 78-86, 2009.

[19] S. S. Rizvi, "Combining private and public key encryption techniques for providing extreme secure environment for an academic institution application," in *International Journal of Network Security & Its Application*, vol. 2, no. 1, 2010.

[20] S. M. Seth, R. Mishra, "Comparative analysis of encryption algorithms for data communication," *International Journal of Scientific Engineering and Applied Science*, vol. 2, no. 2, pp. 495-498, 2016.

[21] M. H. Shnayder, B. Chen, G. W. Allen, and M. Welsh, "Simulating the power consumption of large scale sensor network applications," in *SenSys'04*, Baltimore, Maryland, USA, Nov. 3-5, 2004.

[22] T. R. Sivaramakrishnan, "Implementing end-to-end reliability and energy conservation routing to provide quality of service in mobile ad hoc networks," *European Journal of Scientific Research*, vol. 55, no. 1, pp. 28-36, 2011.

[23] S. Subasree and N. K. Sakthivel, "Design of a new security protocol using hybrid cryptography algorithms," *International Journal of Research and Reviews in Applied Sciences*, vol. 2, no. 2, Feb. 2010.
[24] Y. Xu, J. Heidemann, D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *MOBICOM'01*, 2001.

Biography

Diaa Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers & Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 specializing in Cryptography and network security. He obtained his Ph.D. degree in information system from faculty of computers and information, menufia university, Egypt. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Benha University, Egypt since 2011. He has worked on a number of research topics. Diaa has contributed more than 20+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications, Cloud Computing, Mobile Cloud Computing in international journals, international conferences, local journals and local conferences. He majors in Cryptography, Network Security, IoT, Big Data, Cloud Computing. (Mobile: +20166104747; +201019511000 E-mail: ds_desert@yahoo.com)

A Review of Cryptographic Properties of S-Boxes with Generation and Analysis of Crypto Secure S-Boxes

Sankhanil Dey and Ranjan Ghosh
(Corresponding author: Sankhanil Dey)

Institute of Radio Physics and Electronics, University of Calcutta
92 A P C Road, Kolkata-700009, India
(Email: sankhanil12009@gmail.com, sdrpe_rs@caluniv.ac.in)
(Received Nov. 25, 2017; revised and accepted Jan. 10, 2018)

Abstract

In modern as well as ancient ciphers of public key cryptography, substitution boxes find a permanent seat. Generation and cryptanalysis of 4-bit as well as 8-bit crypto S-boxes is of utmost importance in modern cryptography. In this paper, a detailed review of cryptographic properties of S-boxes has been illustrated. The generation of crypto S-boxes with 4-bit as well as 8-bit Boolean functions (BFs) and Polynomials over Galois field $GF(p^q)$ has also been of keen interest of this paper. The detailed analysis and comparison of generated 4-bit and 8-bit S-boxes with 4-bit as well as 8-bit S-boxes of Data Encryption Standard (DES) and Advance Encryption Standard (AES) respectively, has incorporated with example. Detailed analysis of generated S-boxes claims a better result than DES and AES in view of security of crypto S-boxes.

Keywords: Boolean Functions; Finite Fields; Galois Fields; Polynomials; S-Box; Strict Avalanche Criterion; Substitution Box

1 Introduction

Substitution box or S-box in block ciphers is of utmost importance in public key cryptography from the initial days. A 4-bit S-box has been defined as a box of (24 =) 16 elements varies from 0 to F in hex, arranged in a random manner as used in Data Encryption Standard or DES [2, 30, 116, 117]. Similarly for 8 bit S-box, number of elements are 28 or 256 varies from 0 to 255 as used in Advance Encryption Standard or AES [27, 103]. So the construction of S-boxes is a major issue in cryptology from initial days. Use of Irreducible Polynomials to construct S-boxes had already been adopted by crypto community. But the study of IPs has been limited to almost binary Galois field $GF(2^q)$ as used in AES S-boxes [27, 103]. So it is important to study 4-bit BFs, 8-bit BFs and polynomials over Galois Field $GF(p^q)$ where p¿2 in public key cryptography. A brief literature study on Security in cryptography and polynomials has been elaborated in sec.2.

A 4-bit Boolean Function (BF) gives 1-bit output for 4 input bits [2]. represented in the form of a 16-bit output (column) vector. The Truth Table of a 4-bit BF has been represented by a 16-bit output vector each of whose bit is an output bit corresponding to 16 possibilities of 4-bit sequential

inputs from '0000' to '1111'. The 16 rows of the 4-bit sequential inputs, each bit at the same column position comprises of 16 bits and thereby four 16-bit columns provide four 4-bit input vectors which are common for all 4-bit BFs. Since there are 16 output bits so there are 216 (=65536) different possibilities whose decimal equivalent vary between 0 and 65535 [2]. Hence, 4-bit BFs have four 16-bit input vectors and 65536 possible 16-bit output vectors. Where an 8-bit BF gives 1-bit output for 8 input bits [27]. represented in the form of a 256-bit output (column) vector. The Truth Table of a 8-bit BF is represented by a 256-bit output vector each of whose bit is an output bit corresponding to 256 possibilities of 8-bit sequential inputs from '00000000' to '11111111'. The 256 rows of the 8-bit sequential inputs, each bit at the same column position comprises of 256 bits and thereby eight 256-bit columns provide eight 8-bit input vectors which are common for all 8-bit BFs. The 256 output bits, there are 2256 different possibilities whose decimal equivalent vary between 0 and 2256-1 [103]. Hence, 8-bit BFs have eight 256 bit long 8-bit input vectors and 2256 possible 256-bit output vectors. Hence for generation and security analysis of 4-bit or 8-bit S-boxes it is an urgent need to study cryptographic properties of S-boxes as well as security of S-boxes with 4-bit or 8-bit BFs. In other words a 4-bit S-box can be represented by a four valued 4-bit BF. If the 1st bit of the 4 output bits is taken sequentially for each element of the 16 elements of an S-box, one gets the 1st BF; 2nd sequence of output bit, the 2nd BF; 3rd sequence of output bit, the 3rd BF and 4th sequence of output bit, the 4th BF [2] respectively. Some cryptographic properties and security analysis of 4-bit S-boxes such as Output Bit Independence Criterion (BIC) of 4-bit S-boxes, SAC of 4-bit S-boxes, Higher order SAC of 4-bit S-boxes, Extended SAC of 4-bit S-boxes, Linear Cryptanalysis of 4-bit S-boxes, Differential Cryptanalysis of 4-bit S-boxes, and Differential Cryptanalysis with 4-bit BFs of 4-bit S-boxes as well as Linear Approximation Analysis of 4-bit S-boxes has been reported below in brief.

A 4-bit S-box consists of four 4-bit BFs. In Output Bit Independence Criterion or BIC the difference or xored BFs of all two possible 4-bit BFs of the concerned S-box has been taken under consideration. If all 6 difference 4-bit BFs have been balanced then the criterion has been satisfied for the concerned S-box. Since all 6 difference 4-bit BFs have been balanced so the prediction of a bit value to be one or zero is in at most uncertainty [2].

In Strict Avalanche Criterion, 4 IPVs of a 4-bit BF has been complemented one at a time. If in complemented four 4-bit BFs 8 bit values has been changed and 8 bit values remains same then the 4-bit BF has been said to satisfy Strict Avalanche Criterion of 4-bit BFs [2, 3]. Complementing 4th IPV means interchanging each distinct 8 bit halves of a 4-bit Output BF, whereas complementing 3rd IPV means interchanging each distinct 4 bit halves of each distinct 8 bit halves, whereas complementing 2nd IPV means interchanging each distinct 2 bit halves of each distinct 4 bit halves of each distinct 8 bit halves and complementing 1st IPV means interchanging each bit of all distinct 2-bit halves of a 16 bit long 4-bit BF. In this paper this shifting property has been used to construct an algorithm of SAC of 4-bit BFs. Another new algorithm with flip of index bits has also been introduced in this paper. If all four 4-bit BFs of a 4-bit S-box satisfy SAC for 4-bit BFs then the concerned S-box has been said to satisfy SAC of 4-bit S-boxes [2, 3].

In Higher Order Strict Avalanche Criterion (HO-SAC) of 4-bit BFs four IPVs of a 4-bit S-box have been complemented two or three at a time [14]. If in complemented ten 4-bit BFs 8 bit values has been changed and 8 bit values remains same then the 4-bit BF has been said to satisfy HO-SAC of 4-bit BFs. A detailed review of old as well as two new algorithms with previous shift method and flip of index bits method has been introduced in this paper in Subsection 3.3. of Section 3. In this Paper a detailed review of a new algorithm entitled Extended HO-SAC has been introduced in which four IPVs have been complemented at a time.

In Differential Cryptanalysis of 4-bit crypto S-boxes the 16 distant input S-boxes have been obtained by xor operation with each of 16 input differences varies from 0 to F in hex to all 16 elements of input S-box one at a time. The 16 distant S-boxes have been obtained by shuffling the elements of the original

S-box in a certain order in which the elements of the input S-boxes have been shuffled in concerned distant input S-boxes. The 16 elements of each S-box and the elements in corresponding position of corresponding distant S-box has been xored to obtain the Difference S-box. The Difference S-box may or may not be a Crypto S-box since it may not have all unique and distinct elements in it. The count of each element from 0 to F in Difference S-box have been noted and put in Difference Distribution Table (DDT) for security analysis of the S-box [47, 48].

In this paper a review of the new algorithm using 4-bit BFs for Differential Cryptanalysis of 4-bit crypto S-boxes have been reviewed. An input S-box can be decomposed into four 4-bit Input Vectors (IPVs) with Decimal Equivalents 255 for 4th IPV, 3855 for 3rd IPV, 13107 for 2nd IPV, and 21845 for 1st IPV respectively. Now we complement all IPVs one, two, three and four at a time to obtain 16 4-bit Distant input S-boxes. Each of four Output BFs is shifted according to the Shift of four IPVs of input S-boxes to form four IPVs of Distant input S-boxes to obtain Distant S-boxes. The four 4-bit output BFs of S-boxes are xored bitwise with four 4-bit BFs of Distant S-boxes to obtain four 4-bit Difference BFs. For 16 Distant Output S-boxes there are 64 Difference BFs. Difference BFs are checked for balanced-ness *i.e.* for at most uncertainty. The Table in which the balanced-nesses of 64 Difference BFs have been noted has been called as Differential Analysis Table (DAT).

In Linear Cryptanalysis of 4-bit crypto S-boxes, every 4-bit linear relations have been tested for a particular 4-bit crypto S-box. The presence of each 4-bit unique linear relation is checked by satisfaction of each of them for all 16, 4-bit unique input bit patterns and corresponding 4-bit output bit patterns, generated from the index of each element and each element respectively of that particular crypto S-box. If they are satisfied 8 times out of 16 operations for all 4-bit unique input bit patterns and corresponding 4-bit output bit patterns, then the existence of the 4-bit linear equation is at a stake. The probability of presence and absence of a 4-bit linear relation both are $(= 8/16)\ \frac{1}{2}$. If a 4-bit linear equation is satisfied 0 times then it can be concluded that the given 4-bit linear relation is absent for that particular 4-bit crypto S-box. If a 4-bit linear equation is satisfied 16 times then it can also be concluded that the given 4-bit linear relation is present for that particular 4-bit crypto S-box. In both the cases full information is adverted to the cryptanalysts. The concept of probability bias was introduced to predict the randomization ability of that 4-bit S-box from the probability of presence or absence of unique 4-bit linear relations. The result is better for cryptanalysts if the probability of presence or absences of unique 4-bit linear equations are far away from $\frac{1}{2}$ or near to 0 or 1. If the probabilities of presence or absence of all unique 4-bit linear relations are $\frac{1}{2}$ or close to $\frac{1}{2}$, then the 4-bit crypto S-box has been said to be linear cryptanalysis immune, since the existence of maximum 4-bit linear relations for that 4-bit crypto S-box is hard to predict [47, 48]. Heys also introduced the concept of Linear Approximation Table (LAT) in which the numbers of times, each 4-bit unique linear relation have been satisfied for all 16, unique 4-bit input bit patterns and corresponding 4-bit output bit patterns of a crypto S-box have been noted. The result is better for a cryptanalysts if the numbers of 8s in the table are less. If numbers of 8s are much more than the other numbers in the table then the 4-bit crypto S-box has been said to be more linear cryptanalysis immune [47, 48].

In another look an input S-box can be decomposed into four 4-bit Input Vectors (IPVs) with Decimal Equivalents 255 for 4th IPV, 3855 for 3rd IPV, 13107 for 2nd IPV, and 21845 for 1st IPV respectively. The S-box can also be decomposed into 4, 4-bit Output BFs (OPBFs). Each IPV can be denoted as a input variable of a linear relation and OPBF as a output variable and '+' as xor operation. Linear relations have been checked for satisfaction and 16-bit output variables (OPVs) due to linear relations have been checked for balanced-ness. Balanced OPVs indicates, out of 16 bits of IPVs and OPBFs, 8 bits satisfies the linear relation and 8 bits is out of satisfaction, *i.e.* best uncertainty. 256 4-bit linear relations have been operated on 4, 16-bit IPVs and 4, 16-bit OPBFs and 256 OPVs have been generated. The count of number of 1s in OPVs have been put in Linear Approximation Table or LAT. Better the number of 8s in LAT, better the S-box security [47, 48].

In this paper, a detailed review of a new technique to find the existing Linear Relations or Linear Approximations for a particular 4-bit S-box has been reviewed. If the nonlinear part of the ANF equation of a 4-bit output BF is absent or calculated to be 0 then the equation is termed as a Linear Relation or Approximation. Searching for number of existing linear relations through this method is ended up with number of existing linear relations. I.e. the goal to conclude the security of a 4-bit crypto S-box has been attended in a very lucid manner by this method.

Polynomials over Finite field or Galois field $GF(p^q)$ have been of utmost importance in Public Key Cryptography [14]. The polynomials over Galois field $GF(p^q)$ with degree q have been termed as Basic Polynomials or BPs over Galois field $GF(p^q)$ and Polynomials with degree ¡q have been termed as Elemental Polynomials or EPs over Galois field $GF(p^q)$ [113]. The EPs over Galois field $GF(p^q)$ with only constant terms have been termed as Constant Polynomials or CPs over Galois field $GF(p^q)$. The BPs over Finite field or Galois field $GF(p^q)$ that cannot be factored into at least two non-constant EPs have been termed as Irreducible polynomials or IPs over Finite field or Galois field $GF(p^q)$ and the rest have been termed as Reducible polynomials or RPs over Finite field or Galois field $GF(p^q)$ [113]. The polynomials over Galois field $GF(p^q)$ with coefficient of the highest degree term as 1 have been termed as monic polynomials over Galois field $GF(p^q)$ and rest have been termed as non-monic Polynomials over Galois field $GF(p^q)$ [113].

q bit crypto Substitution box or S-box have 2q elements in an array where each element is unique and distinct and arranged in a random fashion varies from 0 to 2q. Polynomials over Galois field $GF(p^q)$ have been termed as binary polynomials if p = 2. The binary number that has been constructed with binary coefficients of all q values with q = 0 at LSB and q = q at MSB has been termed as binary Coefficient Number or BCN of q+1 bits. The Binary Coefficient Number or BCN over Galois field $GF(p^q)$ has been similar with log 2^{q+1} bit BFs. The log 2^{q+1} bit S-boxes have been generated using log 2^{q+1} bit BCNs. In this paper crypto 4 and 8 bit S-boxes have been generated using BCNs and the procedure has been continued as a future scope to generate 16 and 32 bit S-boxes. The non-repeated coefficients of BPs over Galois field $GF(p^q)$, where p = 2 (log 2^{q+1}) and q = p-1 have been used to generate log 2^{q+1} bit S-boxes. In this paper proper 4 and 8 bit S-boxes have been generated using BCNs and the procedure has been continued as a future scope to generate 16 and 32 bit S-boxes. In this paper polynomials over Galois Field $GF(p^q)$ and roll of IPs to construct substitution boxes have been reviewed in Subsection 3.1 and respectively of section.3. The generation of 4 and 8 bit S-boxes using BCNs have been elaborated in subsec 3.2 of Section 3. The generation of 4-bit and 8-bit S-boxes with coefficients of non-binary Galois Field polynomials has been depicted in Subsection 3.3 of Section 3. The cryptographic and security analysis of 32 DES 4-bit S-boxes has been given in Subsection 3.4 of Section 3. Detailed cryptographic and security analysis of generated 10 4-bit S-boxes with discussed crypto related cryptographic properties and security criterion have also been given in Subsection 3.4. of Section 3. Results have been discussed in Result and Discussion section in Subsection 3.5 of Section 3. Concluding remarks, Acknowledgement and Reference has been given in Sections 4, 5 and 6 respectively.

Key Terminology and Definitions.

Substitution box (S-box). Substitution boxes have often been used in encryption and decryption algorithms or ciphers of public key cryptography. It consists of values from 0 to F for 4-bit S-boxes arranged in a random manner. It has been used for nonlinear substitution of plaintext or cipher-text bit stream.

Irreducible Polynomials (IPs). Basic Polynomials (BPs) with Factors of constant polynomials and BP itself has been termed as Irreducible Polynomials.

Finite Fields or Galois field $GF(p^q)$. A Field with finite number of elements has been termed as finite fields. P has been termed as prime modulus of the field and q has been termed as extension of the field.

2 Literature Survey

In this section an exhaustive relevant literature survey with their specific references has been introduced to crypto literature. in subsec 2.1. the relevant topic has been cryptography and cryptology, in subsec 2.2. the topic has been Linear Cryptanalysis, in subsec 2.3 the topic has been Differential Cryptanalysis, in subsec 2.4 the topic has been cryptanalysis of stream ciphers and in subsec 2.5. the relevant topic has been Strict Avalanche Criterion (SAC) of substitution boxes. At last a literature study on IPs and primitive polynomials have been given in Subsection 2.6.

2.1 Cryptography and Cryptology

In End of Twentieth Century a Bible of Cryptography had been introduced [69]. The various concepts involved in cryptography and also some information on cryptanalysis had been provided to Crypto-community in late nineties [90], a simplified version of DES, that has the architecture of DES but has much lesser rounds and much lesser bits had also been proposed at the same time. The cipher has also been better for educational purposes [88]. Later in early twenty first century an organized pathway towards learning how to cryptanalyze had been charted [92]. Almost at the same time a new cipher as a candidate for the new AES, main concepts and issues involve in block cipher design and cryptanalysis had also been proposed [91] that is also a measure of cipher strength. A vital preliminary introduction to cryptanalysis has also been introduced to cryptanalysts [70]. At the same time somewhat similar notion as [70] but uses a more descriptive approach and focused on linear cryptanalysis and differential cryptanalysis of a given SPN cipher had been elaborated [58]. Particularly, it discusses DES-like ciphers that had been extended with it [94]. Comparison of modes of operations such as CBC, CFB, OFB and ECB had also been elaborated [77].

A new cipher called Camelia had been introduced with its cryptanalysis technique to demonstrate the strength of the cipher [53]. History of Commercial Computer Cryptography and classical ciphers and the effect of cryptography on society had also been introduced in this queue [99]. The requirements of a good cryptosystem and cryptanalysis had also been demonstrated later [59]. Description of the new AES by Rijndael, Provides good insight into many creative cryptographic techniques that increases cipher strength had been included in literature. A bit later a highly mathematical path to explain cryptologic concepts had also been introduced [35], investigation of the security of Ron Rivest's DESX construction, a cheaper alternative to Triple DES had been elaborated [55].

A nice provision to an encyclopedic look at the design, analysis and applications of cryptographic techniques had been depicted later [115] and last but not the least a good explanation on why cryptography has been hard and the issues which cryptographers have to consider in designing ciphers had been elaborated [93]. Simplified Data Encryption Standard or S-DES is an educational algorithm similar to Data Encryption Standard (DES) but with much smaller Parameters [76]. The technique to analyze S-DES using linear cryptanalysis and differential cryptanalysis had been of interest of crypto-community later [76]. The encryption and decryption algorithm or cipher of twofish algorithm had been introduced to crypto community and a cryptanalysis of the said cipher had also been elaborated in subject to be a part of Advance Encryption Algorithm proposals [89].

2.2 Some Old and Recent References on Linear Cryptanalysis

The cryptanalysis technique to 4-bit crypto S-boxes using linear relations among four, 4-bit input Vectors (IPVs) and four, output 4-bit Boolean Functions (OPBFs) of a 4-bit S-box have been termed as linear cryptanalysis of 4-bit crypto S-boxes [47, 48]. Another technique to analyze the security of a 4-bit crypto S-box using all possible differences had also been termed as Differential Cryptanalysis of 4-bit crypto S-boxes [47, 48]. The search for best characteristic in linear cryptanalysis and the maximal

weight path in a directed graph and correspondence between them had also been elaborated with proper example [20]. It had also been proposed that the use of correlation matrix as a natural representation to understand and describe the mechanism of linear cryptanalysis [26]. It was also formalized the method described in [65] and showed that at the structural level, linear cryptanalysis has been very similar to differential cryptanalysis. It was also used for further exploration into linear cryptanalysis [17]. It had also been provided with a generalization of linear cryptanalysis and suggests that IDEA and SAFER K-64 have been secure against such generalization [45]. It had been surveyed to the use of multiple linear approximations in cryptanalysis to improve efficiency and to reduce the amount of data required for cryptanalysis in certain circumstances [50]. Cryptanalysis of DES cipher with linear relations [65] and the improved version of the said cryptanalysis [65] with 12 Computers had also been reported later [66]. The description of an implementation of Matsui's linear cryptanalysis of DES with strong emphasis on efficiency had also been reported [49].

In early days of this century the cryptanalytic attack based on multiple Linear Approximations to AES candidate Serpent had also been reported [23]. Later a technique to prove security bounds against Linear and Differential cryptanalytic attack using Mixed-Integer Linear Programming (MILP) had also been elaborated [71]. Later to this on the strength of two variants of reduced round lightweight block cipher SIMON-32 and SIMON-48 had been tested against Linear Cryptanalysis and had been presented the optimum possible results [1]. Almost at the same time The strength of another light weight block ciphers SIMECK had been tested against Linear Cryptanalysis [10]. The fault analysis of light weight block cipher SPECK and Linear Cryptanalysis with zero statistical correlation among plaintext and respective cipher text of reduced round lightweight block cipher SIMON to test its strength had also been introduced in recent past [111].

2.3 Some Old and Recent References on Differential Cryptanalysis

The design of a Feistel cipher with at least 5 rounds that has been resistant to differential cryptanalysis had been reported to crypto community [21]. The exploration of the possibility of defeating differential cryptanalysis by designing S-boxes with equiprobable output XORs using bent functions had been reported once [4]. The description of some design criteria for creating good S-boxes that are immune to differential cryptanalysis and these criteria are based on information theoretic concepts had been reported later [28]. It had been Introduced that the differential cryptanalysis on a reduced round variant of DES [14] and broke a variety of ciphers, the fastest break being of two-pass Snefru [15] and also described the cryptanalysis of the full 16-round DES using an improved version [14, 16]. It had been shown that there have been DES-like iterated ciphers that does not yield to differential cryptanalysis [75] and also introduced the concept of Markov ciphers and explained its significance in differential cryptanalysis. It had also been Investigated that the security of iterated block ciphers shows how to and when an r-round cipher is not vulnerable to attacks [58].

It had also been proposed that eight round Twofish can be attacked and investigated the role of key dependent S-boxes in differential cryptanalysis [73]. It had been on the same line with [4] but proposed that the input variables be increased and that the S-box be balanced to increase resistance towards both differential and linear cryptanalysis [112]. Early in this century in previous decade estimation of probability of block ciphers against Linear and Differential cryptanalytic attack had been reported. Later a new Algebraic and statistical technique of Cryptanalysis against block cipher PRESENT-128 had been reported [82]. Almost 3 year later a new technique entitled Impossible Differential Cryptanalysis had also been reported [18]. A detailed Comparative study of DES based on the strength of Data Encryption (DES) Standard against Linear and Differential Cryptanalysis had been reported later [80]. At last Constraints of Programming Models of Chosen Key Differential Cryptanalysis had been reported to crypto community [39].

2.4 Linear and Differential Cryptanalysis of Stream Ciphers

In late 20th century a stepping stone of the Differential-Linear cryptanalysis method that is a very efficient method against DES had also been grounded [46]. The relationship between linear and differential cryptanalysis and present classes of ciphers which are resistant towards these attacks had also been elaborated [103]. Description of statistical cryptanalysis of DES, a combination and improvement of both linear and differential cryptanalysis with suggestion of the linearity of S-boxes have not been very important had been depicted [100]. Later in 21st century description of analysis with multiple expressions and differential-linear cryptanalysis with experimental results of an implementation of differential-linear cryptanalysis with multiple expressions applied to DES variants had also been proposed [40]. At the same time the attack on 7 and 8 round Rijndael using the Square method with a related-key attack that can break 9 rounds Rijndael with 256 bit keys had been described [32].

In Late or almost end of 20th century the strength of stream ciphers have been tested against Differential Cryptanalytic attack [29]. Later the strength of them had also been tested against Linear Cryptanalytic attack [41]. A separate method of linear cryptanalytic attack had been reported once [102]. At least 6 years later The strength of stream cipher Helix had been tested against Differential Cryptanalytic attack [72]. Later the strength of stream ciphers Py, Py6, and Pypy had also been tested again Differential Cryptanalytic attack [109]. Recently the test of strength of stream cipher ZUC against Differential Cryptanalytic attack had also been reported to crypto community [110].

2.5 Strict Avalanche Criterion (SAC) of S-boxes

In beginning Strict Avalanche Criterion of 4-bit Boolean Functions and Bit Independence Criterion of 4-bit S-boxes had been introduced [107] and Design of Good S-boxes based on these criteria had also been reported later [3]. In end of 20th century the construction of secured S-boxes to satisfy Strict Avalanche Criterion of S-boxes had been reported with ease [56]. The test of 4-bit Boolean Functions to satisfy higher order strict Avalanche Criterion (HOSAC) have had also been illustrated [86]. In early twenty first century the analysis methods to Strict Avalanche Criterion (SAC) had been reported. A new approach to test degree of suitability of S-boxes in modern block ciphers had been introduced to crypto-community [61]. 16! 4-bit S-boxes had also been tested for optimum linear equivalent classes later [85]. The strength of several block ciphers against several Cryptanalytic attacks had been tested and reported later [7]. Recently the Key dependent S-boxes and simple algorithms to generate key dependent S-boxes had been reported [54]. An efficient cryptographic S-box design using soft computing algorithms have had also been reported [6]. In recent past the cellular automata had been used to construct good S-boxes [67].

2.6 Polynomials

In early Twentieth Century Radolf Church initiated the search for irreducible polynomials over Galois Field $GF(p^q)$ for p = 2, 3, 5 and 7 and for p = 2, q = 1 through 11, for p =3, q = 1 through 7, for p = 5, q = 1 through 4 and for p = 7, q = 1 through 3 respectively. A manual polynomial multiplication among respected EPs gives RPs in the said Galois field. All RPs have been cancelled from the list of BPs to give IPs over the said Galois field $GF(p^q)$ [22]. Later the necessary condition for a BP to be an IPs had been generalized to Even 2 characteristics. It had also been applied to RPs and gives Irreducible factors mod 2 [101]. Next to it Elementary Techniques to compute over finite Fields or Galois Field $GF(p^q)$ had been descried with proper modifications [11]. In next the factorization of Polynomials over Galois Field $GF(p^q)$ had been elaborated [12]. Later appropriate coding techniques of Polynomials over Galois Field $GF(p^q)$ had been illustrated with example [52].

The previous idea of factorizing Polynomials over Galois Field $GF(p^q)$ [12] had also been extended to Large value of P or Large Finite fields [13]. Later Few Probabilistic Algorithms to find IPs over Galois Field $GF(p^q)$ for degree q had been elaborated with example [76]. Later Factorization of multivariate polynomials over Galois fields GF(p) had also been introduced to mathematics community [60]. With that the separation of irreducible factors of BPs [12] had also been introduced later [68]. Next to it the factorization of BPs with Generalized Reimann Hypothesis (GRH) had also been elaborated [8]. Later a Probabilistic Algorithm to find irreducible factors of Basic bivariate Polynomials over Galois Field $GF(p^q)$ had also been illustrated [104]. Later the conjectural Deterministic algorithm to find primitive elements and relevant primitive polynomials over binary Galois Field GF(2) had been introduced [84]. Some new algorithms to find IPs over Galois Field GF(p) had also been introduced at the same time [97]. Another use of Generalized Reimann Hypothesis (GRH) to determine irreducible factors in a deterministic manner and also for multiplicative subgroups had been introduced later [83]. The table binary equivalents of binary primitive polynomials had been illustrated in literature [114]. The method to find roots of primitive polynomials over binary Galois field GF(2) had been introduced to mathematical community [98]. A method to search for IPs in a Random manner and factorization of BPs or to find irreducible factors of BPs in a random fashion had been introduced later [34]. After that a new variant of Rabin's algorithm [79] had been introduced with probabilistic analysis of BPs with no irreducible factors [36]. Later a factorization of univariate Polynomials over Galois Field GF(p) in sub quadratic execution time had also been notified [51]. Later a deterministic algorithm to factorize IPs over one variable had also been introduced [9].

An algorithm to factorize bivariate polynomials over Galois Field GF(p) with hensel lifting had also been notified [37]. Next to it an algorithm had also been introduced to find factor of Irreducible and almost primitive polynomials over Galois Field GF(2) [19]. Later a deterministic algorithm to factorize polynomials over Galois Field GF(p) to distinct degree factors had also been notified [38]. A detailed study of multiples and products of univariate primitive polynomials over binary Galois Field GF(2) had also been done [62]. Later algorithm to find optimal IPs over extended binary Galois Field GF(2m) [95] and a deterministic algorithm to determine Pascal Polynomials over Galois Field GF(2) [33] had been added to literature. Later the search of IPs and primitive polynomials over binary Galois Field GF(2) had also been done successfully [96]. At the same time the square free polynomials had also been factorized [81] where a work on divisibility of trinomials by IPs over binary Galois Field GF(2) [57] had also been notified. Later a probabilistic algorithm to factor polynomials over finite fields had been introduced [44]. An explicit factorization to obtain irreducible factors to obtain for cyclotomic polynomials over Galois Field $GF(p^q)$ had also been reported later [106].

A fast randomized algorithm to obtain IPs over a certain Galois Field $GF(p^q)$ had been notified [24]. A deterministic algorithm to obtain factors of a polynomial over Galois field $GF(p^q)$ had also been notified at the same time [64]. A review of construction of IPs over finite fields and algorithms to Factor polynomials over finite fields had been reported to literature [43, 74]. An algorithm to search for primitive polynomials had also been notified at the same time [105]. The residue of division of BPs by IPs must be 1 and this reported to literature a bit later [113]. The IPs with several coefficients of different categories had been illustrated in literature a bit later [42]. The use of zeta function to factor polynomials over finite fields had been notified later on [78] At last Integer polynomials had also been described with examples [108].

3 S-box Generation

In this section polynomials over Galois Field $GF(p^q)$ and roll of IPs to construct substitution boxes have been reviewed in Subsection 3.1 of section.3. The generation of 4 and 8 bit S-boxes using BCNs have been elaborated in subsec 3.2 of Section 3. The generation of 4-bit and 8-bit S-boxes with Coefficients of

non-binary Galois Field Polynomials has been depicted in Subsection 3.3 of Section 3. The cryptographic and security analysis of 32 DES 4-bit S-boxes has been given in Subsection 3.4 of Section 3. Detailed cryptographic and security analysis of generated 10 4-bit crypto S-boxes with discussed crypto related cryptographic properties and security criterion have also been given in Subsection 3.4. of Section 3. Results have been discussed in Result and Discussion section in Subsection 3.5 of Section 3.

3.1 Polynomials over Galois Field $GF(p^q)$ and Log 2^{q+1} Bit S-boxes

In this section the Subsection 3.1.1. has been devoted to a small review of Polynomials. The Subsection 3.1.2. has been of utmost importance since in it a four bit crypto or proper S-box has been defined in brief. At last in Subsection 3.1.3. The equation among 215 Galois field Polynomials and a 4-bit crypto S-box has been elaborated in details.

3.1.1 Polynomials over Galois Field $GF(p^q)$

Polynomials over Galois field $GF(p^q)$ have been of utmost importance in cryptographic applications. Polynomials with degree q have been termed as Basic Polynomials over Galois field $GF(p^q)$ and Polynomials with degree less than q have been termed as Elemental Polynomials over Galois field $GF(p^q)$. Polynomials with leading coefficient as 1 have been termed as Monic Polynomials irrespective of BPs and EPs over Galois field $GF(p^q)$. An example, of the said criteria have been described as follows, the Example of Basic Polynomial or BP over Galois field $GF(p^q)$ has been given below,

$$BP(x) = co_q x^q + co_{q-1} x^{q-1} + co_{q-1} x^{q-2} + \cdots + co_2 x^2 + co_1 x^1 + a_0. \tag{1}$$

In Equation (1), BP(x) has been represented as Basic Polynomial or BP over Galois field $GF(p^q)$ since the highest degree term of the said polynomial over Galois field $GF(p^q)$ has been q. The BP has been called as a Monic BP over Galois field $GF(p^q)$ if $co_q = 1$. The number of Terms in a BP over Galois field $GF(p^q)$ has been (q+1). The number of possible values of a particular coefficient co_q, where $0 \leq p \leq q$ has been from 0 to p, *i.e.* $(p + 1)$. If the value of q has been $< q$ then The polynomial over Galois field $GF(p^q)$ has been termed as Elemental Polynomial or EPs over Galois field $GF(p^q)$. If a BP or EP contains only constant term then the polynomial has been termed as Constant Polynomial or CP over Galois field $GF(p^q)$. If a BP over Galois field $GF(p^q)$ can be factored into two non-constant EPs then the BP can be termed as Reducible Polynomials or RPs over Galois field $GF(p^q)$. If the two factor of a BP over Galois field $GF(p^q)$ have been the BP itself and a constant Polynomial or CP then The BP have been said as an Irreducible Polynomial or IP over Galois field $GF(p^q)$.

3.1.2 4-bit Crypto S-boxes

A 4-bit crypto S-box can be written as Follows, where the each element of the first row of Table 1, entitled as index, are the position of each element of the S-box within the given S-box and the elements of the 2nd row, entitled as S-box, are the elements of the given Substitution box. It can be concluded that the 1st row is fixed for all possible crypto S-boxes. The values of each element of the 1st row are distinct, unique and vary between 0 and F. The values of the each element of the 2nd row of a crypto S-box have also been distinct and unique and also vary between 0 and F. The values of the elements of the fixed 1st row are sequential and monotonically increasing where for the 2nd row they can be sequential or partly sequential or non- sequential. Here the given Substitution Box is the 1st 4-bit S-box of the 1st S-box out of 8 of Data Encryption Standard [2, 116, 117].

Table 1: 4-bit crypto S-box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	Index	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	S-box	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

3.1.3 Relation Between 4-bit S-boxes and Polynomials over Galois field $GF(2^{15})$

Index of Each element of a 4-bit crypto S-box and the element itself is a hexadecimal number and that can be converted into a 4-bit bit sequence. From row 2 through 5 and row 7 through A of each column from 1 through G of Table 2. shows the 4-bit bit sequences of the corresponding hexadecimal numbers of the index of each element of the given S-box and each element of the S-box itself. Each row from 2 through 5 and 7 through A from column 1 through G constitutes a 16 bit, bit sequence that is a Basic Polynomial or BP over Galois field $GF(2^{15})$. column 1 through G of Row 2 has been termed as 4th IGFP, Row 3 has been termed as 3rd IGFP, Row 4 has been termed as 2nd IGFP and Row 5 has been termed as IGFP whereas column 1 through G of Row 7 has been termed as 4th OGFP, Row 8 has been termed as 3rd OGFP, Row 9 has been termed as 2nd OGFP and Row A has been termed as 1st OGFP. The decimal equivalents of each IGFP and OGFP have been noted at column H of respective rows. Here IGFP stands for Input Galois Field Polynomial and OGFP stands for Output Galois Field Polynomials. The respective Polynomials have been shown in Row 1 through 8 of column 3 of Table 3.

Table 2: Input and Output BCNs of the Substitution Box

Row	**Column**	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	**H.** Decimal Equivalent
1	**Index**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**	
2	**IGFP4**	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	00255
3	**IGFP3**	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	03855
4	**IGFP2**	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	13107
5	**IGFP1**	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	21845
6	**S-box**	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7	
7	**OGFP4**	1	0	1	0	0	1	1	1	0	1	0	1	0	1	0	0	42836
8	**OGFP3**	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1	58425
9	**OGFP2**	1	0	0	0	1	1	1	0	1	1	1	0	0	0	0	1	36577
A	**OGFP1**	0	0	1	1	0	1	1	0	1	0	0	0	1	1	0	1	13965

3.2 4 and 8 Bits S-box Generation by Respective BCNs over Binary Galois Field $GF(2^q)$ where q (15 and 255) Respectively

In this paper 4 and 8 bit identity S-boxes have been taken for example for generation of 4 and 8 bit S-boxes over binary Galois Fields $GF(2^q)$ where $q \in$ (15 and 255) respectively. The generation of identity 4-bit S-box from four BCNs over binary Galois Field $GF(2^{15})$ have been elaborated in Subsection 3.2.1 and The generation of identity 8-bit S-box from Eight BCNs over Binary Galois Field $GF(2^{255})$ have been elaborated in Subsection 3.2.2. The Algorithm for generation of log 2^{q+1} bit S-boxes over Binary Galois Field $GF(2^q)$ has been depicted with Time Complexity of the algorithm in Subsection 3.2.3.

Table 3: Respective Polynomials of IGFP4 through IGFP1 and OGFP4 through OGFP1

Col	1	2	3
Row	Index	DCM Eqv.	Polynomials over Galois Field GF(2^{15}).
1	IGFP4	00255	$BP(x) = x^7+x^6+x^5+x^4+x^3+x^2+x^1+1.$
2	IGFP3	03855	$BP(x) = x^{11}+x^{10}+x^9+x^8+x^3+x^2+x^1+1.$
3	IGFP2	13107	$BP(x) = x^{13}+x^{12}+x^9+x^8+x^5+x^4+x^1+1.$
4	IGFP1	21845	$BP(x) = x^{14}+x^{12}+x^{10}+x^8+x^6+x^4+x^2+1.$
5	OGFP4	42836	$BP(x) = x^{15}+x^{13}+x^{10}+x^9+x^8+x^6+x^4+ x^2.$
6	OGFP3	58425	$BP(x) = x^{15}+x^{14}+x^{13}+x^{10}+x^5+x^4+x^3+1.$
7	OGFP2	36577	$BP(x) = x^{15}+x^{11}+x^{10}+x^9+x^7+x^6+x^5+1.$
8	OGFP1	13965	$BP(x) = x^{13}+x^{12}+x^{10}+x^9+x^7+x^3+x^2+1.$

3.2.1 Generation of 4-bit Identity Crypto S-box from Four Polynomials over Binary Galois Field $GF(2^{15})$

The Concerned 4-bit identity S-box has been shown in Table 4 where each element of the first row of Table 4, entitled as index, have been the position of each element of the S-box within the given S-box and the elements of the 2nd row, entitled as S-box, are the elements of the given identity Substitution box. It can be concluded that the 1st row has been fixed for all possible crypto S-boxes. The values of each element of the 1st row are distinct, unique and vary between 0 and F. The values of the each element of the 2nd row of the identity crypto S-box have also been distinct and unique and also vary between 0 and F. The values of the elements of the fixed 1st row are sequential and monotonically increasing where for the 2nd row, they are also sequential and monotonically increasing for this identity S-box. Here the given Substitution Box is the 4-bit identity crypto S-box.

Table 4: 4-bit Identity Crypto S-box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	Index	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	S-box	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Index of Each element of a 4-bit crypto S-box and the element itself is a hexadecimal number and that can be converted into a 4-bit bit sequence. From row 2 through 5 and row 7 through A of each column from 1 through G of Table 5. shows the 4-bit bit sequences of the corresponding hexadecimal numbers of the index of each element of the given S-box and each element of the S-box itself. Each row from 2 through 5 and 7 through A from column 1 through G constitutes a 16 bit, bit sequence that is a Basic Polynomial over Galois field $GF(2^{15})$. column 1 through G of Row 2 has been termed as 4th IGFP, Row 3 has been termed as 3rd IGFP, Row 4 has been termed as 2nd IGFP and Row 5 has been termed as IGFP whereas column 1 through G of Row 7 has been termed as 4th OGFP, Row 8 has been termed as 3rd OGFP, Row 9 has been termed as 2nd OGFP and Row A has been termed as 1st OGFP. The decimal equivalents of each IGFP and OGFP have been noted at column H of respective rows. Where IGFP stands for Input Galois Field Polynomials and OGFP stands for Output Galois Field Polynomials. The respective Polynomials have been shown in Row 1 through 8 of column 3 of

Table 6.

Table 5: Input and Output BCNs of the Identity Substitution Box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H. Decimal
1	Index	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**	Equivalent
2	IBCN4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	00255
3	IBCN3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	03855
4	IBCN2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	13107
5	IBCN1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	21845
6	S-box	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**	
7	OBCN4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	00255
8	OBCN3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	03855
9	OBCN2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	13107
A	OBCN1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	21845

Table 6: Respective Polynomials of IGFP4 through IGFP1 and OGFP4 through OGFP1

Col	1	2	3
Row	Index	DCM Eqv.	Polynomials over Galois Field GF(2^{15}).
1	IGFP4	00255	$BP(x) = x^7+x^6+x^5+x^4+x^3+x^2+x^1+1.$
2	IGFP3	03855	$BP(x) = x^{11}+x^{10}+x^9+x^8+x^3+x^2+x^1+1.$
3	IGFP2	13107	$BP(x) = x^{13}+x^{12}+x^9+x^8+x^5+x^4+x^1+1.$
4	IGFP1	21845	$BP(x) = x^{14}+x^{12}+x^{10}+x^8+x^6+x^4+x^2+1.$
5	OGFP4	00255	$BP(x) = x^7+x^6+x^5+x^4+x^3+x^2+x^1+1.$
6	OGFP3	03855	$BP(x) = x^{11}+x^{10}+x^9+x^8+x^3+x^2+x^1+1.$
7	OGFP2	13107	$BP(x) = x^{13}+x^{12}+x^9+x^8+x^5+x^4+x^1+1.$
8	OGFP1	21845	$BP(x) = x^{14}+x^{12}+x^{10}+x^8+x^6+x^4+x^2+1.$

3.2.2 Generation of 8-bit Identity Crypto S-box from Eight Polynomials over Binary Galois Field $GF(2^{255})$

The concerned 8-bit identity S-box has been shown in Table 7 where each element of the first row of Table 7, entitled as index, are the position of each element of the S-box within the given S-box and the elements of the column 1 through G of 2nd to 17th row, entitled as S-box, have been the elements of the given 8-bit identity Substitution box sequentially. It can be concluded that the 1st row is fixed for all possible 8-bit bijective crypto S-boxes. The values of each element of the 1st row are distinct, unique and vary between 0 and F. The values of the each element of the column 1 through G of 2nd row to 17th row of the 8-bit identity crypto S-box are also distinct and unique and vary between 0 and 256. The values of the elements of the fixed 1st row are sequential and monotonically increasing where for the 2nd to 17th row, they can be sequential or partly sequential or non- sequential and for this case elements are sequential and monotonically increasing. Here the given substitution box has been the 8-bit identity crypto S-box.

Index of Each element of an 8-bit crypto S-box and the element itself is a hexadecimal number and that can be converted into a 256-bit long 8 bit bit sequence. From row 2 through 9 and row A through

Table 7: 8-bit identity crypto S-box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	Index	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4		32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
5		48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63.
6		64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
7		80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
8		96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
9		112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
10		128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
11		144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
12		160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
13		176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
14		192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
15		208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
16		224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
17		240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

H of column 2 of Table 8. shows the 8-bit bit sequences of the corresponding hexadecimal numbers of the index of each element of the given S-box and each element of the S-box itself. Each row from 2 through 9 and A through H of column 2 constitutes a 256 bit, bit sequence that is a Basic Polynomial over Galois field $GF(2^{255})$. column 2 of Row 2 has been termed as 8th IGFP, Row 3 has been termed as 7th IGFP, Row 4 has been termed as 6th IGFP,Row 5 has been termed as 5th IGFP, Row 6 has been termed as 4th IGFP, Row 7 has been termed as 3rd IGFP, Row 8 has been termed as 2nd IGFP and Row 9 has been termed as 1st IGFP whereas column 2 of Row A has been termed as 8th OGFP, Row B has been termed as 7th OGFP, Row C has been termed as 6th OGFP, Row D has been termed as 5th OGFP, Row E has been termed as 4th OGFP, Row F has been termed as 3rd OGFP, Row G has been termed as 2nd OGFP and Row H has been termed as 1st IGFP. The Binary Coefficient Number of each IGFP and OGFP from MSB [256th bit] to LSB [0th bit] have been given in corresponding rows of each IGFP and OGFP. Where IGFP stands for Input Galois Field Polynomials and OGFP for Output Galois Field Polynomials. The respective polynomial for IGFP8 and OGFP8 has been shown in Table 9

3.2.3 Algorithm to Generate S-box from Polynomials over Galois Field $GF(2^{15})$ or $GF(2^{255})$

START.

Step OA. Choose 4 Galois field Polynomials over Galois field $GF(2^{15})$ or 8 Galois field Polynomials over Galois field $GF(2^{255})$.

Step 01. If Number of Terms in BCNs are Half of Number of total terms Then Step 02. Else Step 0A.

Step 02. Convert to decimal the 4 or 8 bit binary number generated by bits in same position of 4 BCNs for Galois field Polynomials over Galois field $GF(2^{15})$ or 8 Galois field Polynomials over Galois field $GF(2^{255})$.

STOP.

Time Complexity of the given Algorithm $O(n)$.

Table 8: BCNs for 8 IGFPs and OGFPs

Row	Col.	MSB Polynomials (BCNs)[col.2] LSB
1	1	
2	IGFP8	00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111 11111111111111111111111111111111111111111111111111111111111111111111111111111111
3	IGFP 7	00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111 00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111
4	IGFP 6	00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111
5	IGFP 5	00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111
6	IGFP 4	00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111
7	IGFP 3	00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111
8	IGFP 2	00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011
9	IGFP 1	01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101
A	OGFP 8	00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111 11111111111111111111111111111111111111111111111111111111111111111111111111111111
B	OGFP 7	00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111 00000000000000000000000000000000000000000000000000000000000000000000000000000000 11111111111111111111111111111111111111111111111111111111111111111111111111111111
C	OGFP 6	00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111 00000000000000000000000000000000111111111111111111111111111111111111111111111111
D	OGFP 5	00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111 00000000000000001111111111111111000000000000000011111111111111111
E	OGFP 4	00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111 00000000111111110000000011111111000000001111111100000000111111111
F	OGFP 3	00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111 00001111000011110000111100001111000011110000111100001111000011111
G	OGFP 2	00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011 00110011001100110011001100110011001100110011001100110011001100110011
H	OGFP 1	01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101 01010101010101010101010101010101010101010101010101010101010101010101

Table 9: Respective Polynomial of IGFP8 and OGFP8 of the Given 8 bit S-box

BCNs of	Polynomial
IGFP8 &OGFP8	$x^{127}+x^{126}+x^{125}+x^{124}+x^{123}+x^{122}+x^{121}+x^{120}+x^{119}+x^{118}+x^{117}+x^{116}+x^{115}+x^{114}+x^{113}+x^{112}+$ $x^{111}+x^{110}+x^{109}+x^{108}+x^{107}+x^{106}+x^{105}+x^{104}+x^{103}+x^{102}+x^{101}+x^{100}+x^{99}+x^{98}+x^{97}+x^{96}+$ $x^{95}+x^{94}+x^{93}+x^{92}+x^{91}+x^{90}+x^{89}+x^{88}+x^{87}+x^{86}+x^{85}+x^{84}+x^{83}+x^{82}+x^{81}+x^{80}+$ $x^{79}+x^{78}+x^{77}+x^{76}+x^{75}+x^{74}+x^{73}+x^{72}+x^{71}+x^{70}+x^{69}+x^{68}+x^{67}+x^{66}+x^{65}+x^{64}+$ $x^{63}+x^{62}+x^{61}+x^{60}+x^{59}+x^{58}+x^{57}+x^{56}+x^{55}+x^{54}+x^{53}+x^{52}+x^{51}+x^{50}+x^{49}+x^{48}+$ $x^{47}+x^{46}+x^{45}+x^{44}+x^{43}+x^{42}+x^{41}+x^{40}+x^{39}+x^{38}+x^{37}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+$ $x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+$ $x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1.$

3.3 4 and 8 Bits S-box Generation by Respective BCNs over Non Binary Galois Field $GF(16^{15})$ and Galois Field $GF(256^{255})$ Respectively

The coefficients of each polynomial over non binary Galois Field $GF(16^{15})$ forms a 4-bit S-box. The Coefficient of highest or lowest degree term must be the 1st element in 4-bit S-box, the value of other elements are the value of coefficients with immediate degree less than or greater than the previous one. Let The Polynomial be,

$$BP(x) = 0x^{15} + 1x^{14} + 2x^{13} + \cdots 12x^3 + 13x^2 + 14x + 15 \tag{2}$$

For the above Polynomial The Constituted 4-bit S-box have been given in Table 10.

Table 10: Constituted 4-bit Crypto S-box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	Index	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	S-box	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

The Polynomial with coefficients in reverse order,

$$BP(x) = 15x^{15} + 14x^{14} + 13x^{13} + \cdots + 3x^3 + 2x^2 + 1x + 0 \tag{3}$$

For the above Polynomial The Constituted 4-bit S-box have been given in Table 11.

Table 11: Constituted 4-bit Crypto S-box

Row	Column	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	Index	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	S-box	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

The coefficients of each polynomial over non binary Galois Field $GF(256^{255})$ forms an 8-bit S-box. The Coefficient of highest or lowest degree term must be the 1st element in 4-bit S-box, the value of other elements are the value of coefficients with immediate degree less than or greater than the previous one. Let The Polynomial be, Let the Polynomial be given in Table 12.

Table 12: Polynomial to Construct 8-bit Identity S-box

Polynomial BP(x) =
$0.x^{255}+ 1.x^{254}+ 2.x^{253}+ 3.x^{252}+ 4.x^{251}+ 5.x^{250}+ 6.x^{249}+ 7.x^{248}+ 8.x^{247}+ 9.x^{246}+ 10.x^{245}+ 11.x^{244}+ 12.x^{243}+ 13.x^{242}+ 14.x^{241}+ 15.x^{240}+16.x^{239}+ 17.x^{238}+ 18.\ x^{237}+ 19.x^{236}+ 20.x^{235}+ 21.x^{234}+ 22.x^{233}+ 23.x^{232}+ 24.x^{231}+ 25.x^{230}+ 26.x^{229}+ 27.x^{228}+ 28x^{227}+ 29.x^{226}+ 30.x^{225}+ 31.x^{224}+32.\ X^{223}+ 33.\ x^{222}+ 34.x^{221}+ 35.x^{220}+ 36.x^{219}+ 37.x^{218}+ 38.x^{217}+39.\ x^{216}+40.\ x^{215}+ 41.x^{214}+ 42.x^{213}+ 43.x^{212}+ 44.x^{211}+ 45.x^{210}+ 46.x^{209}+ 47.x^{208}+48.x^{207}+ 49.x^{206}+ 50.x^{205}+ 51.x^{204}+ 52.x^{203}+ 53.x^{202}+ 54.x^{201}+ 55.x^{200}+ 56.x^{199}+ 57.x^{198}+ 58.x^{197}+ 59.x^{196}+ 60.x^{195}+ 61.x^{194}+ 62.x^{193}+ 63.x^{192}+ 64.x^{191}+ 65.x^{190}+ 66.x^{189}+ 67.x^{188}+68.x^{187}+ 69.x^{186}+ 70.x^{185}+ 71.x^{184}+ 72.x^{183}+ 73.x^{182}+ 74.x^{181}+ 75.x^{180}+ 76.x^{179}+ 77.x^{178}+ 78.x^{177}+ 79.x^{176}+80.X^{175}+ 81.x^{174}+ 82.x^{173}+ 83.x^{172}+84.\ x^{171}+ 85.x^{170}+ 86.x^{169}+ 87.x^{168}+88.\ x^{167}+ 89.x^{166}+ 90.x^{165}+ 91.x^{164}+ 92.x^{163}+ 93.x^{162}+ 94.x^{161}+ 95.x^{160}+96.x^{159}+ 97.x^{158}+ 98.x^{157}+ 99.x^{156}+ 100.x^{155}+ 101.x^{154}+ 102.x^{153}+ 103.x^{152}+ 104.x^{151}+105.x^{150}+106.x^{149}+ 107.x^{148}+108.\ x^{147}+109.x^{146}+110.\ x^{145}+ 111.x^{144}+112.X^{143}+113.x^{142}+114.x^{141}+115.x^{140}+116.x^{139}+117.\ x^{138}+118.\ x^{137}+119.\ x^{136}+120.\ x^{135}+121.x^{134}+122.x^{133}+123.x^{132}+124.x^{131}+125.x^{130}+126.x^{129}+127.x^{128}+128.x^{127}+129.\ x^{126}+ 130.x^{125}+131.x^{124}+ 132.x^{123}+133.x^{122}+134.x^{121}+ 135.x^{120}+ 136.x^{119}+ 137.x^{118}+ 138.x^{117}+ 139.x^{116}+ 140.x^{115}+ 141.x^{114}+ 142.x^{113}+ 143.x^{112}+144.x^{111}+ 145.x^{110}+ 146.x^{109}+ 147.x^{108}+ 148.x^{107}+ 149.x^{106}+ 150.x^{105}+ 151.x^{104}+ 152.x^{103}+ 153.x^{102}+ 154.x^{101}+ 155.x^{100}+ 156.x^{99}+ 157.x^{98}+ 158.x^{97}+ 159.x^{96}+160.x^{95}+ 161.x^{94}+ 162.x^{93}+ 163.x^{92}+ 164.x^{91}+ 165.x^{90}+ 166.x^{89}+ 167.x^{88}+ 168.x^{87}+ 169.x^{86}+ 170.x^{85}+ 171.x^{84}+ 172.x^{83}+ 173.x^{82}+ 174.x^{81}+ 175.x^{80}+176.x^{79}+ 177.x^{78}+ 178.x^{77}+ 179.x^{76}+ 180.x^{75}+ 181.x^{74}+ 182.x^{73}+ 183.x^{72}+ 184.x^{71}+ 185.x^{70}+ 186.x^{69}+ 187.x^{68}+ 188.x^{67}+ 189.x^{66}+ 190.x^{65}+ 191.x^{64}+192.x^{63}+193.\ x^{62}+ 194.x^{61}+ 195.x^{60}+ 196.x^{59}+ 197.x^{58}+ 198.x^{57}+ 199.x^{56}+ 200.x^{55}+ 201.x^{54}+ 202.x^{53}+ 203.x^{52}+ 204.x^{51}+ 205.x^{50}+ 206.x^{49}+ 207.x^{48}+208.x^{47}+ 209.x^{46}+ 210.x^{45}+ 211.x^{44}+ 212.x^{43}+ 213.x^{42}+ 214.x^{41}+ 215.x^{40}+ 216.x^{39}+ 217.x^{38}+ 218.x^{37}+219.x^{36}+ 220.x^{35}+ 221.x^{34}+ 222.x^{33}+ 223.x^{32}+224.x^{31}+ 225.x^{30}+ 226.x^{29}+ 227.x^{28}+ 228.x^{27}+ 229.x^{26}+ 230.x^{25}+ 231.x^{24}+ 232.x^{23}+ 233.x^{22}+ 234.x^{21}+ 235.x^{20}+ 236.x^{19}+ 237.x^{18}+ 238.x^{17}+ 239.x^{16}+240.x^{15}+ 241.x^{14}+242.\ x^{13}+ 243.x^{12}+ 244.x^{11}+ 245.x^{10}+ 246.x^{9}+ 247.x^{8}+ 248.x^{7}+ 249.x^{6}+ 250.x^{5}+ 251.x^{4}+ 252.x^{3}+ 253.x^{2}+ 254x+ 255.$

Table 13: Constituted identity 8-bit S-box

Row	**Column**	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
1	**Index**	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4		32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
5		48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63.
6		64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
7		80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
8		96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
9		112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
10	**S-box**	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
11		144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
12		160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
13		176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
14		192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
15		208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
16		224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
17		240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

For the above Polynomial The Constituted 8-bit S-box have been given in Table 13.

Note. The 32-bit S-boxes can be constituted by polynomials over Galois field $GF[(2^{32})(2^{32-1})]$ and the 64-bit S-boxes can be constituted by polynomials over Galois field $GF[(2^{64})(2^{64-1})]$.

3.4 Cryptographic Analysis of 32 DES 4-bit S-boxes and 10 Better 4-bit S-boxes with Relevant Cryptographic Properties of 4-bit Crypto S-boxes

In Subsection 3.4.1.the cryptographic analysis procedures of the said cryptographic properties have been described. The cryptographic analysis of 32 DES 4-bit S-boxes has been evaluated in Subsection 3.4.2. cryptographic analysis of 10 generated better S-boxes has been described in Subsection 3.4.3

3.4.1 Analysis Procedure

For SAC, HO-SAC and Extended SAC of 4-bit S-boxes as the numbers of satisfied COPBFs have been increased it will give better security and optimum value gives at most security.

In Difference Distribution Table there have been 256 cells, *i.e.* 16 rows and 16 columns. Each row has been for each input difference varies from 0 to F. Each column in each row represents each output difference varies from 0 to F for each input difference. 0 in any cell indicates absence of that output difference for subsequent input difference. Such as 0 in 2nd cell of Table 7 of relevant DDT means for input difference 0 the corresponding output difference o has been absent. If number of 0 is too low or too high it supplies more information regarding concerned output difference. So an S-box is said to be immune to this cryptanalytic attack if number of 0s in DDT is close to 128 or half of total cells or 256. In the said example of 1st DES 4-bit S-box total numbers of 0s in DDT are 168. That is close to 128. So the S-box has been said to be almost secure from this attack.

As total number of balanced 4-bit BFs increases in Difference Analysis Table or DAT the security of S-box increases since balanced 4-bit BFs supplies at most uncertainty. Since Number of 0s and 1s in balanced 4-bit BFs are equal *i.e.* they are same in number means determination of each bit has been at most uncertainty. In the said example of 1st DES 4-bit S-box total numbers of 8s in DAT are 36. That is close to 32 half of total 64 cells. So the S-box has been said to be almost less secure from this attack.

In Linear Analysis Table or LAT there are 256 cells for 256 possible 4-bit linear relations. The count of 16 4-bit binary conditions to satisfy for any given linear relation has been put into the concerned cell. 8 in a cell indicate that the particular linear relation has been satisfied for 8 4-bit binary conditions and remain unsatisfied for 8, 4-bit binary conditions. That is at most uncertainty. In the said example of 1st DES 4-bit S-box total numbers of 8s in LAT have been 143. That is close to 128. So the S-box has been said to be less secure from this attack.

The value of ${}^{n}C_{r}$ has been maximum when the value of r is $\frac{1}{2}$ of the value of n (when n is even). Here the maximum number of linear approximations is 64. So if the total satisfaction of linear equation is 32 out of 64 then the number of possible sets of 32 linear equations has been the largest. Means if the total satisfaction is 32 out of 64 then the number of possible sets of 32 possible linear equations is ${}^{64}C_{32}$. That is maximum number of possible sets of linear equations.

If the value of total No of Linear Approximations is closed to 32 then it is more cryptanalysis immune. Since the number of possible sets of linear equations are too large to calculate. As the value goes close to 0 or 64 it reduces the sets of possible linear equations to search, that reduces the effort to search for the linear equations present in a particular 4-bit S-box. In this example total satisfaction is 21 out of 64. Which means the given 4-bit S-Box is not a good 4 bit S-Box or not a good Crypt analytically immune S-Box. If the values of total number of Existing Linear equations for a 4-bit S-Box are 24 to 32, then the lowest numbers of sets of linear equations are 250649105469666120. This is a very large number to investigate. So the 4-bit S-Box is declared as a good 4-bit S-Box or 4-bit S-Box with good security. If

it is between 16 through 23 then the lowest numbers of sets of linear equations are 488526937079580. This not a small number to investigate in today's computing scenario so the S-boxes are declared as medium S-Box or S-Box with medium security. The 4-bit S-Boxes having existing linear equations less than 16 are declared as Poor 4-bit S-Box or vulnerable to cryptanalytic attack.

3.4.2 Cryptographic Analysis of 32 DES 4-bit S-boxes

The cryptographic analysis of 32 DES 4-bit S-boxes with the said relevant cryptographic properties of 4-bit BFs has been given below in Table 14. Here in Table 14, column heading 'noelr gives numbers of existing linear relations in a particular 4-bit crypto S-box. Column heading 'nobal' gives numbers of balanced DBFs in linear cryptanalysis. 'n0dif' gives numbers of 0s in difference distribution table or DDT and 'nodif' gives numbers of 8s in DAT. 'nosac' gives numbers of COPBFs satisfy SAC of 4-bit BFs and 'n3sac','n3sac' and 'nalsac' gives numbers of COPBFs satisfy 2nd order SAC of 4-bit BFs, 3rd order SAC of 4-bit BFs and Extended SAC of 4-bit BFs respectively.

Table 14: Cryptographic analysis of 32 DES S-boxes

S-box	Noelr	nobal	n0dif	nodif	nosac	n2sac	n3sac	nalsac
e4d12fb83a6c5907	21	143	168	36	7	15	11	36
0f74e2d1a6cb9538	29	143	168	36	7	17	9	36
41e8d62bfc973a50	23	138	168	36	8	15	11	36
fc8249175b3ea06d	25	154	166	42	10	20	12	42
f18e6b34972dc05a	24	132	162	30	6	12	9	30
3d47f28ec01a69b5	21	143	166	30	8	12	7	30
0e7ba4d158c6932f	31	143	166	21	4	10	6	21
d8a13f42b67c05e9	20	126	168	36	8	12	12	36
a09e63f51dc7b428	17	133	162	30	7	12	8	30
d709346a285ecbf1	22	133	168	30	7	13	8	30
d6498f30b12c5ae7	23	151	166	21	6	9	4	21
1ad069874fe3b52c	28	158	174	30	6	11	10	30
7de3069a1285bc4f	22	136	168	36	8	16	10	36
d8b56f03472c1ae9	22	136	168	36	8	16	10	36
a690cb7df13e5284	20	136	168	36	8	16	10	36
3f06a1d8945bc72e	22	136	168	36	8	16	10	36
2c417ab6853fd0e9	25	137	162	30	6	14	8	30
eb2c47d150fa3986	20	143	166	36	8	16	9	36
421bad78f9c5630e	30	130	160	27	6	11	7	27
b8c71e2d6f09a453	21	134	166	18	3	7	6	18
c1af92680d34e75b	30	141	159	36	8	16	10	36
af427c9561de0b38	29	127	164	36	7	15	11	36
9ef528c3704a1db6	24	127	168	18	5	7	5	18
432c95fabe17608d	24	130	162	30	6	12	9	30
4b2ef08d3c975a61	26	134	168	30	7	13	8	30
d0b7491ae35c2f86	27	145	166	30	7	14	7	30
14bdc37eaf680592	28	137	168	36	8	16	10	36
6bd814a7950fe23c	25	135	173	0	0	0	0	0
d2846fb1a93e50c7	23	144	161	30	8	14	7	30
1fd8a374c56b0e92	20	147	174	27	9	12	4	27
7b419ce206adf358	27	132	166	18	5	7	5	18
21e74a8dfc90356b	28	138	168	39	8	16	12	39

3.4.3 Cryptographic Analysis of 10 Generated Better 4-bit S-boxes

The cryptographic analysis of 10 generated better 4-bit S-boxes with the said relevant cryptographic properties of 4-bit BFs has been given below in Table 15. Here in Table column 49 heading 'noelr gives numbers of existing linear relations in a particular 4-bit crypto S-box. Column heading 'nobal' gives numbers of balanced DBFs in linear cryptanalysis. 'n0dif' gives numbers of 0s in difference distribution table or DDT and 'nodif' gives numbers of 8s in DAT. 'nosac' gives numbers of COPBFs satisfy SAC of 4-bit BFs and 'n3sac','n3sac' and 'nalsac' gives numbers of COPBFs satisfy 2nd order SAC of 4-bit BFs, 3rd order SAC of 4-bit BFs and Extended SAC of 4-bit BFs respectively.

Table 15: Cryptographic analysis of 10 generated Better 4-bit S-boxes

S-box	noelr	nobal	n0dif	nodif	nosac	n2sac	n3sac	Nalsac
01235b8694ca7def	33	162	189	39	16	7	16	39
01235b86a4f97edc	33	200	206	45	16	13	16	45
10324a967b8fced5	27	156	175	39	16	11	8	39
103268957abcfde4	31	147	167	42	16	12	11	42
0132c5794a86fbed	26	164	189	39	16	7	16	39
1032c5684a97ebfd	28	162	189	39	16	7	16	39
1032c56879a4dbfe	27	196	206	39	16	7	16	39
1023c46a5b87e9fd	35	148	182	42	16	9	16	42
0123c7495b86eadf	23	149	170	42	16	11	13	42
103249adc65be87f	30	134	166	39	16	8	13	39

3.5 Results and Discussion

In Table 14. out of 32 DES S-boxes 1 have 17, 3 have 21, 4 have 22, 1 have 23, 3 have 24, 3 have 25, 1 have 26, 2 have 27, 3 have 28, 2 have 29, 2 have 30 and 1 have 31 Existing Linear Relations *i.e.* 24 S-boxes out of 32 have been less secure from this attack and 8 out of 32 have been immune to this attack. Again out of 32 DES S-boxes 1 have 126, 2 have 127, 2 have 130, 1 have 132, 2 have 133, 2 have 134, 1 have 135, 4 have 136, 2 have 137, 2 have 138, 1 have 141, 5 have 143, 1 have 144, 1 have 145, 1 have 147, 1 have 151, 1 have 154 and 1 have 158 8s in LAT. That is All S-boxes are less immune to this attack. Again out of 32 DES S-boxes 1 have 159, 1 have 160, 1 have 161, 4 have 162, 1 have 164, 8 have 166, 13 have 168, 1 have 173 and 2 have 174 0s in DDT. That is all S-boxes have been secured from this attack. At last out of 32 DES S-boxes 1 have 0, 3 have 18, 2 have 21, 2 have 27, 10 have 30, 12 have 36, 1 have 39 and 1 have 42 8s in DAT *i.e.* they have been less secure to this attack. The comparative analysis has proved that Linear Approximation analysis has been the most time efficient cryptanalytic algorithm for 4-bit S-boxes. In 'nosac' the lowest value is 0 and maximum value is 10 where in 'n2sac', 'n3sac' and 'nalsac' lowest values are 0, 0, 0 and maximum values are 16, 12 and 39 respectively. But numbers of optimum as well as better result *i.e.* 16 for 'nosac' is absent, close to 24 for 'n2sac', close to 16 for 'n3sac' and close to 64 for 'nalsac' has been very less in numbers. So the 32 DES 4-bit S-boxes has been observed to be less secure.

But in Table 15. out of 10 generated better 4-bit S-boxes range of 'noelr' has been 27 to 33 so it can be concluded that these S-boxes have been more immune to this attack. Now range of 'nobal' has been 134 to 200 *i.e.* very secure to linear cryptanalysis since number of 8s in LAT is very large in number. Again range of 'n0dif' has been 166 to 206 *i.e.* the result is very similar to 32 DES 4-bit S-boxes. Now All 10 4-bit S-boxes 'nosac' have been 16. *i.e.* they satisfy SAC of 4-bit S-boxes. Again the ranges of 'n2sac', 'n3sac', 'nalsac' have been 7 to 13, 13 to 16 and 39 to 45 respectively. I.e. most of them

satisfies 3rd order SAC of 4-bit S-boxes and for 2nd order SAC of 4-bit S-boxes the results have been very similar to DES 4-bit S-boxes. In case of 'nalsac' or Extended SAC the results are better than DES 32 4-bit S-boxes.

Now it is to be noted that all non-crypto S-boxes and 16! Crypto S-boxes can be generated by these two procedures by IPs over Galois field $GF(p^q)$. The crypto S-boxes have then be chosen through the analysis of relevant cryptographic properties of 4-bit S-boxes. The procedure is same for 8, 16, 32 and 64 bit S-boxes. The generated 8, 16, 32 or 64 bit S-boxes can be chosen like the way the way the 4-bit S-boxes have been chosen in this paper.

4 Conclusion

From results and discussion it can be concluded that generated and analyzed 4-bit S-boxes are better S-boxes than the 32 4-bit DES S-boxes. All algorithms of cryptographic properties and S-box generation have been given in the paper. The review and algorithms have been presented in a very lucid manner in the paper for convenient understanding of readers. The generation of 4-bit and 8-bit S-boxes has been very easy and lucid and the chosen generated 4-bit S-boxes can be claimed to be the best 4-bit and 8-bit S-boxes.

Acknowledgement

For this exhaustive work I would like to acknowledge my supervisors Dr. Ranjan Ghosh, Associate Professor, Institute of Radio Physics and Electronics, University of Calcutta and Prof.(Dr.) Amlan chakrabarti Dean, Faculty counsil of Post graduate Studies in Engineering and Technology, University of Calcutta for their continuous encouragement and help. I would also like to acknowledge Prof.(Dr.) Debatosh Guha Head Dept. Institute of Radio Physics and Electronics, University of Calcutta for providing me with the nice infrastructure.

References

[1] M. A. Abdelraheem, J. Alizadeh, H. AlKhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, *Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48*, Cryptology e-print Archive, Report-2015/988, 2015.

[2] C. Adams, S. Tavares, "The structured design of cryptographically good S-boxes", *Journal of Cryptology*, vol. 344, no. 3, pp. 27-41, 1990.

[3] C. Adams, S. J. Tavares, *Cryptology*, 1990. (`https://doi.org/10.1007/BF00203967`)

[4] C, Adams, "On immunity against Biham and Shamir's differential cryptanalysis", *Information Processing Letters*, vol. 41, pp. 77-80, 1992.

[5] A. Ahmed, A. Lbekkouri, "Determination of irreducible and primitive polynomials over a binary finite field", *Workshop surles Technologies de l'Information et de la Communication*, Agadir, Maroc, pp. 94, Dec. 2009.

[6] M. Ahmad, N. Mittal, P. Garg, M. Maftab Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos", *Perspectives in Science*, vol. 8, pp. 465-468, 2016.

[7] H. A. Alkhzaimi, L. R. Knudsen, *Cryptanalysis of Selected Block Ciphers*, Kgs. Lyngby: Technical University of Denmark (DTU). (DTU Compute PHD; No.360), 2016.

[8] M. Albrecht, C. Cid, "Algebraic techniques in differential cryptanalysis", in *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 5665, Springer, Berlin, Heidelberg, 2009.

[9] E. Bach, J. v. z. Gathen, Jr W. H. Lenstra, "Factoring polynomials over special finite fields", *Finite Fields and Their Applications*, vol. 7, no. 1, pp. 5-28, Jan. 2001.
[10] N. Bagheri, "Linear cryptanalysis of reduced-round SIMECK variants", in *Progress in Cryptology – INDOCRYPT 2015*, Lecture Notes in Computer Science, vol 9462. Springer, Cham, 2015.
[11] T. C. Bartee, D. I. Schneider, "Computation with finite fields", *Information and Control*, vol. 6, no. 2, pp. 79-98, June 1963.
[12] E. R. Berlekamp, "Factoring Polynomials Over Finite Fields", *Bell System Technical Journal*, vol. 46, no. 8, pp. 1853-1859, 1967.
[13] E. R. Berlekamp, "Factoring polynomials over large finite fields", *Math. Comp.*, vol. 24, pp. 713-735, 1970.
[14] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", in *Advances in Cryptology – CRYPTO'90*, Springer-Verlag, pp. 2-21, 1990.
[15] E. Biham and A. Shamir, "Differential cryptanalysis of Snefru", in *Advances in Cryptology – CRYPTO'91*, Springer-Verlag, pp. 156-171, 1991.
[16] E. Biham and A. Shamir, "Differential cryptanalysis of the Full 16-round DES", in *Advances in Cryptology – CRYPTO'92*, Springer-Verlag, pp. 487-496, 1992.
[17] E. Biham, *On Matsui's Linear Cryptanalysis*, Technion, Israel Institute of Technology, Israel, 1994.
[18] C. Bouillaguet, O. Dunkelman, P. A. Fouque, Leurent G, "New insights on impossible differential cryptanalysis", in *Selected Areas in Cryptography. SAC'11*, 2012.
[19] R. P. Brent and P. Zimmermann, "Algorithms for finding almost irreducible and almost primitive trinomials," in *proceedings of Brent'03 Algorithms FF*, 2003.
[20] L. Buttayan. and I. Vajda, "Searching for best linear approximation on DES-like cryptosystems", *Electronics Letters*, vol. 31, no. 11, pp. 873-874, 1995.
[21] A. Canteaut, *Differential cryptanalysis of Fesitel ciphers and differentially d-uniform mappings*, Domaine de Voluceau, France. 1997.
[22] R. Church, "Tables of irreducible polynomials for the first four prime moduli", *The Annals of Maths.*, 2nd Series, vol. 36, no. 1, pp. 198-209, Jan. 1935.
[23] B. Collard, Standaert Fx., J. J. Quisquater, "Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent", in *Fast Software Encryption*, 2008.
[24] J. M. Couveignes & sr. R. I. Lercier, J. Math.194: 77, 2013. (`https://doi.org/10.1007/s11856-012-0070-8`)
[25] T. W. Cusick, "Boolean functions satisfying a higher order strict avalanche criterion," in *Advances in Cryptology - EUROCRYPT'93*, Lecture Notes in Computer Science, vol. 765. Springer, Berlin, Heidelberg, 1994.
[26] J, R. G. Daemen and J. vandewalle, "Correlation Matrices. Fast Software Encryption", *Lecture Notes in Computer Science*, LNCS 1008, Springer Verlag, pp.2-21, 1995.
[27] J. Daemen, V. Rijmen, *AES Proposal: Rijndael*, Feb. 7, 2001. (`http://csrc.nist.gov/encryption/aes/`)
[28] M. Dawson, and S. Tavares, "An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks", in *Advances in Cryptology – EUROCRYPT'91*, pp.353-367, 1991.
[29] D. Ding, "The Differential Cryptanalysis and Design of Natural Stream Ciphers," in *Fast Software Encryption, Cambridge Security Workshop*, LNCS 809, December 1993.
[30] H. Feistel, *Block Cipher Cryptographic System*, US Patent 3798359 (Filed June 30, 1971).
[31] J. Feng, H. Chen, S. Gao, L. Fan, D. Feng, "Improved Fault Analysis on the Block Cipher SPECK by Injecting Faults in the Same Round", in *Proceedings of the 19th International Conference on Information Security and Cryptology*, 2016.
[32] N. Ferguson, *et al.*, *Improved Cryptanalysis of Rijndael*, Counterpane Internet Security, U.S.A, 2001.

[33] C. K. Fernandez, *Pascal Polynomials Over GF(2)*, Master's thesis, naval postgraduate school monterey ca dept of mathematics, Accession Number:ADA483773, year. June 2008.
[34] P. Flajolet, X. Gourdon, D. Panario, "Random polynomials and polynomial factorization," in *Lecture Notes in Computer Science*, vol. 1099, Springer-Verlag, New York/Berlin, pp. 232-243, 1996.
[35] P. Garrett, *Making, Breaking Codes*, Prentice Hall, U.S.A, 2001.
[36] S. Gao, D. Panario, "Tests and Constructions of Irreducible Polynomials over Finite Fields", in *Foundations of Computational Mathematics*, Springer, Berlin, Heidelberg, 1997.
[37] S. Gao, A. G. B. Lauder, "Hensel lifting and bivariate polynomial factorization over finite fields", *Math. Comp*, vol. 71, pp. 1663-1676, 2002.
[38] S. Gao, Erich Kaltofen, Alan G. B. Lauder, "Deterministic distinct-degree factorization of polynomials over finite fields", *Journal of Symbolic Computation*, vol. 38, no. 6, pp. 1461-1470, December 2004.
[39] D. Gerault, M. Minier, C. Solnon, "Constraint Programming Models for Chosen Key Differential Cryptanalysis", in *Principles and Practice of Constraint Programming*, 2016.
[40] A. Gorska *et al.*, *New Experimental Results in Differential-Linear Cryptanalysis of Reduced Variant of DES*, Polish Academy of Sciences, 2000.
[41] D. Golic, "Linear Cryptanalysis of Stream Ciphers", in *Fast Software Encryption, Second International Workshop*, LNCS 1008, December 1994.
[42] J. Ha, "Irreducible polynomials with several prescribed coefficients", *Finite Fields and Their Applications*, vol. 40, pp. 10-25, July 2016.
[43] G. Hammarhjelm, *Construction of Irreducible Polynomials over Finite Fields*, U.U.D.M Project Report 2014:17, Uppasala Universitet, 2014.
[44] S. Hanif, M. Imran, *Factorization Algorithms for Polynomials over Finite Fields*, Degree Project, School of Computer Science, Physics and Mathematics, Linnaeus University, 2011.
[45] C. Harpes, G. Kramer and J. Massey, "A Generation of Linear Cryptanalysis and the applicability of Matsui's Pilling-up Lemma", in *Advances in Cryptology–Eurocrypt'95*, pp. 24-38, 1995.
[46] M. Hellman and S. Langford, "Differential-Linear Cryptanalysis", in *CRYPTO'94*, LNCS 839, pp. 26-39, 1994.
[47] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis", *Journal of Cryptology*, vol. 9, pp.1-19, 1996.
[48] H. M. Heys, "A tutorial on linear and differential cryptanlysis," *Cryptologia*, vol. 26, pp. 189-221, 2002.
[49] P. A. Junod, "Linear Cryptanalysis of DES", *Lecture Notes in Computer Science*, vol. 5086. Springer, Berlin, Heidelberg, 1998.
[50] B. Kaliski, and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations", in *Advances in Cryptology - CRYPTO'94*, pp.26-39, 1994.
[51] E. Kaltofen, V. Shoup, "Subquadratic-time factoring of polynomials over finite fields", *Mathematics of Computation of the American Mathematical Society*, vol. 67(223), pp. 1179-1197, 1998.
[52] T. Kasami, S. h. Lin, W. Peterson, "Polynomial Codes", *IEEE Transactions on Information Theory*, vol. 14, no. 6, pp. 807-814, Nov. 1968.
[53] A. Kazumaro, *et al.*, *Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms*, NTT Corporation and Mitsubishi Electric Corporation, 2000.
[54] K. Kazlauskas, R. Smailiukas, G. Vaicekaus, "A Novel Method to Design S-boxes Based on Key-Dependent Permutation Schemes and its Quality Analysis", *IJACSA*, vol. 7, no. 4, pp. 93-99, 2016.
[55] J. Kilian and P. Rogaway, *How to Protect DES Against Exhaustive Key Search*, NEC Research Institute U.S.A, 2000.

[56] K. Kim, T.Matsumoto, H. Imai, "A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion," in *Advances in Cryptology-CRYPT0'90*, Lecture Notes in Computer Science, vol. 537. Springer, Berlin, Heidelberg, 1991.
[57] R. Kim, W. Koepf, "Divisibility of Trinomials by Irreducible Polynomials over F2", *International Journal of Algebra*, vol. 3, no. 4, pp.189-197, 2009.
[58] X. Lai, J. L. Massey, *Markov Ciphers and Differential Cryptanalysis*, Swiss Federal Institude of Technology, Royal Holloway University of London, 1991.
[59] S. Landau, *Standing the Test of Time: The Data Encryption Standard*, Sun Microsystems, 2000.
[60] A. K. Lenstra, "Factoring multivariate polynomials over finite fields," *Journal of Computer and System Sciences*, vol. 30, no. 2, pp. 235-248, 1985.
[61] I. V. Lisiskaya, E. D. Melnychuk, K. E. Lisitskiy, "Importance of S-Blocks in Modern Block Ciphers", *IJCN&IS*, vol. 10, pp. 1-12, 2012.
[62] S. Maitra, K. C. Gupta, A. Venkateswar, "Results on multiples of primitive polynomials and their products over GF(2)", *Theoretical Computer Science*, vol. 341, no. 1-3, pp. 311-343, 2005.
[63] P. P. Mar, K. M. Latt, "New Analysis Methods on Strict Avalanche Criterion of S-boxes", *WASE&T*, vol. 2. no. 12, 2008.
[64] D. Marquis, *Deterministic Factorization of Polynomials over Finite Fields*, Thesis : MS in Pure Mathematics, Carleton University, Ottawa, Canada, 2014.
[65] M. Matsui, "Linear Cryptanalysis method for DES cipher", in *EUROCRYPT'94*, LNCS 765, pp.386-397, 1994.
[66] M. Matsui, "The First Experimental Cryptanalysis of Data Encryption Standard," in *Advances in Cryptology–CRYPTO'94*, pp. 1-11, 1994.
[67] M. I. Mazurkov, A. V. Sokolov, "Radioelectron," *Commun.Syst*, vol. 59, pp. 212, 2016. (`https://doi.org/10.3103/S0735272716050034`)
[68] R. J. McEliece, "Factoring Polynomials over Finite Fields", in *Finite Fields for Computer Scientists and Engineers*, pp. 75-96, January 1987.
[69] A. Menezes, S. P. V. Oorschot, Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[70] F. Mirzan, *Block Ciphers and Cryptanalysis*, Department of Mathematics, Royal Holloway University of London, 2000.
[71] N. Mouha, Q. Wang, D. Gu, Preneel B, "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming", in *Information Security and Cryptology. Inscrypt 2011*, Lecture Notes in Computer Science, vol. 7537. Springer, Berlin, Heidelberg, 2012.
[72] F Muller, "Differential Attacks against the Helix Stream Cipher", in *Fast Software Encryption. FSE 2004*, Lecture Notes in Computer Science, vol. 3017. Springer, Berlin, Heidelberg, 2004.
[73] S. Murphy, M. J. B. Robshaw, *Differential Cryptanalysis, Key-dependant, S-boxes, and Twofish*, 2000.
[74] C. Nicholas, *Polynomial Factoring Algorithms and their Computational Complexity*, Honors Scholar Theses. 384, 2014.
[75] K. Nyberg, "Perfect nonlinear S-boxes", *Advances in Cryptology – EUROCRYPT'91*, pp. 378-386, 1991.
[76] K. S. Ooi, B. C. Vito, *Cryptanalysis of S-DES*, University of Sheffield Center, Taylor College, 2002.
[77] L. G. Pierson, *Comparing Cryptographic Modes of Operation using Flow Diagrams*, Sandia National Laboratories, U.S.A, 2000.
[78] B. Poonen, "Using zeta functions to factor polynomials over finite fields,", arXiv:1710.00970, Oct.3, 2017.
[79] M. O. Rabin, "Probabilistic Algorithms In Finite Fields", *SIAM Journal on Computing*, vol. 9, no. 2, pp. 273-280, May 1980.
[80] K. M. Rajashekarappa, S. Soyjaudah, K. A. S. Devi, *Comparative study on data encryption standard using differential cryptanalysis and linear cryptanalysis*, 2013.

[81] C. Richards, *Algorithms for Factoring Square-Free Polynomials over Finite Fields*, August 7, 2009.
[82] L. R?nyai, "Factoring polynomials over finite fields," *Journal of Algorithms*, vol. 9, no. 3, pp. 391-400, September 1988.
[83] L. R?nyai, "Galois Groups and Factoring Polynomials over Finite Fields", *SIAM Journal on Discrete Mathematics*, vol. 5, no. 3, August 1992.
[84] M. Rybowicz, "Search of primitive polynomials over finite fields", *Journal of Pure and Applied Algebra*, vol. 65, no. 2, pp. 139-151, 24 August 1990.
[85] M. J. O. Saarinen, "Cryptographic Analysis of All 4 4-Bit S-boxes," in *Selected Areas in Cryptography*, Lecture Notes in Computer Science, vol. 7118.Springer, Berlin, Heidelberg, 2012.
[86] C. Saha, *A Note on Irreducible Polynomials and Identity Testing*, 2008.
[87] N. R. Saxena and E. J. McCluskey, *Primitive Polynomial Generation Algorithms Implementation and Performance Analysis*, TECHNICAL REPORT(CRC TR 04-03), April-2004, Center for Reliable Computing.
[88] E. Schaefer, "A Simplified Data Encryption Standard Algorithm", *Cryptologia*, vol. 96, 1996.
[89] B. Schneier *et al.*, *The Twofish Encryption Algorithm*, John Wiley and Sons, 1999.
[90] B. Schneier, *Applied Cryptography*, Second Edition, John Wiley and Sons, 1996.
[91] B. Schneier *et al.*, *The Twofish Encryption Algorithm*, John Wiley and Sons, 1999.
[92] B. Schneier, *A Self-Study Course in Block-Cipher Cryptanalysis*, Counterpane Internet Security, 2000.
[93] B. Schneier, *Why Cryptography Is Harder than It looks*, Counterpane Internet Security, 2001.
[94] H. Schulzrinne, *Network Security: Secret Key Cryptography*, Columbia University, New York, 2000.
[95] M. Scott, *Optimal Irreducible Polynomials for* $GF(2^m)$ *Arithmetic*, Published in IACR Cryptology e-Print Archive, 2007.
[96] A. A. Sel?uk, J. Cryptol, pp. 21: 131. 2000. (`https://doi.org/10.1007/s00145-007-9013-7`)
[97] V. Shoup, "New Algorithms for Finding Irreducible Polynomials over Finite Fields", *29th Annual Symposium on Foundations of Computer Science*, 1988.
[98] I. Shparlinski, "On finding primitive roots in finite fields", *Theoretical Computer Science*, vol. 157, no. 2, pp. 273-275, 5 May 1996.
[99] S. Singh, *The Science of Secrecy*, Fourth Estate Limited, 2000.
[100] S. Vaudenay, *An Experiment on DES Statistical Cryptanalysis*, Ecole Normale Sup?rieure, France, 1995.
[101] R. G. Swan, "Factorization of polynomials over finite fields," *Pacific J. Math.*, vol. 12, no. 3, pp. 1099-1106, 1962.
[102] M. Tanaka, T. Hamaide, K. Hisamatsu and T. Kaneko, "Linear cryptanalysis by Linear Sieve Method," *IECE Transactions on Fundamentals of Electronics, Communications and Computer Science*, vol. E81-A(1), pp. 82-87, 1998.
[103] S. Vaudenay and S. Moriai, "Comparison of the Randomness Provided by Some AES Candidates", in *EUROCRYPT'94*, Springer Verlag no. 950, pp. 386-397, 1994.
[104] D. Q. Wan, "Factoring multivariate polynomials over large finite fields", *Math. Comp.*, vol. 54, pp, 755-770, 1990.
[105] J. Wang, D. Zheng, *Simple method to find primitive polynomials of degree n over* $GF(2)$ *where* 2^n-1 *is a Mersenne prime OL*, 4 March 2014. (`http://www.paper.edu.cn/lwzx/en_releasepaper/content/4587059`)
[106] L. Wang, Q. Wang, Des. Codes Cryptogr. 63: 87, 2012. (`https://doi.org/10.1007/s10623-011-9537-6`)
[107] A. F. Webster, S. E Tavares, "On the Design of S-boxes," in *Advances in Cryptology - CRYPTO'85*, Lecture Notes in Computer Science, vol. 218. Springer, pp.523-534, Berlin, Heidelberg, 1986,
[108] E. W. Weisstein, *Integer Polynomial*, From MathWorld–A Wolfram Web Resource. (`http://mathworld.wolfram.com/IntegerPolynomial.html`)

[109] H. Wu, B. Preneel, "Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy," in *Advances in Cryptology - EUROCRYPT'07*, Lecture Notes in Computer Science, vol. 4515, Springer, Berlin, Heidelberg, 2007.
[110] H. Wu, T. Huang, P. H. Nguyen, H. Wang, S. Ling, "Differential Attacks against Stream Cipher ZUC", in *Advances in Cryptology - ASIACRYPT'12*, Lecture Notes in Computer Science, vol. 7658. Springer, Berlin, Heidelberg, 2012.
[111] X. L. Yu, W. L. Wu, Z. Q. Shi, et al, J. Comput. Sci. Technol. 30: 1358. 2015. (`https://doi.org/10.1007/s11390-015-1603-5`)
[112] A. Youssef, S. Tavares, "Resistance of Balanced S-boxes to Linear and Differential Cryptanalysis," *Information Processing Letters*, vol. 56, pp. 249-252, 1995.
[113] J. K. M. S. U. Zaman, S. Dey, R. Ghosh, "An Algorithm to find the Irreducible Polynomials over Galois Field $GF(p^m)$", *International Journal of Computer Applications*, vol. 109, no. 15, pp. 24-29, January 2015.
[114] M. Zivkovic, "Table of Primitive Binary Polynomials," *Mathematics of Computation*, vol. 63(207), pp. 301-301, July 1994.
[115] C. Y. Y. Design, *Analysis and applications of cryptographic techniques*, Department of Mathematics, Royal Holloway University of London, year, 2000.
[116] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC 1977.
[117] Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, MD 1999.

Biography

Sankhanil Dey has now been a Registered Ph.D. student of A K Choudhury School of Information Technology, University of Calcutta, Kolkata, India. He did M. Tech. from department of Radio Physics and Electronics, University of Calcutta and was a Senior Research Fellow in Institute of Radio Physics and Electronics of University of Calcutta upto 30th November 2016. He was a teaching assistant as well as a guest teacher in A K Choudhury School of Information Technology, University of Calcutta, Kolkata, India. His research interest includes cryptography and cryptology, Boolean functions, applications of Finite fields or Galois fields in cryptography, elliptic curve cryptography, light weight cryptography and application of cryptographic algorithms in FPGA technology.He authored many research articles in several archives, International Journals, Books and conferences.

Prof. Ranjan Ghosh was born on November 1947 is now associated with Dumkal Institute of Engineering and Technology, Murshidabad after complete retirement at the age of 65 from the department of Radio Physics and Electronics of the Calcutta University as Associate Professor after rendering continuous services since March 1980. Prof. Ghosh studied for B. Tech, M. Tech and Ph. D (Tech) degrees of the Calcutta University from the same department between 1967 and 1980. Between 1982 and 1984 he had a brief stay at the Ioffe Physico-Technical Institute, Leningrad (now St. Petersburg) for post-doctoral research. The area of his pre-doctoral and post-doctoral research interest was the simulation studies of IMPATT Devices and its applications in microwave and optical engineering. Subsequently, he shifted to simulation studies of ion implantations undertaken in silicon process technology. His latest interest is involved with security issues of data, text as well as video, covered by the field of cryptography.

Guide for Authors
International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.