Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

MANETs using Pairings

Research Analysis of Cyber

Two-Party Threshold Key

Introduction to WiMAX Technology

Discovering Thoughts, Inventing Future

VOLUME 15 ISSUE 4 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 15 Issue 4 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board (Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 July-1 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Two-Party Threshold Key Agreement Protocol for Manets using Pairings

By Ch. Asha Jyothi, G. Narsimha, J. Prathap & Gorti Vnkv Subba Rao
JNTUH College of Engineering Jagtial, India

Abstract- In MANET environment, the nodes are mobile i.e., nodes move in and out dynamically. This causes difficulty in maintaining a central trusted authority say Certification Authority CA or Key Generation Centre KCG. In addition most of cryptographic techniques need a key to be shared between the two communicating entities. So to introduce security in MANET environment, there is a basic need of sharing a key between the two communicating entities without the use of central trusted authority. So we present a decentralized two-party key agreement protocol using pairings and threshold cryptography ideas. Our model is based on Joux's three-party key agreement protocol which does not authenticate the users and hence is vulnerable to man-in-the-middle attack. This model protects from man-in-the-middle attack using threshold cryptography.

Keywords: pairing-based cryptography, threshold cryptography, bilinear maps, mobile ad hoc networks, key agreement protocol.

GJCST-E Classification : C.2.2

TWOPARTYTHRESHOLDKEYAGREEMENTPROTOCOLFORMANETSUSINGPAIRINGS

Strictly as per the compliance and regulations of:

Two-Party Threshold Key Agreement Protocol for Manets using Pairings

Ch. Asha Jyothi [α], G. Narsimha [σ], J. Prathap [ρ] & Gorti Vnkv Subba Rao [ω]

Abstract- In MANET environment, the nodes are mobile i.e., nodes move in and out dynamically. This causes difficulty in maintaining a central trusted authority say Certification Authority CA or Key Generation Centre KCG. In addition most of cryptographic techniques need a key to be shared between the two communicating entities. So to introduce security in MANET environment, there is a basic need of sharing a key between the two communicating entities without the use of central trusted authority. So we present a decentralized two-party key agreement protocol using pairings and threshold cryptography ideas. Our model is based on Joux's three-party key agreement protocol which does not authenticate the users and hence is vulnerable to man-in-the-middle attack. This model protects from man-in-the-middle attack using threshold cryptography.

Keywords: pairing-based cryptography, threshold cryptography, bilinear maps, mobile ad hoc networks, key agreement protocol.

I. Introduction

Wireless technology [22] is suitable of communicating virtually every location on the plane of the earth. Most of the people exchange information every day using pagers, cellular telephones, laptops, several types of personal digital assistants (PDAs) and other wireless communication products. A Mobile Ad hoc NETwork (MANET) is one that comes into practice as needed, without the support of existing infrastructure or any other kind of fixed stations. MANET is an independent system of mobile hosts (also serving as routers), connected by wireless links. In a MANET, no infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. The important natural characteristics of MANETs [22] include frequently changing Topology, Lack of Central Administration, Battery Power supply or Restricted Energy, Restricted bandwidth, Physical Security fear.

Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures extremely vulnerable to penetration, eavesdropping, interference, and so on. Security [22] is considered to be the major "barrier" in the commercial use of this technology. Security is indeed one of the most difficult problems to be solved in these networks due to lack of centralized network management. Most of the security mechanisms essentially require a secret key or session key or master key to be shared between the two communicating entities. So there is a need to share a key between the sender and receiver without the use of centralized network management or certification authority.

Key agreement is one of the basic cryptographic essentials. This is needed in cases where two or more users want to communicate securely among themselves. The first two-party key sharing protocol was introduced by Diffie-Hellman. Since its detection in 1976, the Diffie-Hellman protocol [1] has become one of the most well-known and mostly used cryptographic primitive. In its basic version, it is an efficient solution to the problem of creating a common secret between two participants. Since this protocol is also used as a building block in many complex cryptographic protocols, finding a generalization of Diffie-Hellman would give a new tool and might lead to new and more efficient protocols. But this is an unauthenticated protocol in the sense that an adversary who has control over the communication channel can use the man-in-the-middle attack to share two separate keys with the two users, without the users being aware of this. In this paper, we present a secure two-party key agreement protocol that protects from man-in-the-middle attack. Our protocol is based on Joux's protocol [1] which in turn is the generalization of Diffie-Hellman protocol.

One round tripartite key agreement Joux's protocol [1] uses Weil and Tate Pairings and the idea of Diffie-Hellman. These pairings were first used in cryptology as cryptanalysis tools to decrease the complexity of the discrete logarithm problem on some "weak" elliptic curves, but they are also used today to build cryptographic systems.

In this paper, we present a secure two-party key agreement protocol for MANET environment. This model extends the popular known Joux's tripartite key agreement protocol [1] to two-partite with minor modifications. Similar to Joux model [1], this model uses pairings or bilinear maps, unlike Joux this model uses threshold cryptography. Recently Pairing-based

Author α σ : JNTUH College of Engineering, Jagtial, Nachupally, Kondagattu, Karimnagar, Telangana, India.
e-mails: asha.prathap@yahoo.co.in, narsimha06@gmail.com
Author ρ : Visvesvaraya College of Engg & Tech, Hyderabad.
e-mail: prathap.jakati@gmail.com
Author ω : Vice Principal,Sree Dattha Institutions,Hyderabad.
e-mail: gvnkvsubbarao@yahoo.com

cryptography in the form of Identity-based cryptography has become a highly working research issue.

The paper is organized as: Section II discusses on the background fundamentals needed to understand the proposed model. Section III discusses on the previous work done to share a key between two entities using pairings. Section IV talk about the detailed description of the proposed model. Section V gives the software implementation of the proposed model and Section VI confers the conclusion and future enhancements that can be done to improve the model.

II. Preliminaries

a) Bilinear Maps

The bilinear map was proposed originally as a tool for attacking elliptical curve encryption by reducing the problem of discrete algebra on an elliptical curve to the problem of discrete algebra in a finite field, thereby reducing its complexity. However, this method has been used recently as an encryption tool for information protection, instead of an attacking tool. Bilinear pairing is equivalent to a bilinear map.

Consider two additively written abelian groups A1 and A2; the identity element being 0. Also consider a multiplicatively written cyclic group C; the identity element being 1. A pairing [2][17] on A_1, A_2 and C is a non-degenerate, bilinear map

$$e : A_1 \times A_2 \rightarrow C.$$

A bilinear pairing e is a function which maps a pair of points on an elliptic curve E, defined over fields A1 and A2, to an element of the multiplicative group of a finite extension field C. This mapping is said to be pairing as it maps a pair of elliptic curve points. The pairing e has the following characteristics:

Non-degenerate: Given a point $\mathcal{O} \neq X \in A_1$ there exists a point $Y \in A_2$ such that e $Y \in A_2$; Where $\mathcal{O}$ is the point at infinity on the elliptic curve over the finite field A1.

Bilinear: for all points $X, X_1, X_2 \in A_1$, and $Y, Y_1, Y_2 \in A_2$ and $u, v \in Z$ we have

$$e(X_1 + X_2, Y_1) = e(X_1, Y_1)\, e(X_2, Y_1),$$
$$e(X_1, Y_1 + Y_2) = e(X_1, Y_1)\, e(X_1, Y_2).$$

This can be redefined in the following way:

$$e([u]X, [v]Y) = e(X, Y)^{uv} = e([v]X, [u]Y;.$$

where $[u]X = X + X + .. + X$ (u times)

Computable: There exists a computationally efficient algorithm to find e(X, Y) for all $X \in A_1$ and $Y \in A_2$.

Laws of Bilinear Pairings: The following equations holds good for the bilinear pairing e. Consider $X \in A_1$, and $Y \in A_2$ and $u, v \in Z$ and $\mathcal{O}$ is the point at Infinity.

$$e(X, \mathcal{O}) = e(\mathcal{O}, Y) = 1$$
$$e(-X, Y) = e(X, Y)^{-1} = e(X, -Y)$$
$$e([u]X, Y) = e(X, Y)^{u} = e(X, [u]Y)$$
$$e([u]X, [v]Y) = e(X, Y)^{uv}$$

Some of the examples of cryptographic bilinear maps are Weil Pairing [11] and Tate Pairing [5]. Pairings in elliptic curve cryptography are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field.

There are two types of pairings commonly used in the cryptography literature. The first type of pairing called Symmetric Pairings are of the form

$e : A_1 \times A_1 \rightarrow C$, where A_1 and C are cyclic groups of prime order p written additively and multiplicatively respectively.

The second type of pairing called Asymmetric Pairings are of the form

$e : A_1 \times A_2 \rightarrow C$, where A1, A2 are additively written cyclic groups of prime order p and C is a multiplicatively written cyclic group of prime order p.

The first form is just the special case with A2= A1. Asymmetric Pairings are further divided into two types and hence leading to totally three types of Pairings [19]

Type 1: $A_1 = A_2$ Symmetric Pairing;

Type 2 : $A_1 \neq A_2$ Asymmetric Pairing but there is an efficiently computable homomorphism function ψ: $A_2 \rightarrow A_1$;

Type 3 : $A_1 \neq A_2$ Asymmetric Pairing and there are no efficiently computable homomorphism functions between A_1 and A_2.

b) Threshold Cryptography

Let t and n be positive integers, $t \leq n$. A (t, n)-threshold scheme [25] is a method of sharing a secret K among a set of n participants in such a way that any t participants can compute the value of the secret, but no group of t−1 or fewer can do so.

Let the set of participants be denoted by E. The value of the secret K is chosen by the dealer, denoted D, who is a special participant not in E. When D wants to share the secret K among the participants in E, D gives each participant some partial information, called a share. The shares are distributed secretly, so no participant knows any other participant's share.

At a later time, when some qualified subset of participants $F \subseteq E$ want to compute the secret K, they will then pool their shares together. The most famous construction of a (t, n)-threshold scheme, called the Shamir Threshold Scheme [18][21], is invented in 1979. Therefore, a (t, n) threshold secret sharing scheme can protect the secret against an adversary who can intercept at most t− 1 paths. In t he proposed model D don't want to share the secret K among several participants in E, but D wants to share the key with the other end of communication say G, with whom he wants a secure communication. So D sends the shares of the secret key K through n independent paths [24] to G. When G receives at least t shares, he can recover the secret and there by a key is shared between D and E.

The opponent is facing the challenge of getting at least t shares by intercepting t paths at the same time, unless until he cannot recover the secret key.

III. Related Work

There are many key agreement protocols based on bilinear maps, and later most of them have been broken. One of the first applications of pairing based cryptography was a tripartite key agreement protocol given by Joux [1]. This key agreement protocol does not authenticate the users, and thus is subject to the attack namely man-in-the-middle. Of course, it was an important step in the advancement of pairing based cryptography. This protocol only uses pairings especially Tate pairing but does not use identity-based cryptography.

Many key agreements from bilinear maps and identity based cryptography have been since proposed. Scott [7], Smart [8], and Chen and Kudla [6] have proposed two-party key agreement protocols, none of which have been broken. All of these schemes require that all parties involved in the key agreement are clients of the same Key Generation Centre (KGC). Nalla recommends a tripartite identity-based key agreement in [9], and Nalla and Reddy recommends a authenticated tripartite identity-based key agreement scheme in [10], but both have been broken down [12, 13]. Shim presents two key agreement protocols [14, 15], but both of these schemes have been broken by Sun and Hsieh [16]. Another authenticated tripartite key agreement protocol recommended by Al-Riyami and Patterson [3] was broken by Shim [4]. Cullagh and Barreto recommend a two-party identity based authenticated key agreement. Most of the above protocols are based on identity-based cryptography.

Our proposed model is based on Joux's Protocol [1]. It uses bilinear maps (Pairings) and Threshold cryptography concepts. It does not uses Identity based cryptography(IDC) because IDC needs the use of Key Generation Centre (KCG), a centralized controller and which is infeasible in MANETs environment .

a) Joux's Protocol

Joux Protocol [1] considers the three communicating parties A, B and C want to share a secret key KABC among them. Let A, B and C chooses random integers u, v, and w $\in Z_q^*$ respectively. Consider the Symmetric Pairing e: $A_1 \times A_1 \rightarrow C$ and P is the generator of the cyclic group A1 publicly known. The Protocol continues as follows and shown in Fig. 1:

1. $A \rightarrow B, C$: $[u]P$
2. $B \rightarrow A, C$: $[v]P$
3. $C \rightarrow A, B$: $[w]P$
4. A computes $K_A = e([v]P, [w]P)^u$
5. B computes $K_B = e([u]P, [w]P)^v$
6. C computes $K_C = e([u]P, [v]P)^w$

From the laws of bilinear pairings, K_A, K_B, K_C result in the same value, say K_{ABC} . So common agreed key of A, B, C $K_{ABC} = K_A = K_B = K_C = e(P, P)^{uvw}$.

- *Assumption :* Bilinear Diffie-Hellman (BDH) [2] [Sec. 3.2.] problem is hard to compute.
- *Security :* Secure against passive opponent under the assumption that BDH problem is hard.
- *Efficiency :*
- *Communication :* Number of Rounds required is 1; number of group elements sent are 3.

Computation : 3 scalar multiplications; 3 pairing computations; 3 exponentiations.

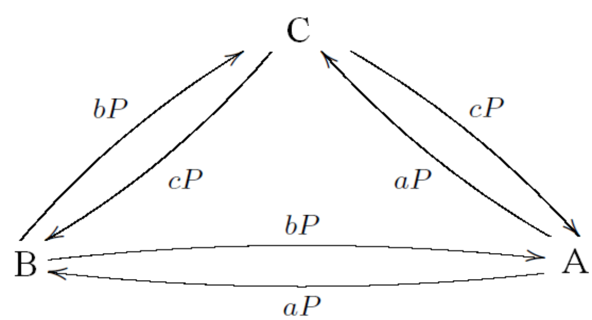


Figure 1: Joux's Tripartite Key Agreement

b) Diffie-Hellman Assumption

In this subsection we specify the version of the Diffie-Hellman problem which we will require. Consider the triple $< A_1, C, e >$ where A_1 , C are two cyclic subgroups of a large prime order q and e : A1 x $A_1 \rightarrow C$ is a cryptographic bilinear map. We take A_1 as an additive group and C as a multiplicative group.

Bilinear Diffie-Hellman BDH Problem

The strength of Joux's protocol is based on the Bilinear Diffie-Helman (BDH) [2] assumption. Let P be the generator of A1 and a, b, c are positive integers . The BDH assumption considers the computation of $e(P, P)^{abc}$ given <P, aP , bP, cP> to be hard.

c) Man-in-the-middle Attack

Let three parties A, B, C respectively have chosen secrets at random $\in Z_q^*$ and let D be the attacker chooses three random secrets u', v', w' and let D be the Consider the Symmetric Pairing e: $A_1 \times A_1 \rightarrow C$ and P is the generator of the cyclic group A1 publicly known. The attack functions as follows:

1. $A \rightarrow B, C$: [u]P.

D intercepts [u]P and instead sends [u']P to B, C.

2. $B \rightarrow A, C$: [v]P.

D intercepts [v]P and instead sends [v']P to A, C.

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

3. C $\to$ A, B: [w]P.
   D intercepts [w]P and instead sends [w']P to A, B.
4. A computes $K_1 = e([w']P, [v']P)^u = e(P, P)^{uv'w'}$.
   D computes $K_1 = e([u]P, [v']P)^{w'} = e(P, P)^{uv'w'}$.
5. B computes $K_2 = e([u']P, [w']P)^v = e(P, P)^{u'vw'}$.
   D computes $K_2 = e([v]P, [w']P)^{u'} = e(P, P)^{u'vw'}$.
6. C computes $K_3 = e([u']P, [v']P)^w = e(P, P)^{u'v'w}$.
   D computes $K_3 = e([u']P, [w]P)^{v'} = e(P, P)^{u'v'w}$.

Finally instead of a key shared between three users A, B and C, three keys are shared among four users A, B, C and D where one key K1 between A and D, another K2 between B and D and another K3 between C and D.

IV. Proposed Model

One of the applications of Joux's protocol is to share a master key between two communicating parties and one central authority say certification Authority CA or Public Key Generator PKG. MANET environment lacks central management and hence there is need for two-party key agreement protocol. Our proposed two party key agreement algorithm is based on Joux's Protocol. It makes use of Pairings (or Bilinear Maps) and Threshold cryptography concepts. Let A and B be the two communicating parties want to share a secret or session key. Let A, B respectively select integers at random $v \in Z_q^*$.

1. A $\to$ B : [u]P
2. B $\to$ A : [v]P
3. A computes $e(P, [v]P)^u = e(P,P)^{uv}$.
4. B computes $e([u]P, P)^v = e(P,P)^{uv}$.

If R=[u]P and S=[v]P are transmitted as is without applying threshold cryptography as shown in Fig 2., adversary can easily compute the key as e([u]P,[v]P) = e(P,P)uv by just intercepting [u]P and [v]P during steps 1 and 2.

To counter this we apply the concept of threshold cryptography for steps 1 and 2; steps 3 and 4 remain the same. The secrets 'u' and 'v' are split into n shares each using Shamir's secret sharing mechanism [21] to get u_i and v_i $\forall\ 1 \le i \le n$, where n is the number of multiple independent paths that exist between sender and receiver. The shares of the products [u] P and [v]P are then calculated as R_i = $[u_i]P$ and S_i = $[v_i]P$. These shares are then exchanged through n independent paths with the other party as shown in Fig 3. The n independent paths used to transmit $[u_i]P$ and $[v_i]P$ are the same, but shown differently in Fig 3 for easy understanding.

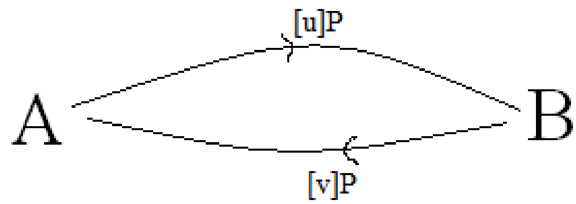


Figure 2 : [u]P and [v]P exchanged between A and B without Threshold Cryptography (i.e without dividing into n shares)

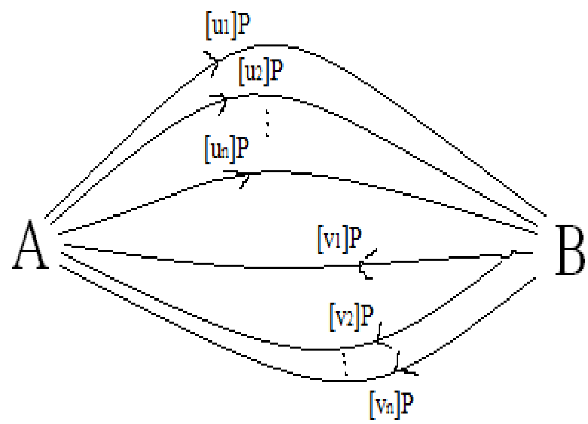


Figure 3 : The n shares of [u]P and [v]P exchanged between A and B over n independent paths

When A and B receives at least t shares of Si and Ri respectively, they can reconstruct S and R as

$$R = \sum_{i=1}^{t} R_i \prod_{1 \le m \le t, m \ne i} \frac{m}{i-m}$$

$$S = \sum_{i=1}^{t} S_i \prod_{1 \le m \le t, m \ne i} \frac{m}{i-m}$$

Hence unless the adversary intercepts at least t shares of Ri and Si, he cannot reconstruct R and S and therefore the key. Also the key is the session key that has small life time i.e., over a single session; hence the time scope for adversary to reconstruct the key is small, thereby protecting the protocol from man-in-the-middle attack.

V. Implementation

The proposed key agreement protocol is implemented in software using the Pairing-Based Cryptography Library (PBC) [20]. The results are as follows:

The Elliptic curve is chosen as: y2 = x3 + x, with x, y elements of a Field Fq; q is a prime number. A1 is a subgroup of E(Fq). C is a subgroup of Fq2. There are q+1 points on the ECC curve, i.e. #ECC(Fq) = q+1. We consider symmetric bilinear map A1 x A1 □ C.

q = 3 modulus 4.
r = order of A1 = prime factor of q+1.
h = cofactor = #ECC(Fq) / r.

The values for the parameters of the elliptic curve are chosen as:

q=87807107996633125224377819847540498158068831994142082110286533992664756308802229570786251794226622214231558587695823174592777133673174813249251299982247 91

r = 730750818665451621361119245571504901405976559617

h=12016012264891146079388821366740534204802954401251311822919615131047207289359704531102844802183906537786776

The below figure shows the output of the proposed model using the above elliptic curve parameters and pairing based cryptography library:

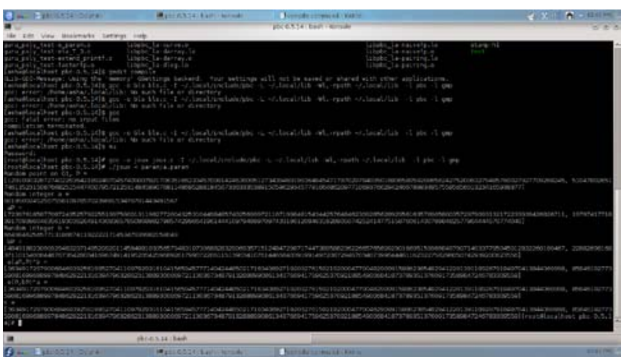


Figure 4 : Snapshot showing the execution of the proposed model

From the above execution, the key K shared between the two communicating parties A and B takes the value as (for certain integer values of u and v):

K =

[36349172979006846939256199527041109782931610415659457771404244850217163408927192032761592192000477004829099158862385482941220139118926791849704138440609 98,
85846192773590816996889978486292213163947963286231388930006972113036734879132888990861343766941759625370921885490068418737893513760917358984724678330 9559]

VI. Conclusion and Future Scope

In this article, we described a generalization of the Diffie-Hellman protocol and Joux Protocol to two-parties. Our two-party key agreement protocol uses the pairings and threshold cryptography concepts. Our model also does not assume a centralized trusted authority, which is difficult to establish in MANET environment. Therefore, this new protocol seems quite promising as a new building block to construct new and efficient complex cryptographic protocols. On the other hand, there is a scope to ensure the integrity of the secret shares. Additionally, there is scope to use this shared secret key in pairing based cryptography for encryption and decryption of messages, there by secret transmission of messages between the two communicating parties.

References Références Referencias

1. Antoine Joux.: A One Round Protocol for Tripartite Diffie-Hellman. LNCS 1838, pp. 385-393, Springer-Verlag Berlin Heidelberg 2000
2. Ian F. Blake, Gadiel Seroussi, Nigel P. Smart.: Advances in Elliptic Curve Cryptography. London Mathematical Society Lecture Note Series. 317 © Cambridge University Press 2005
3. S. S. Al-Riyami and K. G. Paterson.: Tripartite authenticated key agreement protocols from pairings. In: IMA Conference on Cryptography and Coding, volume 2898 of Lecture Notes in Computer Science, pages 332–359. Springer-Verlag, 2003.
4. K. Shim.: Cryptanalysis of Al-Riyami-Paterson's authenticated three party key agreement protocols. Cryptology ePrint Archive, Report 2003/122, 2003. http://eprint.iacr.org/2003/122.
5. P. S. L. M. Berreto, H. Y. Kim and M. Scott.: Efficient algorithms for pairing-based cryptosystems. Advances in Cryptology - Crypto '2002, LNCS 2442, Springer-Verlag (2002), pp. 354-368.
6. L. Chen and C. Kudla.: Identity based authenticated key agreement from pairings. Cryptology ePrint Archive, Report 2002/184, 2002. http://eprint.iacr.org/2002/184.
7. M. Scott.: Authenticated ID-based key exchange and remote log-in with insecure token and PIN number. Cryptology ePrint Archive, Report 2002/164, 2002. http://eprint.iacr.org/2002/164/.
8. N. P. Smart.: An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 38:630–632, 2002.
9. D. Nalla.: ID-based tripartite key agreement with signatures. Cryptology ePrint Archive, Report 2003/144, 2003. http://eprint.iacr.org/2003/144.
10. D. Nalla and K. C. Reddy.: ID-based tripartite authenticated key agreement protocols from pairings. Cryptology ePrint Archive, Report 2003/004, 2003. http://eprint.iacr.org/2003/004.
11. D. Boneh, M. Franklin.: Identity Based Encryption from the Weil Pairing. In Advances in Cryptology - Crypto '2001, LNCS 2139, Springer-Verlag (2001), pp. 213-229.
12. Z. Chen.: Security analysis on Nalla-Reddy's ID-based tripartite authenticated key agreement

protocols. Cryptology ePrint Archive, Report 2003/103, 2003. http://eprint.iacr.org/2003/103.
13. K. Shim.: Cryptanalysis of ID-based tripartite authenticated key agreement protocols. Cryptology ePrint Archive, Report 2003/115, 2003. http://eprint.iacr.org/2003/115.
14. K. Shim.: Efficient ID-based authenticated key agreement protocol based on Weil pairing. Electronics Letters, 39(8):653–654, 2003.
15. K. Shim.: Efficient one round tripartite authenticated key agreement protocol from Weil pairing, 2003.
16. H.-M. Sun and B.-T. Hsieh.: Security analysis of Shim's authenticated key agreement protocols from pairings. Cryptology ePrint Archive, Report 2003/113, 2003. http://eprint.iacr.org/2003/113.
17. Rana Barua, Ratna Dutta, and Palash Sarkar.: Extending Joux's Protocol to Multi Party Key Agreement. INDOCRYPT 2003, LNCS 2904, pp. 205–217, Springer-Verlag Berlin Heidelberg 2003
18. Sorin Iftene,: Secret Sharing Schemes with Applications in Security Protocols. Thesis submitted to the "Al. I. Cuza" University of Iasi for the degree of Doctor of Philosophy in Computer Science.
19. Steven D. Galbraith, Kenneth G. Paterson, Nigel P. Smart,: Pairings for cryptographers. 2008 Elsevier, doi:10.1016/j.dam.2007.12.010
20. PBC (Pairing-Based Cryptography) Library. http://crypto.stanford.edu/pbc/
21. A. Shamir.: How to share a secret. Communications of the ACM, 22(11):612–613, 1979.
22. Carlos de Morais Cordeiro, Dharma Prakash Agrawal.: AD HOC AND SENSOR NETWORKS Theory and Applications - Copyright © 2006 by World Scientific Publishing Co. Pte. Ltd.
23. Noel McCullagh and Paulo S. L. M. Barreto.: A New Two-Party Identity-Based Authenticated Key Agreement - Topics in Cryptology–CT-RSA 2005, Springer.
24. Gorti VNKV Subba Rao & Dr. Garimella Uma.: An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme - Global Journal of Computer Science and Technology (Network, Web & Security) Volume 13 Issue 9 Version 1.0 Year 2013.
25. Maggie Xiaoyan Cheng, Deying Li(Eds).: Advances in Wireless Ad Hoc and Sensor Networks - Springer Science & Business Media, 15-Dec-2008.

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 July-1 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Research Analysis of Cyber Security

By Rabea Masood, Qaria Zainab & Mehreen Sarshar

Fatima Jinnah Women University, Pakistan

Abstract- In an age of cyber technology with it fast pacing and ever evolving, securing data in cyber space is a major enigmawhich needs to be resolved.With vulnerabilities everywhere, data security and privacy is always at risk. This specially comes in play when services of third party are used knowingly or unknowingly. Government and business organizations are testing and implementing security and monitoring techniques to stand a better chance in raging war against cyber-crimes. Moreover, the formulation of new methods also poses new limitations of the systems as well as the users like lack of efficiency or complexity which need to be resolved in order to get better results. In this research paper some of those limitations and their solutions are discussed.

Keywords: cybercrime, security, complexity, usage, efficiency.

GJCST-E Classification : C.2.0

RESEARCHANALYSISOFCYBERSECURITY

Strictly as per the compliance and regulations of:

Research Analysis of Cyber Security

Rabea Masood [α], Qaria Zainab [σ] & Mehreen Sarshar [ρ]

Abstract- In an ageof cyber technology with it fast pacing and ever evolving, securing data in cyber space is a major enigmawhich needs to be resolved.With vulnerabilities everywhere, data security and privacy is always at risk. This specially comes in play when services of third party are used knowingly or unknowingly. Government and business organizations are testing and implementing security and monitoring techniques to stand a better chance in raging war against cyber-crimes. Moreover, the formulation of new methods also poses new limitations of the systems as well as the users like lack of efficiency or complexity which need to be resolved in order to get better results. In this research paper some of those limitations and their solutions are discussed.

Keywords: cybercrime, security, complexity, usage, efficiency.

I. Introduction

One of the major issues of today's ever updating technology dependent world is the safety of their private data. Whether it is data of the major organizations launching a new product or secret military operation details, the safety and protection of that data is the most important enigma.

In present time, the ratio of cybercrimes is increasing by each day. In a recent list presented by FBI, it is very clear that cybercrimes now are not only limited to small data theft or simple hacks through malware, but their scope is expanding way behind that horizon. Some of the recent cases of FBI (Cyber Crime branch) areRansom-ware, more than 2000 ATM hits at once, Phishing attacks and more crimes of same nature.

Even though research is being done in cyber security field and practices are also being updated but the problem of cyber-crimes is far from being solved. According to recent researches, the main limitation seems to be the approach used. The methods used are not evolving fast enough to combat the problem.

While many approaches have been implemented, there are limitations that arise with their use. Major limitations are complexity for local user, if more than one different security infrastructures used. Some of other known limitations are decrease in usage, etc. In order for these limitations to be efficiency, data collection, need for monitoring of resolved, more work needs to be done especially in field of research. Research needs to be done starting at institution level. For this purpose, usage is also needed to be monitored to study the user habits and patterns.

Author α : Department of Computer Sciences Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail: rabeam@outlook.com
Author σ : Department of Computer Sciences, Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail: qariazainab@gmail.com
Author ρ : Department of Computer Sciences, Fatima Jinnah Women University Rawalpindi, Pakistan. e-mail: msarshar@gmail.com

Another issue that needs attention is validation of software used and methods and standards used to test or validate them. This is the issue that calls out for attention desperately. As with the ever growing trend of third-party applications and new launch of software every day, there is no telling which one is safe and which is not. So to check their validity and to declare them safe or non-safe, old methods are not enough.

New methods should be built based on International Society of Automation (ISA) standards. The importance of organizational level security is also discussed.

Through this work the importance of cyber security in the modern world has been conveyed. It has also been discussed as to which limitations need to be resolved for it to be effective.

II. Related Work

Even though research is being done in cyber security field and practices are also being updated but the problem of cyber-crimes is far from being solved. According to recent researches, the main limitation seems to be the approach used. The methods used are not evolving fast enough to combat the problem.

While many approaches have been implemented, there are limitations that arise with their use. Major limitations are complexity for local user, if more than one different security infrastructures used. Some of other known limitations are decrease in efficiency, data collection, need for monitoring of usage, etc.

In order for these limitations to be resolved, more work needs to be done especially in field of research. Research needs to be done starting at institution level. For this purpose, usage is also needed to be monitored to study the user habits and patterns.

Another issue that needs attention is validation of software used and methods and standards used to test or validate them. This is the issue that calls out for attention desperately. As with the ever growing trend of third-party applications and new launch of software every day, there is no telling which one is safe and which is not. So to check their validity and to declare them safe or non-safe, old methods are not enough.

New methods should be built based on International Society of Automation (ISA) standards.

III. Conclusion

From the above work, the importance of cyber security is emphasized. It is also concludedthat closely monitoring systems and users provide and insight on the attacks and user reaction to them. Also monitored systems are less vulnerable to threats, data theft, phishing, frauds and other cyber-crimes.

Since the validation of software is necessary, so ISA standardized systems should be developed to validate them.

Also one of the major roles should be played by Government. It should take hold of every bit of events that occur in cyber space including formulation of new algorithms and techniques to prevent unauthorized access to any intruder.

In future, work would be done on monitoring techniques, their shortcomings and role play. Also, further research will include methods of secure authorizations.

a) Analysis

While analyzing the data, the first keen thing observed was the possibility of System being noncomplex as well as vulnerability free very narrow. If a system is to be secure to the highest level, user-friendliness or ease of access especially to users with basic knowledge cannot be provided. Also the fault tolerance of currently existing systems is very low, even in the high-end computers. It could only be increased by closely monitoring the capabilities of existing systems in their ability to treat vulnerabilities. The systems with higher level of robustness have more reliability rate. Some other components related to cyber security are as follows:

b) Security

The most important and most basic requirement of any system is security. In order for any system to qualify as reliable, at least basic level of security need to be provided. With passing time, the need better cyber security seems to be the basic one.

c) Efficiency

Efficiency is to use least possible resources to achieve most functionality. Encryption, antispyware and secure routes etc. are used to achieve this purpose.

d) Ease of use

The user being able to operate even with basic skill is important. With increase in level of security comes the implementation of complex infrastructures, which makes it difficult to keep the system difficulty free for a basic skilled user. Open source development and other such methodologies are being used to achieve this.

e) Robustness

To achieve this at a standard level, iterative techniques and human brain inspired infrastructures are being developed.

f) Case study

Analyses not only at organization level but at much larger level are being conducted. To make comparisons using these studies, surveys and volunteer research are being conducted.

g) Testability

Testing plays extremely important role to check functionality of the systems. The security techniques before massive or global level implementation are tested several times on smaller networks.

h) System availability

The system availability to perform the necessary immunization steps before connecting to networks are to be done.

i) Fault tolerance

User participation in detecting vulnerabilities, phishing attacks and other such threats play an important role in increase of fault tolerance.

j) Monitoring

By closely monitoring the habits of users and keeping a close watch at young user habits can reduce the number of vulnerabilities at immense level.

IV. Acknowledgements

We wish to acknowledge the guidelines and effort provided by designated professors.

References Références Referencias

1. John Malgeri, "Cyber security: a national effort to improve",Kennesaw State University, IEEE, September 2009.
2. Pal, R. ; Golubchik, L. ; Psounis, K. ; Pan Hui,"Will cyber-insurance improve network security? A market analysis",INFOCOM, 2014 Proceedings IEEE, 2014.
3. Kowtha, S.; Nolan, L.A.; Daley, R.A.Homeland Security (HST), "Cyber security operations center characterization model and analysis", IEEE, 2012.
4. Trim, P.R.J., Yang-Im Lee, "A security framework for protecting business, government and society from cyber-attacks", IEEE, 2010.
5. Feglar, T.; Comput. Sci. Consultant, Prague; Levy, J.K., "Protecting cyber critical infrastructure (CCI): integrating information security risk analysis and environmental vulnerability analysis", IEEE, 2004.
6. Teixeira, A.Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S., "Cyber security analysis of state estimators in electric power systems", Atlanta G.A, December 2010.

7. PengXie,Li, Jason H.; XinmingOu; Peng Liu; Levy, R., "Using Bayesian networks for cyber security analysis", IEEE, 2010.
8. Alex Malin, "Continuous monitoring and cyber security for high performance computing", ACM, 2007-2013.
9. Sandhu, R.; Krishnan, R.; White, Gregory B., "Towards Secure Information Sharing models for community Cyber Security", IEEE, October 2010.
10. Prof Marthie; Zama Dlamini; siphoNgobeni., "Towards a cyber-security aware rural community", IEEE, 2011.
11. Dr. Peter R.J. Trim; Dr. Yang-Im Lee; "A Security Framework for Protecting Business, Government and Society from Cyber Attacks", IEEE, 2015.
12. Rayne Reid ;Iohan Van Niekerk; "From Information Security to Cyber Security Cultures Organizations to Societies" ,IEEE, 2014
13. Jan Kallberg ;BhavaniThuraisingham; "Towards Cyber Operations, the New Role of Academic Cyber Security Research and Education", IEEE, 2012
14. Robert K. Abercrombie; Frederick T. Sheldon; Ali Mili; "Validating Cyber Security Requirements: A Case Study" IEEE, 2014.
15. Ian ELLEFSEN; "The Development of a Cyber Security Policy in Developing Regions and the Impact on Stakeholders", IEEE, 2013.
16. Anis Ben Aissa; Robert K. Abercrombie; Frederick T. Sheldon ; Ali Milli; "Quantifying Security Threats and Their Impact", IEEE, 2013.
17. Dennis K. Holstein; Keith Stouffer; "Trust but Verify Critical Infrastructure Cyber Security Solutions", IEEE, 2010.
18. Sajjan Shiva; Sankardas Roy; DipankarDasgupta; "Game Theory for Cyber Security" IEEE, 2010.
19. Rebecca LeFebvre; "The Human Element in Cyber Security: A Study on Student Motivation to Act", IEEE, 2012
20. TziporaHalevi; James Lewis;NasirMemon; "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits", IEEE,2013

Evaluation parameters	Meanings	Possible value
Security	The proposed technique is able to detect and correct errors	Yes, No
Efficiency	System is efficient in terms of software	Yes, No
Case study	Examples can use to support the methodology	Yes, No
Ease of use	Software is easy to use or learn for the user	Yes, No
Robustness	System is able to correct errors that are not specified	Yes, No
Testability	Proposed design tested or not	Yes, No
Reliability	System is working or not till the time line given	Yes, No
System availability	The time when the application must be available for use	Yes, No
Fault tolerance	The ability to remain partially operational during a failure	Yes, No
Monitoring	To keep under systematic review	Yes, No

S #	Technique	Security	Efficiency	Case study	Ease of use	Robustness	Testability	System availability	Fault tolerance	Monitoring
1	J. Malgeri et al, 2009	Yes	Yes	No	No	No	No	No	No	Yes
2	R. Pal et al, 2014	Yes	No	Yes	No	No	No	No	No	No
3	S. Kowtha et al, 2012	Yes	Yes	No	No	Yes	No	Yes	No	No
4	L. yang et al, 2010	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015
9

5	T. Feglar	Yes	No	No	Yes	No	No	Yes	No	No
6	H.Sandberget al,2010	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes
7	H. Peng et al 2010	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
8	M. Alex et al,2013	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
9	R. Sandhu et al, 2010	Yes	Yes	No	No	No	Yes	Yes	No	Yes
10	D. Zama et al,2011	Yes	Yes	N.A	Yes	No	No	Yes	No	Yes
11	T. Peter et al,2010	Yes	Yes	Yes	No	Yes	Yes	N.A	Yes	No
12	R.Rayne et al, 2014	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
13	K .Jan et al, 2012	Yes	N.A	Yes	No	N.A	Yes	N.A	Yes	Yes
14	A. Robert et al, 2011	Yes	No	No	Yes	Yes	Yes	N.A	Yes	Yes
15	E. Ian, 2014	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N.A
16	S. Robert et al, 2009	Yes	No	Yes	N.A	Yes	Yes	Yes	Yes	No
17	H. Dennis et al ,2010	Yes	N.A	No	No	Yes	Yes	Yes	Yes	Yes
18	D. Dipankaret al, 2010	No	No	Yes	No	No	Yes	No	No	Yes
19	F. Rebecca, 2012	Yes	No	Yes	Yes	No	No	Yes	N.A	Yes
20	L. James et al, 2013	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Implementation of AES with Time Complexity Measurement for Various Input

By Shraddha More & Rajesh Bansode
Mumbai university, India

Abstract- Network Security has a major role in the development of data communication system, where more randomization in the secret keys increases the security as well as the complexity of the cryptography algorithms. In the recent years network security has become an important issue. Cryptography has come up as a solution which plays a vital role in the information security system against various attacks. This security mechanism uses the AES algorithm to scramble data into unreadable text which can only be decrypted with the associated key. The AES algorithm is limited only for text as an input. It also has, the more time complexity. So it suffers from vulnerabilities associated with another type of input and time constraints. So its challenge to implement the AES algorithm for various types of input and require less decryption time. The propose work demonstrate implementation of a 128-bit Advanced Encryption Standard (AES), which consists of both symmetric key encryption and decryption algorithms for input as a text, image and audio. It also gives less time complexity as compared to existing one. At the last stage comparing the time complexity for encryption and decryption process for all three types of input. This paper also demonstrates a side channel attack on the standard software implementation of the AES cryptographic algorithm.de

Keywords: side channel attack, aes, des,rsa, encryption, decryption, cryptography, network security..

GJCST-E Classification : F.1.3 C.2.1

IMPLEMENTATIONOFAESWITHTIMECOMPLEXITYMEASUREMENTFORVARIOUSINPUT

Strictly as per the compliance and regulations of:

Implementation of AES with Time Complexity Measurement for Various Input

Shraddha More [α] & Rajesh Bansode [ρ]

Abstract- Network Security has a major role in the development of data communication system, where more randomization in the secret keys increases the security as well as the complexity of the cryptography algorithms. In the recent years network security has become an important issue. Cryptography has come up as a solution which plays a vital role in the information security system against various attacks. This security mechanism uses the AES algorithm to scramble data into unreadable text which can only be decrypted with the associated key. The AES algorithm is limited only for text as an input. It also has, the more time complexity. So it suffers from vulnerabilities associated with another type of input and time constraints. So its challenge to implement the AES algorithm for various types of input and require less decryption time. The propose work demonstrate implementation of a 128-bit Advanced Encryption Standard (AES), which consists of both symmetric key encryption and decryption algorithms for input as a text, image and audio. It also gives less time complexity as compared to existing one. At the last stage comparing the time complexity for encryption and decryption process for all three types of input. This paper also demonstrates a side channel attack on the standard software implementation of the AES cryptographic algorithm.de

Keywords: side channel attack, aes, des,rsa, encryption, decryption, cryptography, network security.

I. Introduction

Cryptography plays an important role in the security of data transmission. Data Security is a challenging concern of data communications that focuses on many areas including secure communication channel and strong data encryption technique. The secure transmission of confidential data enclosed gets a great deal of attention because of the rapid development in information technology. The predictable methods of encryption can only maintain the data security. The development of computing technology imposes stronger requirements on the cryptography schemes. The rapidly growing number of wireless communication users has led to the increasing demand for security measures and devices to protect user data transmitted over wireless channels[1].

Two types of cryptographic systems have been developed for that purpose symmetric (secret key) and asymmetric (public key) cryptosystems. Symmetric cryptography, such as in the Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) uses an identical key of the sender to encrypt the message text and receiver to decrypt the encrypted text. Asymmetric cryptography, such as the Rivest-Shamir-Adleman (RSA) uses different public keys for encryption and decryption, eliminating the key exchange problem.[2] Symmetric cryptography is more suitable for the encryption of a large amount of data. The Data Encryption Standard (DES) has been used by the U.S. government standard since 1977. However, now, it can be cracked quickly and inexpensively. The AES algorithm defined by the National Institute of Standards and Technology (NIST) of the United States has widely accepted to replace DES as the new symmetric encryption algorithm [3]. This above cryptographic algorithms are not more secure. To overcome the vulnerabilities in network security in 2000, the Advanced Encryption Standard (AES) replaced the DES to meet the ever-increasing requirements for security. In cryptography, the AES, also called as Rijndael, is a block cipher adopted as an encryption standard by the US government, which specifies an encryption algorithm capable of protecting sensitive information[4]. The Rijndael algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data into an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its unique form which is called plaintext. The AES algorithm supports 128, 192 and 256 bit key length to encrypt and decrypt data in blocks of 128 bits , hence the name AES-128, AES-192 and AES-256 respectively[5]. The hardware implementation of the AES algorithm can provide high performance, low cost for specific applications and trustworthiness compared to its software counterparts[6].

The organization of the paper is as follows, Section II describes the design overview of AES algorithm for both encryption and decryption. Section III presents implementation Details, Section IV is discussed on Experimental Results. Section V projects on future scope and conclusion.

II. Design Overview of AES

AES is a symmetric block cipher with block length of 128 bits. It allows three different key lengths 128,192 and 256 bits. In encryption process processing of 128 bit keys required for 10 rounds, 192 bit keys

Author α : Master of engineering in Information technology, TCET, Mumbai university, India. e-mail: moreshraddha30@gmail.com
Author ρ : Associate professor in Department of Information technology, TCET, Mumbai university, India.
e-mail: rajesh.bansode@thakureducation.org

required for 12 rounds and 256 bit keys required for 14 rounds which is shown in table1. AES is a round based algorithm. For encryption and decryption each round has four functions excepting last round. Last round required three functions. The encryption algorithm has four round functions SubByte( ), ShiftRows( ), MixColumn( )and AddRoundKey( ). The decryption, also has the same number of rounds with reverse transformation, order of round function is different i.e. InvShiftRow( ), InvSubByte( ), AddRoundKey( ) and InvMixColumn( ) [2]-[3].

Table 1 : AES parameters for the various AES versions

AES PARAMETERS	AES-128	AES-192	AES-256
Key Size (Bits)	128	192	256
Number of rounds	10	12	14
Plaintext box size (Bits)	128	128	128

a) AES Encryption Algorithm

The Encryption process consists of a number of different transformations applied consecutively over the data block bits in a fixed number of iterations which is called as rounds. The number of rounds depends on the length of the key used for the encryption process. 10 iterations are required for key length of 128 bits.

i. *High-level description of the algorithm*

KeyExpansions -round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

ii. *InitialRound*

1. AddRoundKey( )- Each byte of the state is combined with a block of the round key using bitwise xor.
   Rounds
2. SubBytes( )- A non-linear substitution step where each byte is replaced with another according to a lookup table.
3. ShiftRows( )-A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
4. MixColumns( )-A mixing operation which operates on the columns of the state, combining the four bytes in each column.

iii. *Final Round (No MixColumns)*

SubBytes( )
ShiftRows( )
AddRoundKey( ).

Steps : These steps are used to encrypt128-bit block.

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9 : Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

iv. *Encryption process*

Each round consists of the following four steps:

SubBytes Transformation: In this transformation, each of the byte in the state matrix is replaced with another byte as per the S-box (Substitution Box)[7]. The S-box is generated by firstly calculating the respective reciprocal of that byte in GF (2^8) and then affine transform is applied.

ShiftRows Transformation: In this transformation, the bytes in the first row of the State do not change. The second, third, fourth and fifth rows shift cyclically to the left by one byte, two bytes, three bytes and four bytes respectively [7].

MixColumns Transformation: It is the operation that mixes the bytes in each column by the multiplication of the state with a fixed polynomial matrix [7]. It completely changes the scenario of the cipher even if all bytes look very similar. The Inverse Polynomial Matrix does exist in order to reverse the mix column transformation.

AddRoundKey Transformation: In AddRoundKey transformation, a roundkey is added to the State by bitwise Exclusive-OR (XOR) operation. AddRoundKey proceeds onecolumn at a time. AddRoundKey adds a roundkey word with each state column matrix.The operation performed in AddRoundKey is matrix addition.

b) AES Decryption Algorithm

Decryption is the process of extracting the plaintext from cipher text. For decryption the same process occurs simply in reverse order by taking the 128-bit block of cipher text and converting it to plaintext by the application of the inverse of the four operations. Decryption involves reversing all the steps taken in encryption using following inverse functions.

InvSubBytes Transformation: InvSubBytes is the inverse transformation of SubBytes, in which the inverse S-box is applied to individual bytes in the State. The inverse S-box is constructed by first applying the inverse of the affine transformation, then computing the multiplicative inverse in GF(2^8).

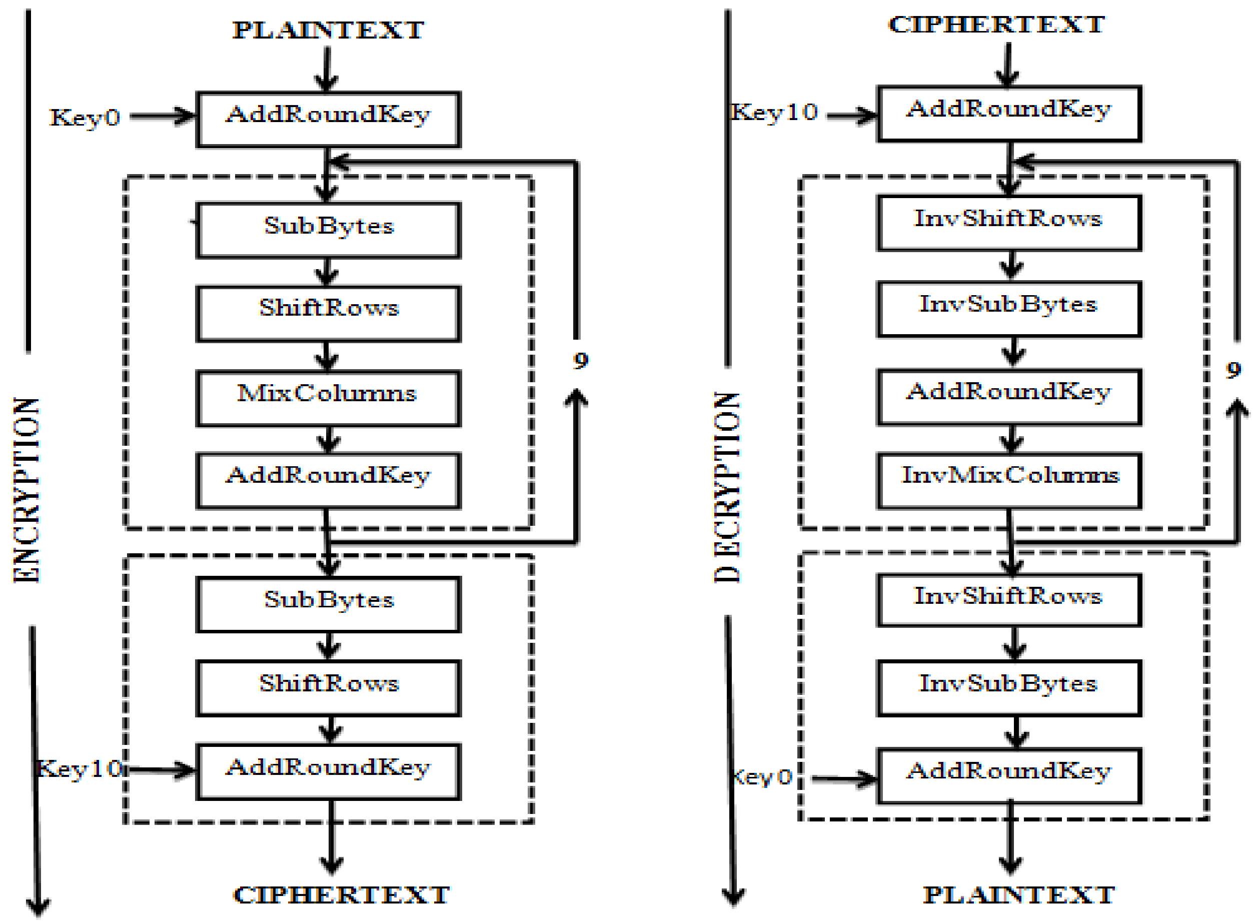


Figure 1: AES Encryption and Decryption

InvShiftRows Transformation: InvShiftRows is the inverse transformation of ShiftRows. In this transformation, the bytes in the first row of the State do not change. The second, third, and fourth and fifth rows are shifted cyclically by one byte, two bytes, three bytes and four bytes to the right respectively [2].

InvMixColumns Transformation: InvMixColumns is the inverse transformation of MixColumns. This is a complex procedure as it involves severely the byte multiplication under GF (2^8)[2].

Key Expansion (Keyexpansion Operation)

Keyexpansion refers to the process in which the 128 bits of the original key are expanded into eleven 128-bit round keys.

To compute round key (n+1) from round key (n) these steps are performed:

1. Compute the new first column of the next round key. First all the bytes of the old fourth column have to be substituted using the Subbytes operation. These four bytes are shifted vertically by one byte position and then
   XORed to the old first column. The result of these operations is the new first column.
2. Columns 2 to 4 of the new round key are calculated as shown:

- [new second column] = [new first column] XOR [old second column]
- [new third column] = [new second column] XOR [old third column]
- [new fourth column] = [new third column] XOR [old fourth column]

The key expansion algorithm generates 128 bit key for each round and one more key for initial AddRoundKey function. The same expanded key is used for encryption and decryption except for decryption it reads in reverse order.

III. Implementation Details

The system proposing aims to achieve network security by implementing appropriate countermeasures based on concept of constant time encryption against side channel timing attack to protect implementations of secret key cryptography. The contribution work includes implementing more suitable countermeasures against side channel attack.

a) System Overview

The propose system, is intended to provide secure transmission of data over the network by implementing the appropriate countermeasures against side channel attack on AES implementation which is shown in Fig.2. Here the work implementing AES 128-bit algorithm using 10 rounds by taking input as text, image and audio. In AES encryption process, system performs round functions like SubByte( ), ShiftRows( ), MixColumn( ) and AddRoundKey( ). On the other side, the decryption processperforms round functions like InvShiftRow( ), InvSubByte( ), AddRoundKey( ) and InvMixColumn( ). After that the work implementing side channel attack on the AES implementation in such a way that the receiver cannot decrypt the encrypted data. After successful implementation of side channel attack, research work implementing some appropriate countermeasures against side channel attack on AES implementation and finally evaluating their performance and soundness to prevent possible vulnerabilities and develop more secure systems.

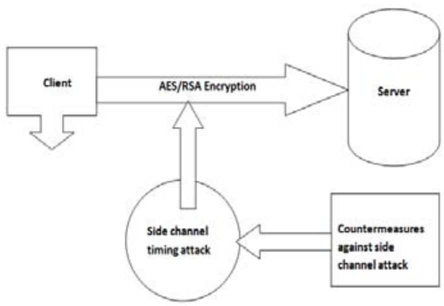


Figure 2 : System architecture

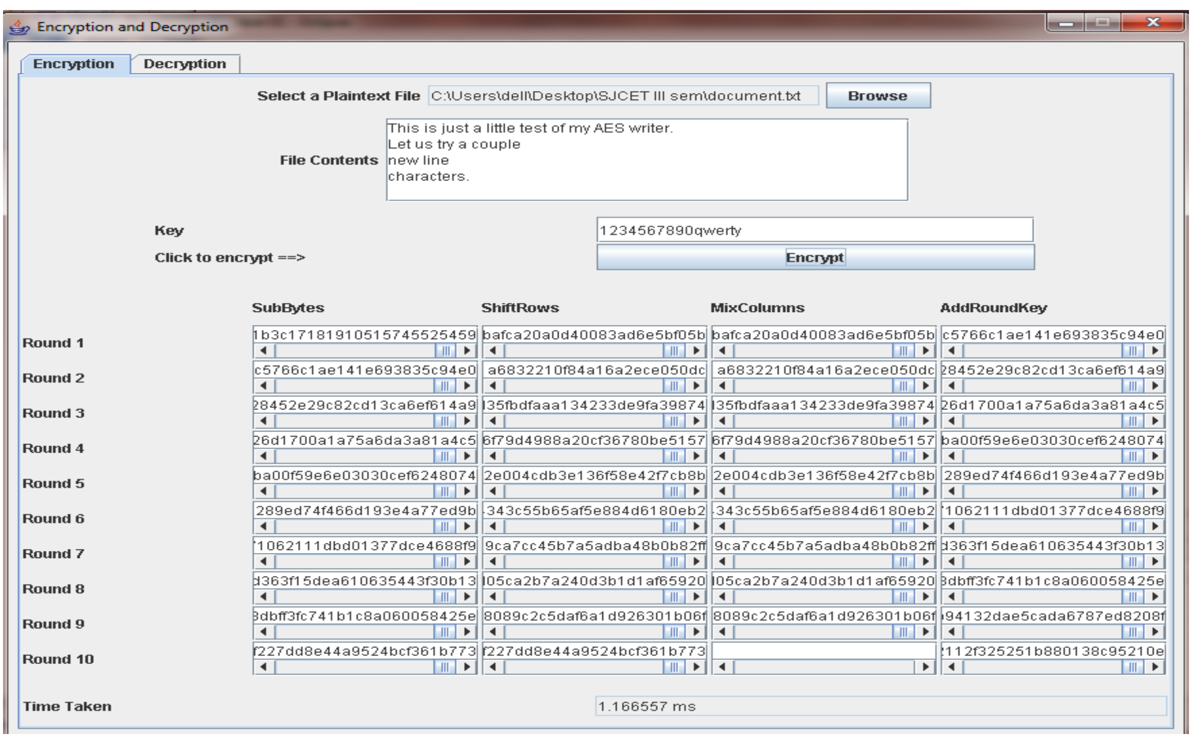


Figure 3 : AES Encryption: Input as Text

Decryption Process when input as an Text file

The work implemented 128 bit AES algorithm (10 round) decryption using text as an input by measuring performance parameter as time complexity which is shown in Fig.4.Time required for decryption process is 2.128282 milliseconds.

b) AES Implementation

The work implemented AES 128-bit, 10 rounds algorithm by taking input as text, image and audio.

Encryption Process when input as an Text file

The work implemented 128 bit AES algorithm (10 round) encryption using text as an input by measuring performance parameter as time complexity which is shown in Fig.3.Time required for encryption process is 1.166557 milliseconds.

Encryption Process when input as an audio file

The work implemented 128 bit AES algorithm (10 round) encryption using audio as an input by measuring performance parameter as time complexity which is shown in Fig.5.Time required for encryption process is 13.899532 milliseconds.

Decryption Process when input as an audio file

The work implemented 128 bit AES algorithm (10 round) decryption using audio as an input by measuring performance parameter as time complexity which is shown in Fig.6.Time required for decryption process is 20.183485milliseconds.

Encryption Process when input as an Image file

The work implemented 128 bit AES algorithm (10 round) encryption using image as an input by measuring performance parameter as time complexity which is shown in Fig.7. Time required for encryption process is 61.958627 milliseconds.

Decryption Process when input as an Image file

The work implemented 128 bit AES algorithm (10round) decryption us ing image as an input by measuring performance parameter as time complexity which is shown in Fig.8.Time required for decryption process is 31.509569milliseconds.

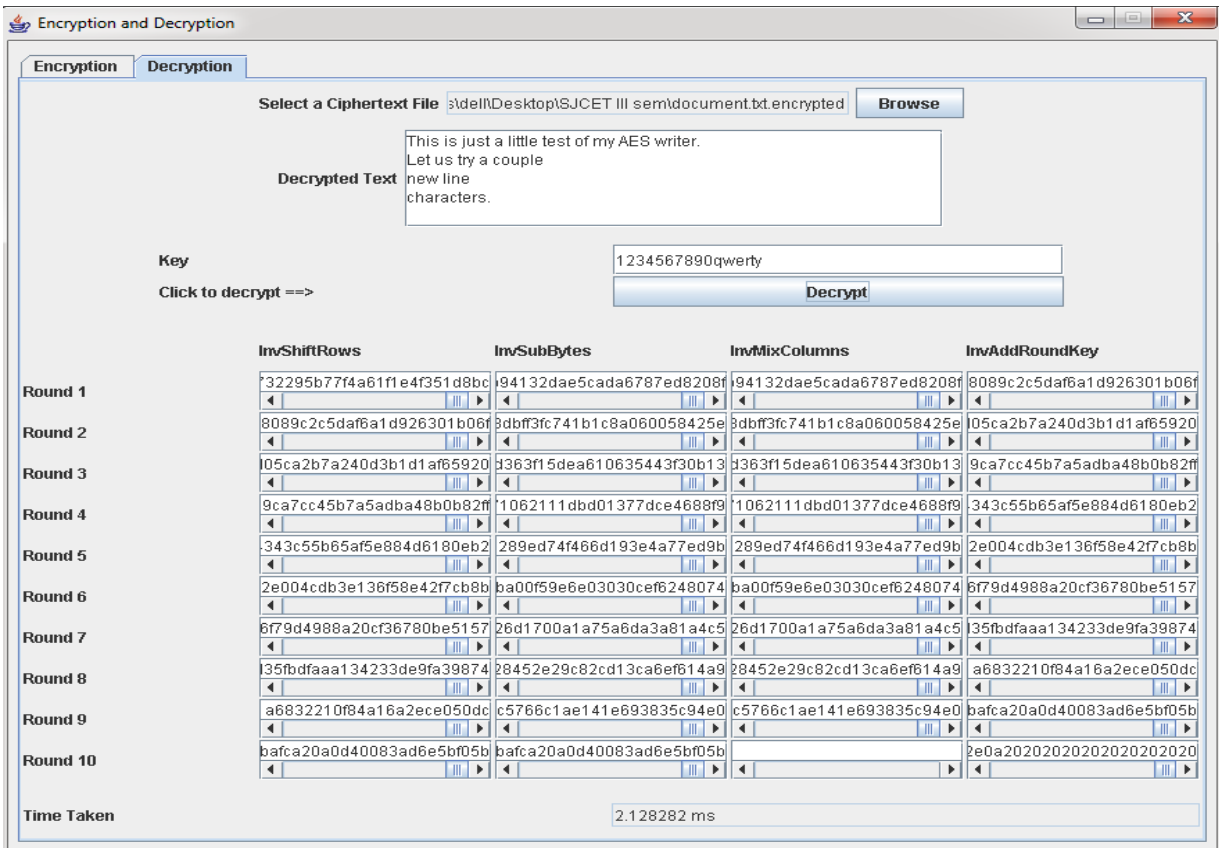


Figure 4 : AES Decryption :Input as Text

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

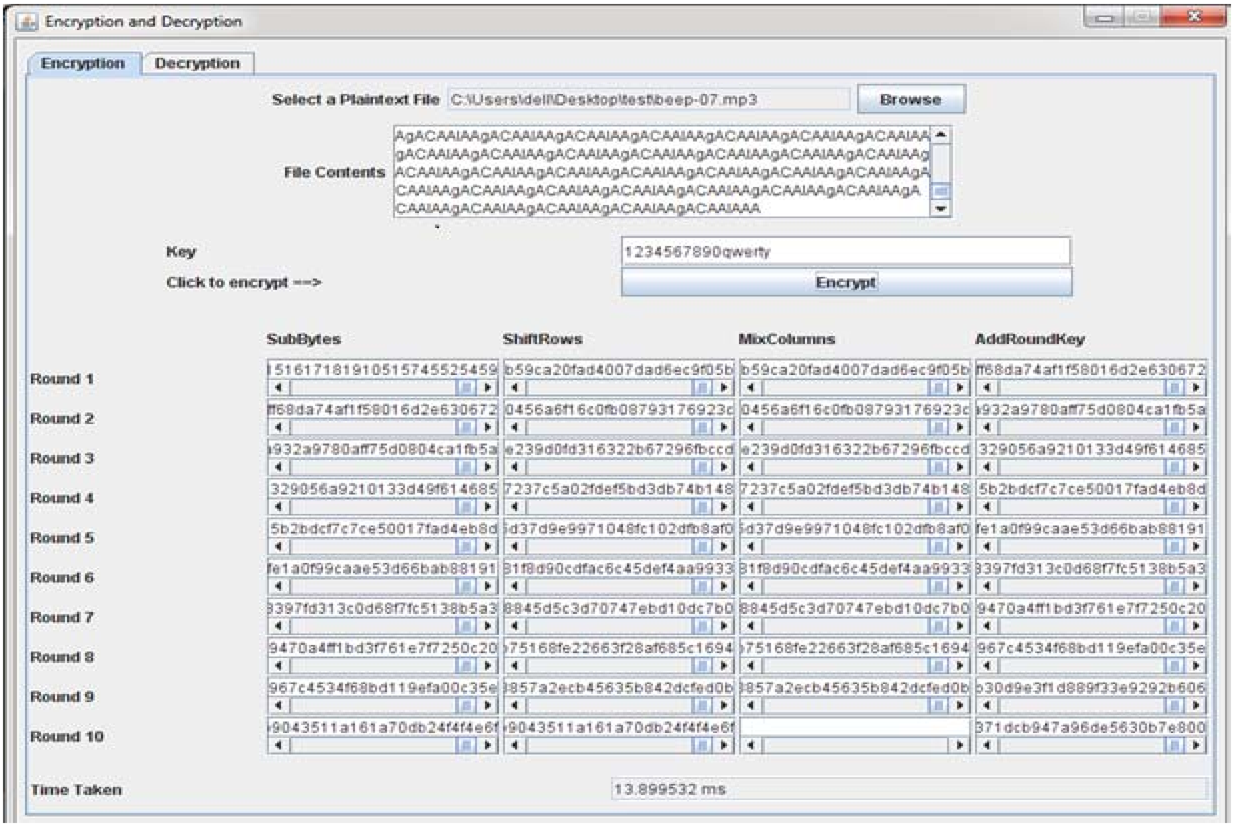


Figure 5 : AES Encryption: Input as Audio

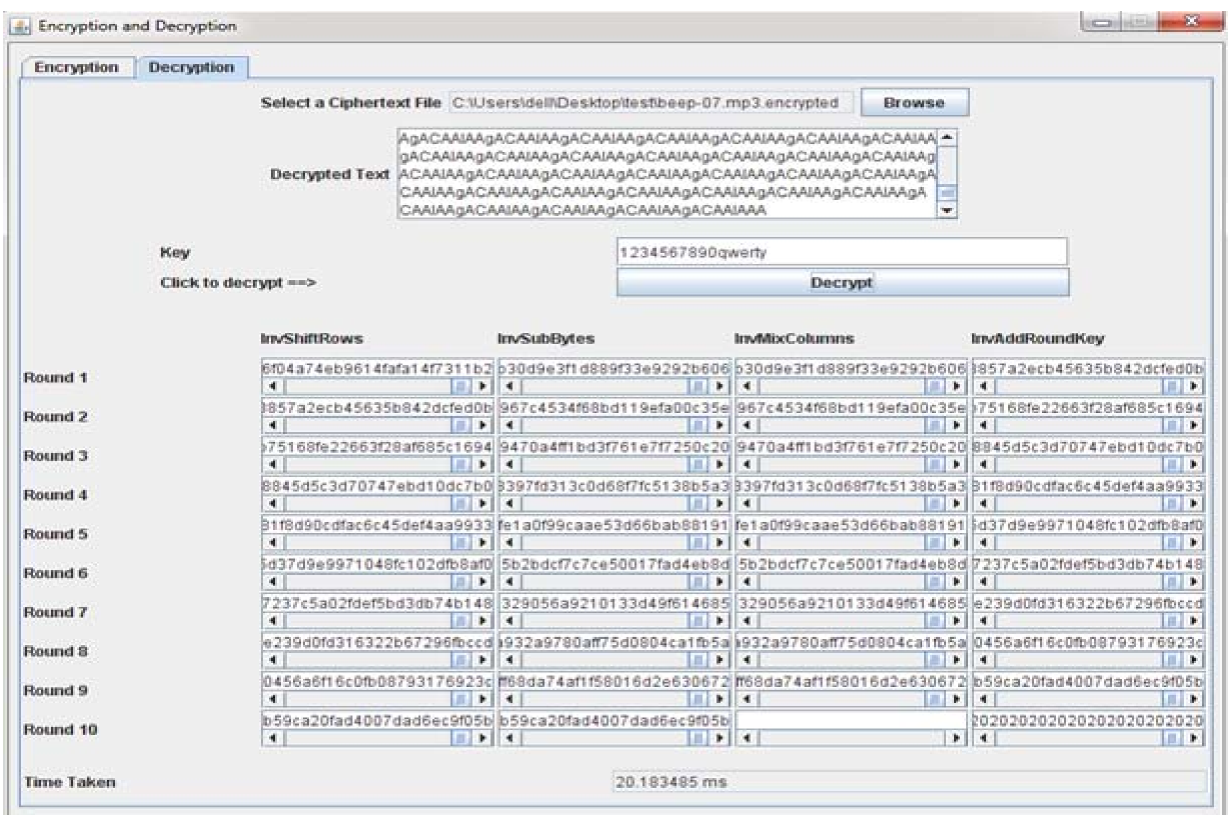


Figure 6 : AES Decryption: Input as Audio

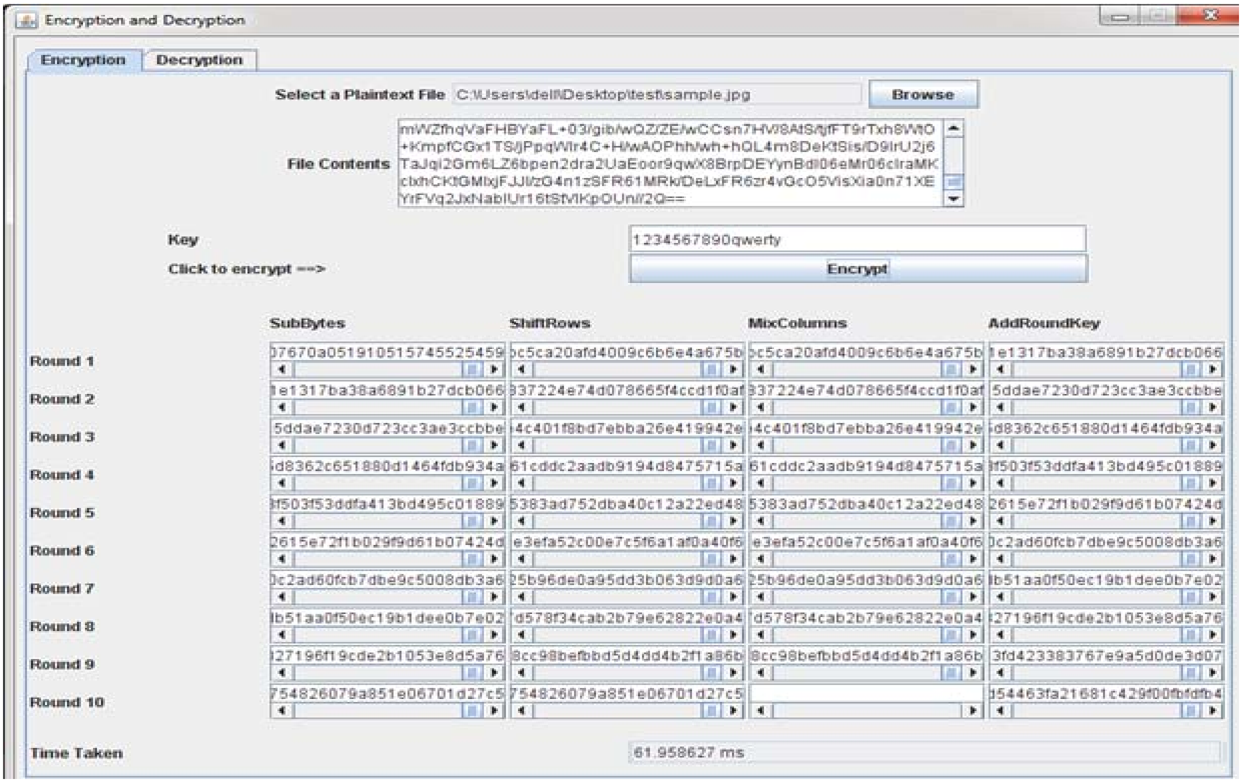


Figure 7 : AES Encryption: Input as Image

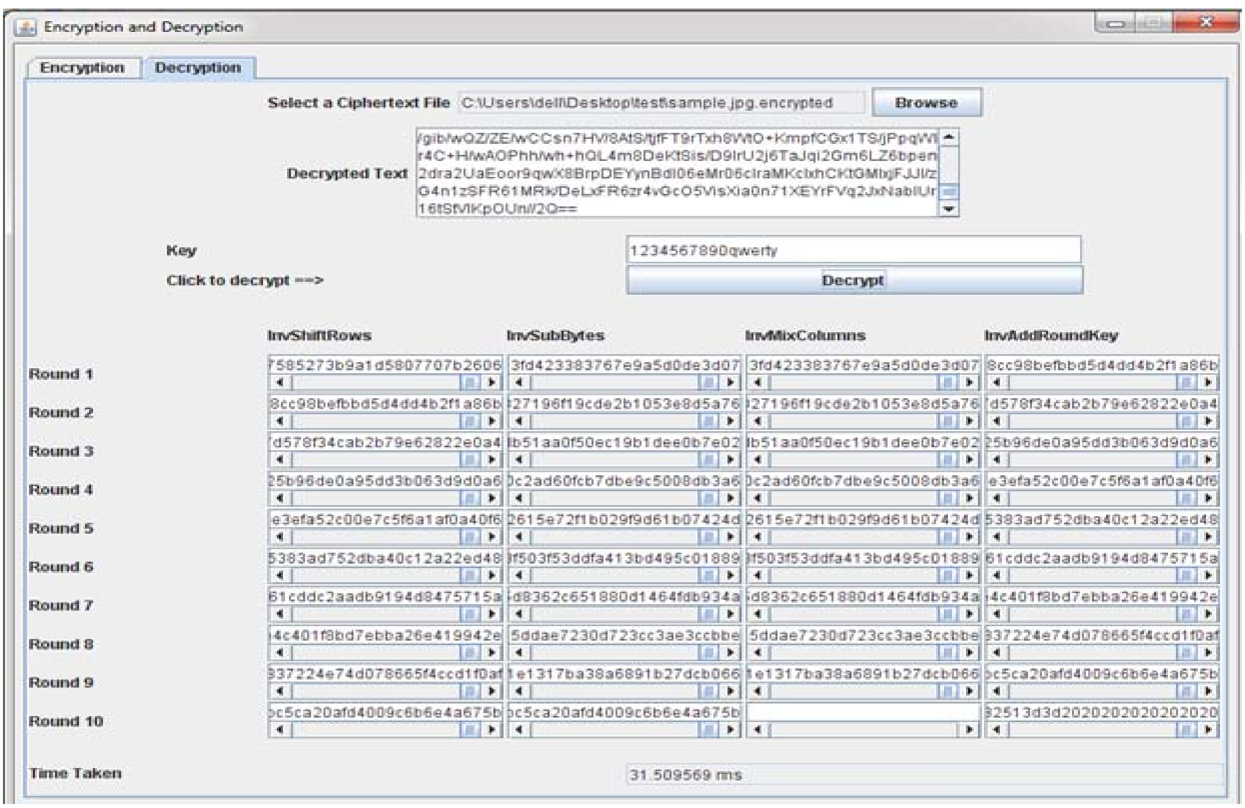


Figure 8 : AES Decryption Process: Input as Image

c) Attack on AES implementation

After successful implementation of AES algorithm. The work implemented attack in such a way that at the time of decryption, receivers cannot get the decrypted file as a plain text file instead of that the user will get the file which is in the human non-readable format which is shown in the Fig.9.

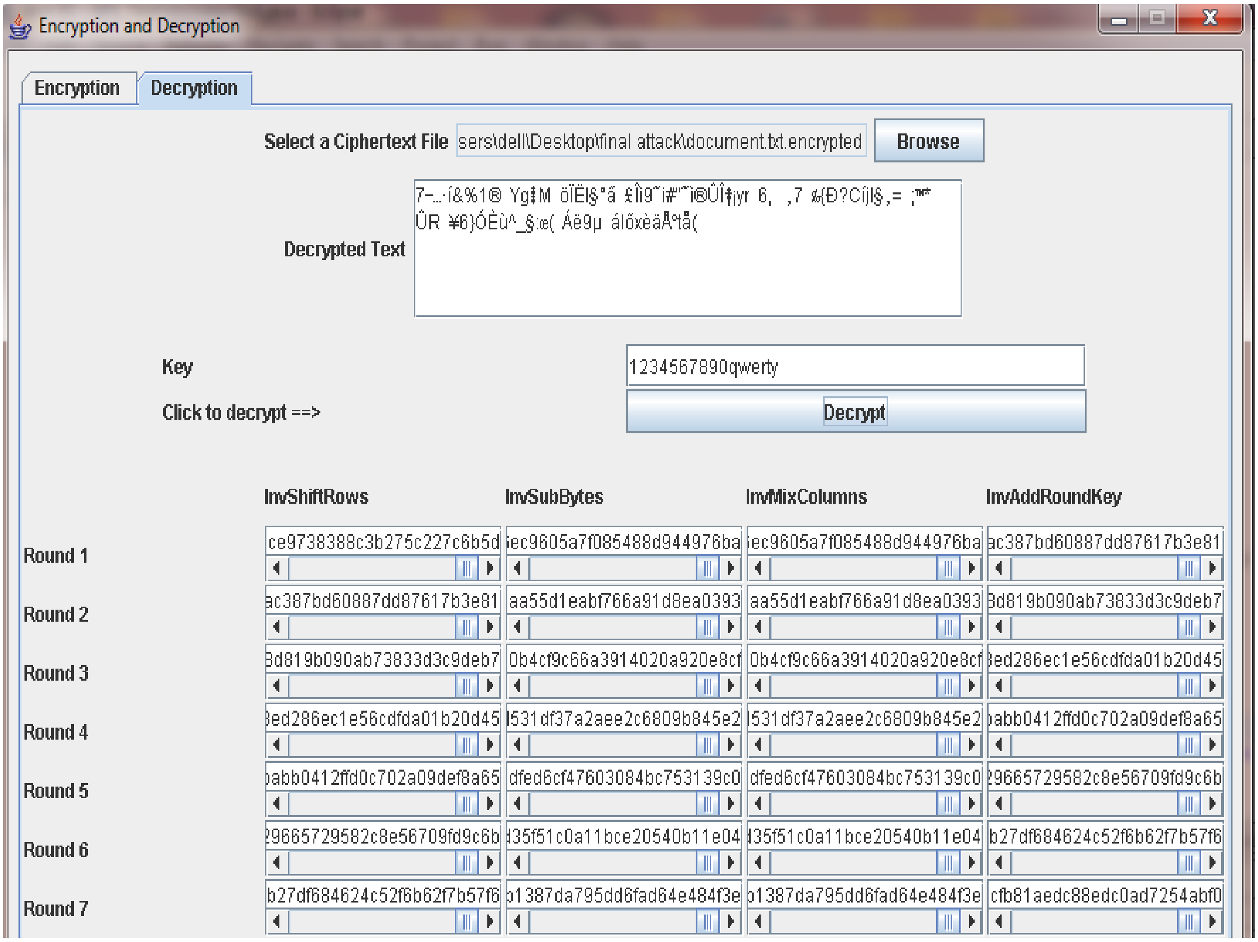


Figure 9 : A on AES implementation

IV. Experimental Results

In this section The work presented result graph of our proposed system, implementation of the AES algorithm by taking text, image and audio as input. The work used 10 rounds technique for implementing AES 128- bit algorithm.

a) Result graph for encryption time

In Fig. 10. The graph shows the time needed to encrypt the input as a text, image and audio data file by the proposed system .

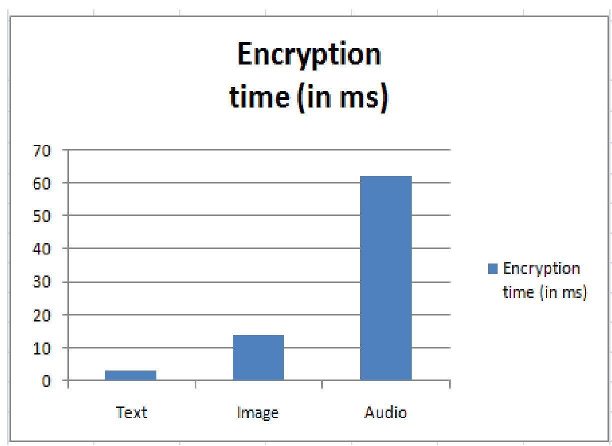


Figure 10 : Encryption time taken by AES algorithm

b) Result graph for decryption time

In Fig. 11. The graph shows the time needed to decrypt the input as a text, image and audio data file by the proposed system .

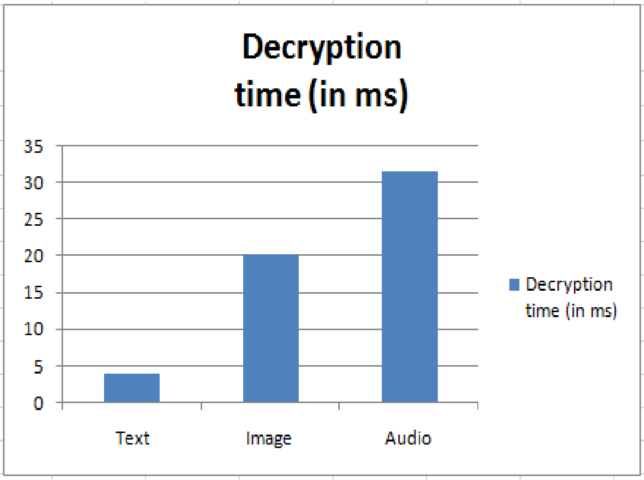


Figure 11: Decryption time taken by AES algorithm

V. Conclusion Andfuture Scope

Due to the increasing needs for secure communications a safer and more secured cryptographic algorithm has to be proposed and implemented. The Advanced Encryption Standard (AES-128bit) is widely used nowadays in many applications. In this paper, the work implemented an efficient AES128 bit encryption and decryption algorithm. The execution time for AES encryption and decryption is calculated by performing 10 round functions. The system presented an attack on AES software implementations. Future work will focus on investigating and implementing a number of countermeasures against side channel attack on AES implementation and have evaluated their performance and soundness to prevent possible vulnerabilities and develop more secure systems.

References Références Referencias

1. Vinayak Bajirao Patil, Prof.Dr.Uttam.L.Bombale ,Pallavi Hemant Dixit, "Implementation of AES algorithm on ARM processor for wireless network, " in International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, August 2013, pp.3204-3209.
2. Xinmiao Zhang and Keshab K. Parhi, "Implementation approaches for the advanced encryption standard algorithm," in IEEE Transactions , 2002.
3. Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu,"A high throughput low cost AES processor," in IEEE Communications Magazine, 2003 .
4. "Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, Nov. 2001.
5. M.Gnanambika, S.Adilakshmi, Dr.Fazal Noorbasha, "AES-128 Bit Algorithm Using Fully Pipelined Architecture for Secret Communication," in International Journal of Engineering Research and Applications Vol. 3, Issue 2, March -April 2013, pp.166-169.
6. Rishabh Jain, Rahul Jejurka2, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap, "AES Algorithm Using 512 Bit Key Implementationfor Secure Communication," in International Journal of Innovative Research in Computerand Commun-ication Engineering, Vol. 2, Issue 3, March 2014, pp. 3516-3522.
7. Vinayak Bajirao Patil, Prof. Dr. Uttam. L.Bombale, Pallavi Hemant Dixit, "Implementation of AES algorithm on ARM processor for wireless network, " in International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 8, August 2013,pp.3204-3209.
8. Ritu Pahal and Vikas kumar, "Efficient Implementation of AES," in International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 7, July 2013, pp. 290-295
9. K. Soumya, G. Shyam Kishore, "Design and Implementation of Rijndael Encryption Algorithm Based on FPGA," in International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 9, September 2013, pp.120 – 127.
10. Sumedha Kaushik and Ankur Singhal, "Network Security Using Cryptographic Techniques ,"in International Journal of Advanced Research in Computer Science and Software Engineering ,Vol. 2, Issue 12, December 2012, pp.105-107.
11. Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA forSecurity," in Global Journal of Computer Science and Technology Network, Web & Security, Vol 13, Issue 15,2013, pp.15-22.
12. H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/sec VLSImple mentation of the AES Rijndael algorithm," in Proc. CHES 2001, Paris, France, May 2001, pp. 51-64.
13. Navraj Khatri, Rajeev Dhanda, Jagtar Singh," Comparison of power consumption and strict avalanche criteria at encryption/Decryption side of Different AES standards,'' International Journal Of Computational Engineering Research, Vol. 2 Issue. 4, August 2012.
14. Das Debasis, Misra Rajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No.6, November 2011, pp. 204.
15. Hiremath.S. and Suma.M.S.,"Advanced Encryption Standard Implemented on FPGA,"in IEEE Inter. Conf. Comp Elec Engin. (IECEE), vol. 02,issue. 28, pp.656-660,Dec.2009.
16. Chehal Ritika, Singh Kuldeep. "Efficiency and Security of Data with Symmetric Encryption Algorithms," inInternational Journal of Advanced

Research in Computer Science and Software Engineering, Vol. 2, Issue 8, August 2012, pp. 1.

17. Z. Xinjie, W. Tao, M. Dong , Z. Yuanyuan, L. Zhaoyang, "Robust First Two Rounds Access Driven Cache Timing Attack on AES," in IEEE InternationalConference on Computer Science and Software Engineering , Dec. 2008, Wuhan, Hubei, China, pp. 785 – 788.
18. P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems," in 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1996, Springer-Verlag London UK, pp. 104-113.
19. W. Stallings, Cryptography and network security.
20. J. Daemen and V. Rijmen, AES Proposal: Rijndael (Version 2).

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Cross Layer Model to Support Qos for Multimedia Applications on Wireless Networks

By Vijayalakshmi M & Linganagouda Kulkarni
BVB College of Engineering and Technology, India

Abstract- Supporting multimedia application over wireless networks poses multiple challenges. Currently the use of cross layer architectures and Scalable Video Coding (SVC) techniques are considered to support multimedia applications. The current architectures fail to address the tradeoff that exists between the end to end delay and the Quality of Service (QoS) provisioning of the video data to be delivered. To address this issue this paper introduces the QoS improvement scheme in video transmission model based on a cross layer architecture. A novel MAC encoding of the SVC video is considered in the proposed model. Based on the physical layer conditions and the QoS achievable the model adapts to meet the stringent delay requirements of video delivery. Routing layer optimization is achieved by accounting for the pending packets queues in every neighboring node. The experimental study conducted prove the robustness of the proposed model by comparing with the existing schemes. Comparisons in terms of the transmission error rates, system utility and quality of reconstruction are presented.

Keywords: scalable video coding (SVC), cross layer, H.264, multimedia, quality of service (QoS), MAC, routing, encoding.

GJCST-E Classification : *C.2.1*

ACROSSLAYERMODELTOSUPPORTQOSFORMULTIMEDIAAPPLICATIONSONWIRELESSNETWORKS

Strictly as per the compliance and regulations of:

A Cross Layer Model to Support Qos for Multimedia Applications on Wireless Networks

Vijayalakshmi M [α] & Linganagouda Kulkarni [σ]

Abstract- Supporting multimedia application over wireless networks poses multiple challenges. Currently the use of cross layer architectures and Scalable Video Coding ($\boldsymbol{SVC}$) techniques are considered to support multimedia applications. The current architectures fail to address the tradeoff that exists between the end to end delay and the Quality of Service ($\boldsymbol{QoS}$) provisioning of the video data to be delivered. To address this issue this paper introduces the $\boldsymbol{QoS}$ improvement scheme in video transmission model based on a cross layer architecture. A novel $\boldsymbol{MAC}$ encoding of the SVC video is considered in the proposed model. Based on the physical layer conditions and the $\boldsymbol{QoS}$ achievable the model adapts to meet the stringent delay requirements of video delivery. Routing layer optimization is achieved by accounting for the pending packets queues in every neighboring node. The experimental study conducted prove the robustness of the proposed model by comparing with the existing schemes. Comparisons in terms of the transmission error rates, system utility and quality of reconstruction are presented.

Keywords: scalable video coding (SVC), cross layer, H.264, multimedia, quality of service (QoS), MAC, routing, encoding.

I. Introduction

The increasing demand by of users to access infotainment solutions on wireless networks aid development of novel models to support applications [1] [2]. To support such multimedia application delivery on wireless networks high bandwidth [3], quality of service (QoS) [4], stringent delay requirements have to be accounted for. Wireless networks are characterized by limited bandwidth, hop based routing and error prone nature. This nature tends to induce transmission loss, delayed delivery and high jitter in supporting video streaming applications [5] [6]. The $ISO/IEC\ MPEG$ [7] group and the $ITU-T\ VCEG$ [8] groups have standardized the Scalable Video Coding (SVC) extension to the existing $H.264$video compression standard which can be adopted to support multimedia applications on wireless networks [9]. The SVC compression technique enables video encoding taking into account the varied quality, spatial and temporal parameters, thus providing adaptability. Considering wireless networks based on the network conditions, network configuration, application demands and QoS parameters the SVC video encoding can be adopted to support multimedia transmissions.

Author α σ: Department of Computer Science and Engineering BVB College of Engineering and Technology, Vidyanagar, Hubli.
e-mail: vijum11@gmail.com, linganagouda@yahoo.co.uk

Adoption of the SVC for multimedia data delivery on wireless networks cannot be considered as a holistic solution. Video transmissions are delay bound and delivery of the data packets within the delay deadlines is of most importance [1] [5] [11] [14]. The multimedia data delivery is achieved through hop based mechanisms in wireless networks. The distortion and the available channel capacity vary during data delivery which needs to be accounted for. The end to end delay varies based on the physical layer condition and the buffering mechanism at the medium access. The transmission errors induced cause packet retransmission overheads. Based on the physical layer conditions the next hop routing mechanism also requires constant updation. In short it can be stated that, delivery of delay sensitive data on wireless networks put forth variations in the physical layer, medium access control layer (MAC) and the routing layer. Apart from these variations observed it is also critical to establish a balance between the data delivery and the QoS provided. Providing QoS at the cost of delayed data delivery is ineffective in the case of multimedia data [1] [14]. To address these issues researchers have proposed a cross layer architectures to account for the dynamics observed at the physical, MAC and routing layer for multimedia data [3] [12] [13] [14]. Combining cross layer optimization and SVC encoding for multimedia data delivery has been considered in [11], [15] and the results obtained prove the efficiency and assure QoS provisioning.

The existing models fail to address the tradeoff relation that exist between the QoS of the SVC encoded data transmission and end to delay i.e. if the QoS to be provisioned is high the end to end delays are high proved in [14]. To address this issue this paper introduces the QoS improvement scheme in video transmission ($QIVST$) model adopting a cross layer optimization approach. The $QIVST$ model considers the SVC encoded video streams for transmissions. Based on the physical layer conditions of the wireless network, the quality adaptation specifier (S_{s1}) and the physical layer knowledge specifier$(S_{s2})$are identified. A novel encoding scheme of the SVC video utilizing the S_{s1}andS_{s2} is considered at the MAC layer. The packets constructed at the MAC layer are routed through the next hop node based on the S_{s1}, S_{s2} and pending packets in that node. A similar approach is adopted at every intermediate hop node. The $QIVST$ model proposed is designed to address the tradeoff between QoS provisioning and delivery of the delay bound multimedia data. The cross layer optimization adopted in the $QIVST$ model provides adaptability to achieve better QoS in wireless networks and ensures the essential delay bound multimedia data delivery.

The remaining manuscript is organized as follows. A brief of the literature review discussing the state of the art mechanisms that currently exist is discussed in section 2. The proposed $QIVST$ model is presented in Section 3 of this paper. The simulation study with performance comparisons is discussed in the penultimate section of this paper. The conclusions and future work is discussed in the Section 5.

II. Literature Review

Numerous work considering multimedia data delivery on wireless networks has been proposed by researchers. A brief of the literature studied during the course of the research presented here is discussed in this section.

An ant colony optimization algorithm to support video streaming services on wireless mobile networks is proposed in [3]. A dual layer architecture constituting of the mini-community network layer and the community member layer is considered in [3]. The mini-community layer enables robust video data delivery and access methodologies. The resource and member management is achieved by the community member layer. The results presented prove the efficiency of the biologically inspired ant colony optimization.

A cross layer optimization technique to support video transmissions on wireless networks has been proposed by Yuanzhang Xiao et al [12]. The importance of resource allocation to support video transmissions is discussed. The cross layer architecture proposed by Yuanzhang Xiao et al enables dynamic scheduling and resource allocations among the wireless user nodes based on the physical channel conditions and the dynamics of video transmissions.

The cross layer fairness driven stream control transmission protocol based concurrent multipath transfer solution $(CMT-CL/FD)$ is proposed in [13]. The efficiency of utilizing multipaths for video content delivery is highlighted. Optimizations were adopted at the physical, data link and transport layer in the $CMT-CL/FD$ to support video applications on heterogeneous wireless networks. In $CMT-CL/FD$ the cross layer optimization is adopted only at the transmitter.

Hypertext Transfer Protocol $(HTTP)$ based Dynamic Adaptive Streaming $(DASH)$ of SVC video in wireless networks is discussed in [11]. A cross layer optimization based on the Lagrangian method is adopted in $DASH$ to support streaming of SVC video. A novel resource allocation and packet scheduling algorithm is considered in $DASH$. Th e tradeoff that exists between data delivery and QoS of video transmissions is discussed. The tradeoff issue is addressed by Mincheng Zhao et al through a proxy based bitrate stabilization algorithm introduced in $DASH$.

Transmission of SVC video data in multi input multi output $(MIMO)$ wireless systems is proposed by Xiang Chen et al [15]. A cross layer approach adopting optimizations based on the physical and application layer is proposed by Xiang Chen et al. To reduce transmission errors and reduce the number of retransmissions FEC mechanisms are also employed by the authors in [15]. An adaptive channel power allocation scheme is used in [15] to improve the QoS of video transmissions. The work proposed by Xiang Chen et al bears the closest similarity to the work proposed here and is further used for performance comparisons with our proposed $QIVST$ model. The major drawback of the cross layer approach proposed in [15] is that the tradeoff that exists between QoS provisioning and video data delivery is not addressed.

III. QoS Improvement Scheme in Video Transmission $QISVT$

a) *Wireless Network Modelling*

Let us consider a wireless network $\mathcal{N}$ deployed over an area of $\mathcal{A}$ sq.meters. The network N consists of a set of I nodes sharing the multimedia content D with J receiver nodes. The channel matrix of the b^{th} node is represented as $C[b]$ where $b \in I \parallel J$. The wireless channel Bandwidth considered is R_c and the channel error rate is represented by R_e. The channel noise is represented as N . The SVC video data [1] is considered as the multimedia content. Video transmissions are bulky and require efficient transmission mechanisms to meet the desired QoS. In the $QISVT$ model introduced in this paper the video content is initially encoded using the MPEG video coder. The $MPEG$ video coder considered adopts the Group of Pictures (GOP) structure described in [2] [14]. The GOP structure is shown in Fig.1. of this paper.

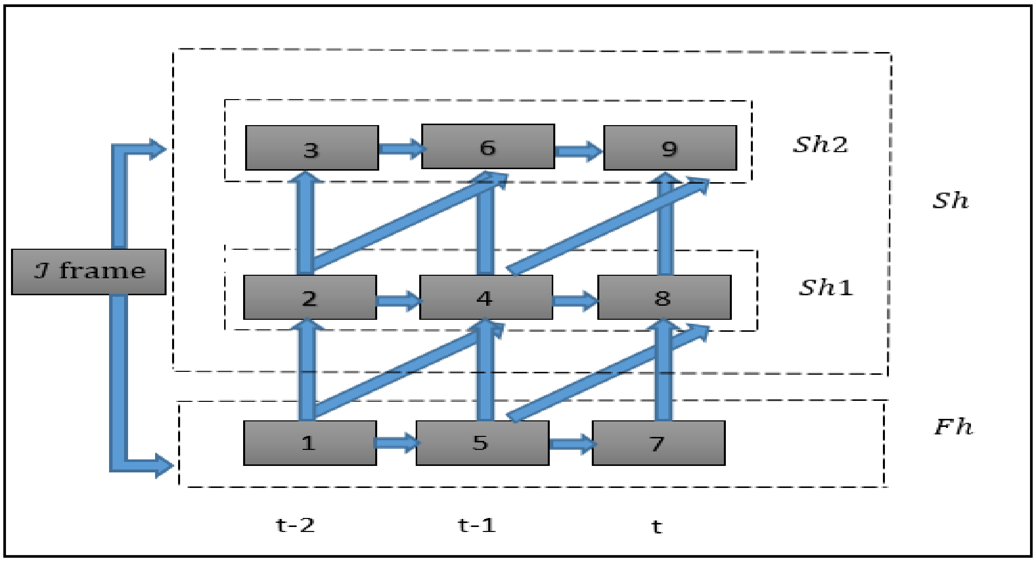


Figure 1 : Packet loss compensation by error correction in video transmission using QISVT scheme

The encoded frames are indexed by $g = 1,2,3 \dots \dots$. In the $QISVT$ model introduced the initial frame/reference frame $\mathcal{J}$ is transmitted first. The base layer B frame is donated as Fh and the enhancement/quality layer P frame is represented as Sh. In the existing mechanisms discussed earlier a loss of the FH and SH frame results in a retransmission enhancing end to end delays and reducing the wireless transmission QoS. To improve the QoS in multimedia content delivery over the network $\mathcal{N}$ the $QISVT$ model introduces a novel cross layer adaption technique[3]. By acquiring the prevailing physical layer properties of the node, the MAC layer packetization techniques and the routing to the neighboring nodes are accordingly adapted to achieve a cross layer design discussed in the proceeding sub-section of the paper.

b) Cross-Layer Design Of The $QISVT$ model

A discrete time based model to describe the cross layer architecture of the $QISVT$ model is considered. Let us consider a node $i \in I$ transmitting content D to its neighbor $j \in J$. At time $t-2$ the I frame is transmitted. The X_{t-1} frame consisting of $X_{t-1}^{F_h}$ and $X_{t-1}^{S_h}$ is transmitted at the $(t-1)^{th}$ time instance. In the $QISVT$ model the Sh frame is assumed to consist of two sub-frames namely $Sh1$ and $Sh2$ i.e. $Sh = Sh1 + Sh2$. The sub frame construction is considered to encode the previous Fh frame into the $Sh1$ and transmit it wirelessly to the node j at time t . The adoption of the sub-framing technique enables reconstruction of the Fh in case of transmission errors. The encoded frame ${X_1}_t^{S_h,e}$ is defined as

$$ {X_1}_t^{S_h,e} = \left((1-S_{s1})X_{t-1}^{F_h}\right) + \left(S_{s1} \times X_{t-1}^{S_h}\right) \quad (1) $$

Where S_{s1} is the Quality layer adaptation specifier introduced in the $QISVT$ model. Based on the physical layer parameters, the node bandwidth supported, the pending packets in the MAC queue and channel noise thevalue of S_{s1} is established on runtime. The quality adaptation specifier is constrained by the set $S_{s1} \in \{0,0.1,0.2 \dots 1\}$. The S_{s1} specifier enables in controlling the quality of the video transmission between the nodes i and j . Considering $S_{s1} = 1$ the best QoS can be achieved. When $S_{s1} = 0$ only the Fh is transmitted resulting in lower quality.

To account for the physical layer conditions in the MAC encoder the Physical Layer Knowledge Specifier S_{s2} parameter is introduced and is defined as

$$ S_{s2} = Val : Val = \{0, \dots 1\} \quad (2) $$

By introducing the S_{s2} parameter the composition of the $Sh1$ and $Sh2$ sub frames is achieved accounting for the physical layer parameters. If $S_{s2} = 0$ then $Sh1 = Fh$ and $Sh2 = \emptyset$ i.e. the physical layer exhibits high distortion and the transmission of the Fh layer is only considered. If $S_{s2} = 1$ then $Sh1 = Sh$ and $Sh2 = \emptyset$ is considered as an ideal condition when the physical channel exhibits no signal distortion hence the entire Sh layer is considered for transmission. The S_{s2} and S_{s1} parameters are derived based on the physical layer measurements carried out at Δt intervals. The channel noise, packet delay and the error rate observed in transmitting the frame $\mathcal{J}$ enables in initialization. The proposed MAC layer encoding can be now defined as

$$ {X_1}_t^{S_h,e,S_{s2}} = \left((1-S_{s1})X_{t-1}^{F_h}\right) + \left(S_{s1} \times X_{t-1.}^{S_h,S_{s2}}\right) \quad (3) $$

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

Where $X_{1_t}^{S_h,e,S_{s2}}$ represents the MAC encoded data derived from the previous $X_{t-1}^{F_h}$ and $X_{t-1}^{S_h,S_{s2}}$ frame to be transmitted.

The MAC encoding is presented in Fig.2. of this paper.

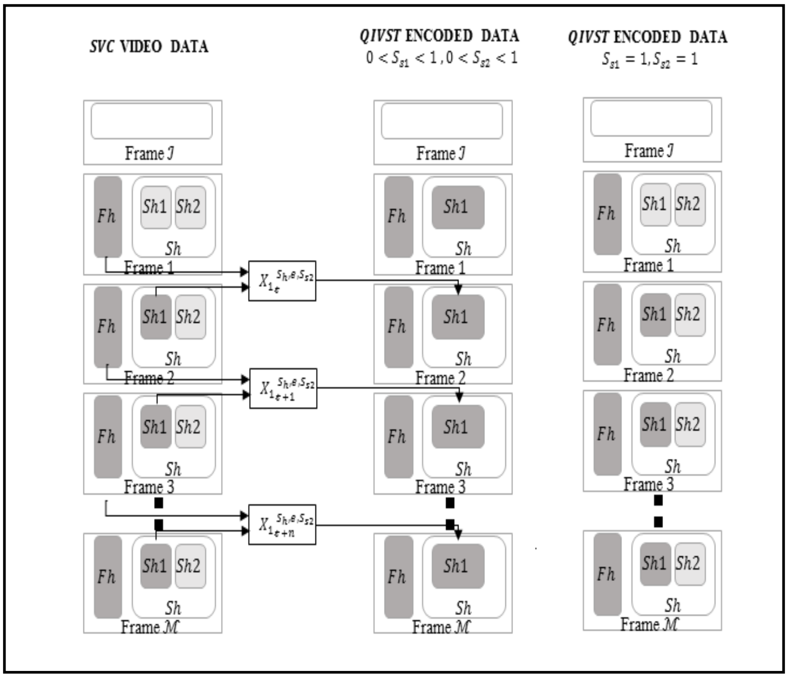


Figure 2 : Adaptive MAC encoding based on the QISVT model

Based on the MAC queues pending, S_{s1} and the S_{s2} parameter the routing layer is optimized to select the next hop neighbor node to achieve QoS.

The $QISVT$ model can be summarized as follows:

Step 1: Initialize Encoded Multimedia Data D

Step 2: Initialize Transmitting Node i and Receiving Node j

Step 2: Extract the frame $\mathcal{J}$ and transmit from Node $i \rightarrow j$

Step 3: Measure Error Rate, Delay.

Step 4: Based on the measurements initialize S_{s2} and S_{s1}

Step 5: Based on D the Fh and Sh frame Data is derived.

Step 6: Based on S_{s2} and S_{s1} derive $Sh1$ and $Sh2$ and perform MAC encoding using Equation 3.

Step 7: Based on the MAC packet Queues Pending, S_{s2} and S_{s1} perform routing optimization to select hop node.

i. *Video Distortion in the $QIVST$ model*

Transmission over wireless channels induces errors in transmission. The transmission errors result in a huge number of video packet errors and losses. On packet error or loss occurrences, packet retransmission request and response messages are propagated. This phenomena induces huge amounts of overheads and the video packet delivery time increases effecting QoS. To improve QoS the cross layer $QIVST$ model to reduce packet delivery delays is introduced in this paper. The distortion observed at the receiver is proportional to the channel noise. When the channel noise observed is large, the $QIVST$ adapts to enable successful transmissions compromising QoS as video data delivery is delay bound. Packets delivered beyond the delay bound possess no significance and are generally dropped. The $QIVST$ model proposed provides a delicate tradeoff between timely delivery of data packets and QoS .The encoding at the MAC layer $X_{1_t}^{S_h,e,S_{s2}}$ enables recovery of the Fh from the encoded enhancement layer packet in case the base layer packet is lost. The encoding enables to achieve optimal QoS in noisy environments. In this section the modelling of the packet error probabilities, video frame transmissions, frame reconstruction, frame decoding, frame errors and the distortions observed is discussed.

Let the data D to be transmitted using the $QISVT$ model form $\mathcal{M}^{total}$ encoded packets. Each packet consists of b symbols. The symbols b need to be transmitted on the wireless Radio Layer Switching mode of $T_{(b)}$ through a channel which has an allocated bandwidth based channel rate of $R_{c(b)}$.The additive white gaussian noise present in the wireless channels induces transmission errors. The error rate experienced by the symbol b is given by $R_{e(b)}\left(R_{c(b)}, T_{(b)}\right)$.

Let us assume that there are $\mathcal{M}^{total}$ number of video packets formed from the video to be transmitted.In error free enviromets the complete $\mathcal{M}^{total}$ packets when transmitted will be received, decoding which would form the data D.In practical envirometes or actual conditions transmission errors occour due to the noise present in the wireless transmission medium. If out of $\mathcal{M}^{total}$ Packets only $\mathcal{M}$ packets are transmitted successfully and remaining $(\mathcal{M}^{total} - \mathcal{M})$ packets are lost during transmission such that error occurs at the $(\mathcal{M}+1)th$ packet, the probability of such an occurrence if $\mathcal{M} = 0$ is

$$Occ(\mathcal{M}|\mathcal{M}^{total}) = R_{e(b)}(R_{c(b)}, T_{(b)}) \quad (4)$$

The probability of occurrence during the transmission being active i.e. $0 < \mathcal{M} < \mathcal{M}^{total}$ is given by

$$Occ(\mathcal{M}|\mathcal{M}^{total}) = \prod_{d=1}^{\mathcal{M}}\left(1 - R_{e(d)}(R_{c(d)}, T_{(d)})\right) \times \left(R_{e(p+1)}(R_{c(p+1)}, T_{(p+1)})\right) \quad (5)$$

Considering $\mathcal{M} = \mathcal{M}^{total}$ the error probablity occurance is defined as

$$Occ(\mathcal{M}|\mathcal{M}^{total}) = \prod_{d=1}^{\mathcal{M}^{total}}\left(1 - R_{e(d)}(R_{c(d)}, T_{(d)})\right) \quad (6)$$

Let us consider at the t^{th}time the receiver node receives $\mathcal{M}$ video packets successfully out of the $\mathcal{M}^{total}$ packets. If $A_d$represents the number of symbols in the d^{th} packet, then the cumulative video data available at the receiver i.e. R^{rx}can be computed using

$$R^{rx} = \sum_{d=1}^{\mathcal{M}}(R_{c(d)} \times A_d) \quad (7)$$

The $QIVST$ model priorities the delivery of the Fh ensuring the delay constraints are attained. If the Fh encoded packet at thet^{th}time instance i.e. $X_t^{F_h}$ is lost then its recovery is possible from the ${X_1}_{t+1}^{S_h,e,S_{s2}}$ encoded packet. Let the function $Dt(R^{rx}, S_{s1}, S_{s2})$ represent the distortion observed per frame at the receiver post decoding considering all the symbols of the Fh layer, the quality layer adaptation specifier S_{s1} , the physical layer knowledge specifier S_{s2} and $R^{rx}$is the total symbols of the Sh layer. Based on the error probabilities and the distortions of the individual frames the average distortion $Dt_{avg}[(S_{s1}, S_{s2})]$can be computed using

$$Dt_{avg}[(S_{s1}, S_{s2})] = Dt(0, S_{s1}, S_{s2})Occ(0 \mid \mathcal{M}^{total}) + \sum_{\mathcal{M}=1}^{\mathcal{M}^{total}}\{Dt(R^{rx}, S_{s1}, S_{s2})Occ(\mathcal{M} \mid \mathcal{M}^{total})\} \quad (8)$$

where $Dt(0, S_{s1}, S_{s2})$ represents the distortion observed with respect to the reference frame$\mathfrak{I}$.

The parameter S_{s2} controls the composition of the Sh data. In the case when channel noise is present and the channel bandwidth cannot support the transmission of the entire Sh layer i.e. $0 < S_{s1} < 1$ and$0 < S_{s2} < 1$, a part of theSh_2 is not considered for encoding and transmission and is defined as

$$V_t^{S_h} = X_t - (X_t^{F_h} - X_{t-1}^{F_h}) - {X_1}_t^{S_h,e,S_{s2}} \quad (9)$$

Where $X_t$is the original frame considered at the t^{th}time instance.

To achieve optimum QoS the Fh layer is transmitted and the $Sh1$ is encoded at the MAC layer and transmitted. Let$V_t^{S_h1}$ represent the MAC encoded data of $Sh1$ and $V_t^{S_h2}$denote the decoded $Sh1$ data at the receiver. In the $QIVST$ model the packet loss probability of the Fh is assumed to be 0. The frame reconstructed at the decoder at the t^{th}time instance is defined as

$${X_2}_t = V_t^{S_h2} + (X_t^{F_h} - X_{t-1}^{F_h}) + {X_2}_t^{S_h,d,S_{s2}} \quad (10)$$

where ${X_2}_t^{S_h,d,S_{s2}}$represents the data at the receiver on performing the MAC layer decoding on the encoded data${X_1}_t^{S_h,e,S_{s2}}$.

The decoded version of ${X_1}_t^{S_h,e,S_{s2}}$at the receiver on the basis of the partially decoded data of the Sh data i.e. ${X_2}_{t-1.}^{S_h,S_{s2}}$is defined as

$${X_2}_t^{S_h,d,S_{s2}} = \left((1 - S_{s1})X_{t-1}^{F_h}\right) + \left(S_{s1} \times {X_2}_{t-1.}^{S_h,S_{s2}}\right) \quad (11)$$

Utilizing the above definition in Equation 10 we obtain

$${X_2}_t = V_t^{S_h2} + \left(S_{s1} \times ({X_2}_{t-1.}^{S_h,S_{s2}} - X_{t-1}^{F_h})\right) + X_t^{F_h} \quad (12)$$

where ${X_2}_{t-1.}^{S_h,S_{s2}}$ is the partially decoded data of the Sh layer at the $(t-1)^{th}$time instance and is defined as

$${X_2}_{t-1.}^{S_h,S_{s2}} = V_{t-1}^{S_h2,S_{s2}} + (X_{t-1}^{F_h} - X_{t-2}^{F_h}) + {X_2}_{t-1}^{S_h,d,S_{s2}} \quad (13)$$

The partially encoded data of the Sh layer i.e. $Sh1$ at the $(t-1)^{th}$ time instance is defined as

$$X_{t-1.}^{S_h,S_{s2}} = V_{t-1}^{S_h,S_{s2}} + \left(X_{t-1}^{F_h} - X_{t-2}^{F_h}\right) + X_{1\,t-1}^{S_h,e,S_{s2}} \quad (14)$$

To compute the transmission error the difference between the encoded video frame at the transmitter X_t and the decoded video frame at the receiver $X_{2\,t}$ is considered and is defined as

$$T_e = X_t - X_{2\,t} = V_t^{S_h} - V_t^{S_h 2} + X_{1\,t}^{S_h,e,S_{s2}} - X_{2\,t}^{S_h,d,S_{s2}} \quad (15)$$

Using Equation 8 and Equation 12 the error can be simplified as

$$T_e = V_t^{S_h} - V_t^{S_h 2} + \left(S_{s1} \times \left(X_{t-1.}^{S_h,S_{s2}} - X_{2\,t-1}^{S_h,S_{s2}}\right)\right) \quad (16)$$

Using Equations 13 and equation 14 $\left(X_{t-1.}^{S_h,S_{s2}} - X_{2\,t-1}^{S_h,S_{s2}}\right)$cab be represented as

$$\left(X_{t-1.}^{S_h,S_{s2}} - X_{2\,t-1}^{S_h,S_{s2}}\right) = V_{t-1}^{S_h,S_{s2}} - V_{t-1}^{S_h 2,S_{s2}} + \left(S_{s1} \times \left(X_{t-2}^{S_h,S_{s2}} - X_{2\,t-2}^{S_h,S_{s2}}\right)\right) \quad (17)$$

The distortion of the m^{th} frame at the receiver post decoding at the at the t^{th} time instance is computed using

$$Dt_m(\mathcal{TM}, S_{s1}, S_{s2}) = Avg[(T_e)^2] \quad (18)$$

where$\mathcal{TM}$ is the throughputs observed as the receiver post decoding considering all the frames from the reference frame $\mathcal{J}$ to the m^{th} frame

From equation 18 it can be observed that the transmission errors effect the throughput observed and also induce distortion in video reconstruction at the receiver. The $QIVST$ model adapts based on the physical layer conditions to minimize the transmission errors by adopting adaptive MAC encoding and route optimization.

IV. Experimental Study

In this section the experimental study conducted to evaluate the performance of the proposed $QIVST$ model is discussed. The experimental study was conducted using Matlab. The performance of the $QIVST$ model is compared with the state of art $Bisection\ Algorithm - A1$ proposed by Xiang Chen et al [15]. Video clips 'City' and 'Stefan' of Common Interchange Format are considered for the experimental study. The video clips 'City' and 'Stefan' are encoded by the reference SVC codec JSVM (Joint Scalable Video Model). The 'City' video consists of 300 frames and the 'Stefan' video of 90 frames. The frame rate considered for both the videos is 30 frames per second. The SVC codec considers the GOP structure.

A wireless network consisting of 15 nodes is considered. The simulation study considers 4 transmitter nodes and 4 receiver nodes. Experiments considering the 'City' and 'Stefan' video were independently conducted. The M-QAM modulation and demodulation schemes were considered in the experimental study. An additive white Gaussian wireless noise channel is considered and the signal to noise ratio 0, 10, 20 and 30 dB is considered. The video transmissions carried out are monitored and the video is reconstructed at the receiver. An average of the monitored values considering 4 transmitters and 4 receivers is presented.

In the prevision section it has been stated that the distortion observed Dt is directly proportional to the transmission errors T_e i.e. $Dt \propto T_e$. The transmission errors observed per frame is represented in terms of the bit error rates (BER) observed for the duration of the simulation. The BER observed considering the 90 frames of the "Stefan" video transmitted is shown in Figure 3, 4 and 5. From the figures it is clear that as the channel noise i.e. SNR increased the distortion increases considering the QIVST model and the $Bisection\ Algorithm - A1$. At a $SNR = 30\,dB$ (in Figure 3) it is observed that the average BER considering the $Bisection\ Algorithm - A1$ is 0.21 and for the $QIVST$ model is 0.17. When the channel noise induced in the simulation environment is $20\,dB$ (in Figure 4) and $10\,dB$ (in Figure 5) the proposed $QIVST$ model based video transmissions achieves a BER reduction of 45.7% and 36.99% when compared to the $Bisection\ Algorithm - A1$. Based on the BER results it is evident that the proposed QIVST model is adaptive and performs better than the existing the $Bisection\ Algorithm - A1$ under varying channel noise conditions. Lower $BER's$ observed tend to enhance the QoS provided to multimedia data delivery over wireless networks.

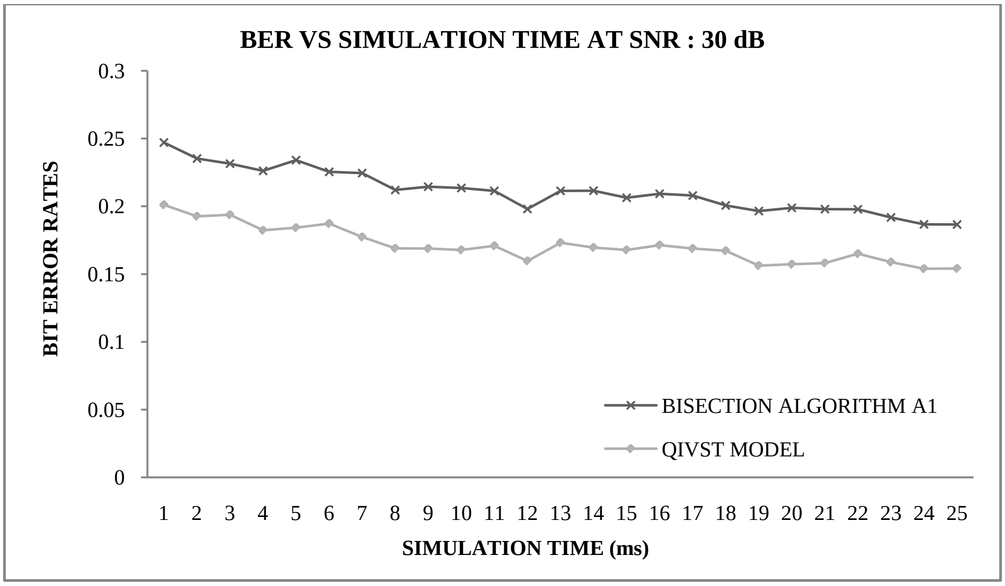


Figure 3 : Distorting Observed in terms of BER at SNR= 30dB vs Simulation Time

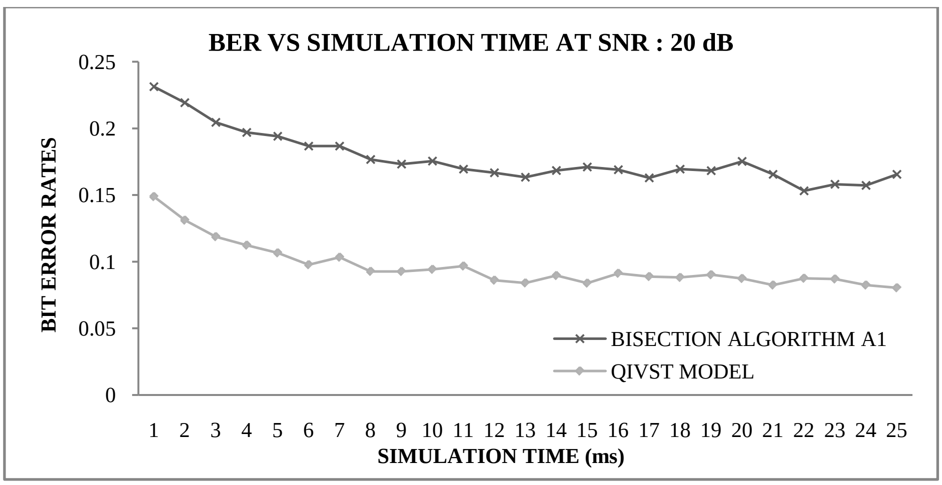


Figure 4 : Distorting Observed in terms of BER at SNR= 20dB vs Simulation Time

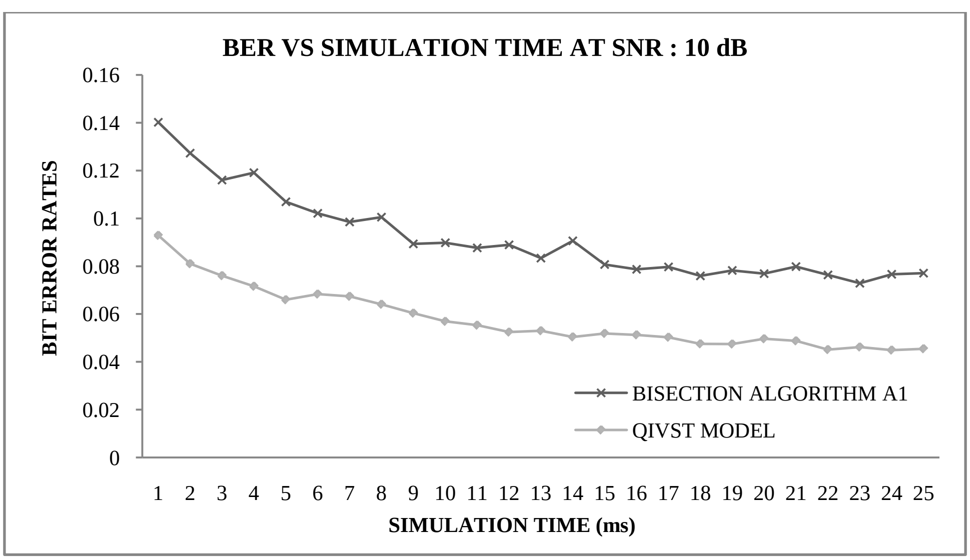


Figure 5 : Distorting Observed in terms of BER at SNR= 10dB vs Simulation Time

From equation 18 it can be observed that the transmission errors effect the throughput observed and also induce distortion in video reconstruction at the receiver. The $QIVST$ model adapts based on the physical layer conditions to minimize the transmission errors by adopting adaptive MAC encoding and route optimization.

In [15] the authors have introduced the "System utility" parameter for performance evaluation. Considering the GOP of video "Stefan" the system utility computed using the $QIVST$ model and the $Bisection\ Algorithm - A1$. The results obtained are graphically shown in Figure 6 of this paper. The system utility increases as the channel noise increases due to transmission errors. The increase in transmission errors induce an additional network overhead by introducing retransmission messages. From the figure it is evident that the proposed $QIVST$ model exhibits a higher system utility when compared to the $Bisection\ Algorithm - A1$. The adaptive encoding and the cross layer architecture of the QIVST model also contribute to the increased system utility observations.

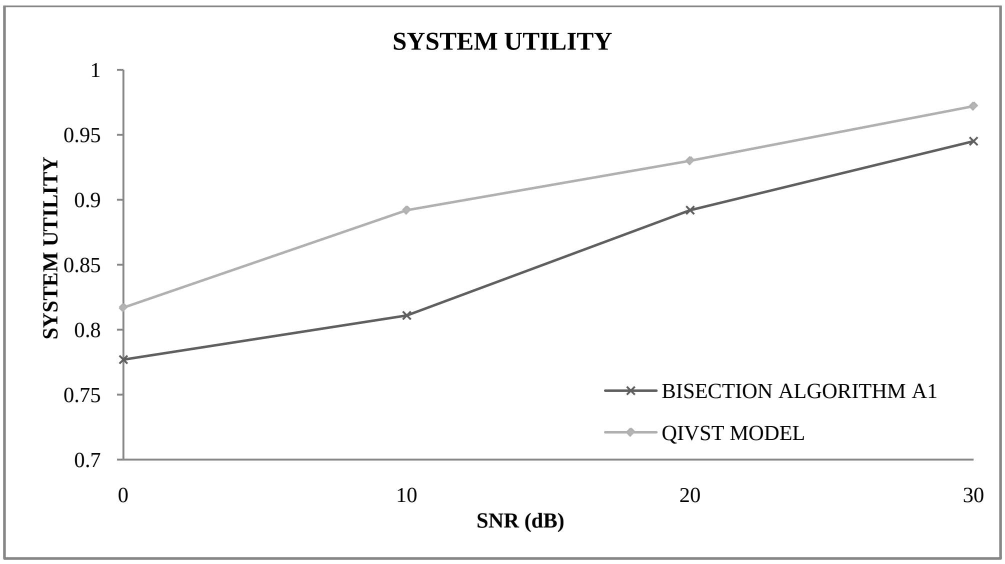
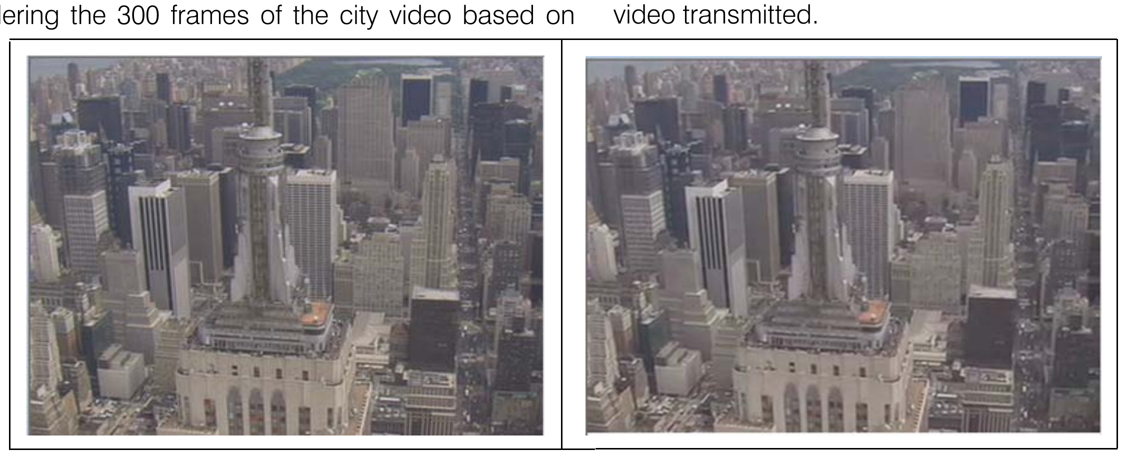


Figure 6 : System Utility

To evaluate the performance of the video delivery on the wireless network the 'City' video and the 'Stefan' video are transmitted. The reconstruction quality is observed in terms of the SNR per frame. For the City video a sample frame reconstructed at the receiver is shown in Figure 7 a considering the $QIVST$ model and Figure 7 b considering the $Bisection\ Algorithm - A1$. The reconstruction quality observed at the receiver considering the 300 frames of the city video based on the proposed QIVST model is shown in Figure 8. The reconstruction quality considering the $Bisection\ Algorithm - A1$ is shown in Figure 9. The reconstruction quality is computed per frame reconstructed at the receiver and is expressed in terms of the $PSNR$ observed. From Figure 8 and 9 it is evident that the $QIVST$ model outperforms the $Bisection\ Algorithm - A1$ in terms of the quality of video transmitted.



a b

Figure 7 : A sample reconstructed frame at the receiver for the "City" video considering the a. QIVST model proposed and b. Bisection Algorithm – A1

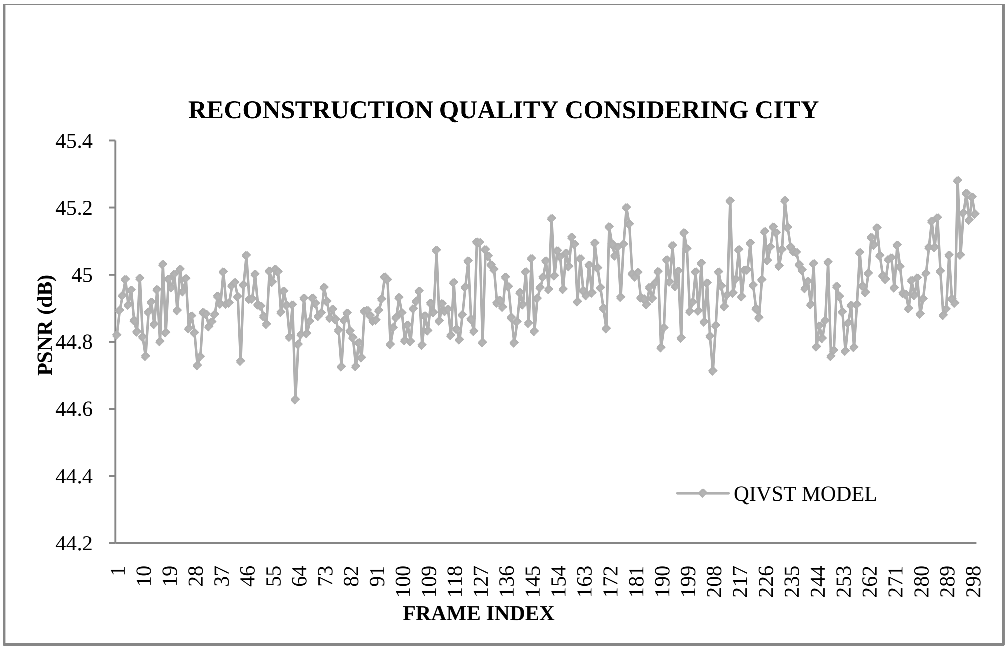


Figure 8 : Reconstruction quality per frame in terms of PSNR for the City video based on the QIVST model

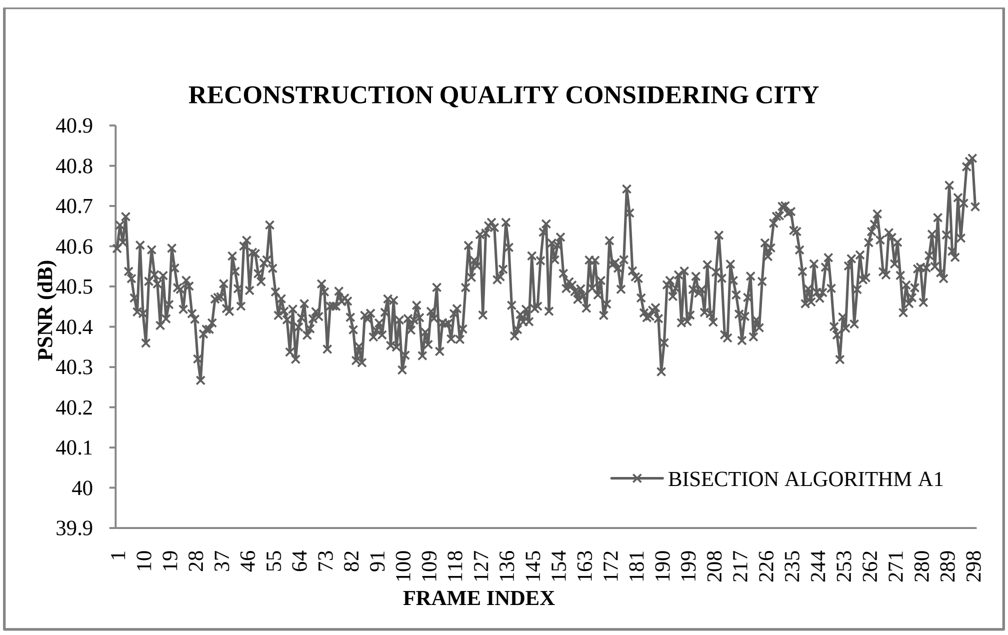
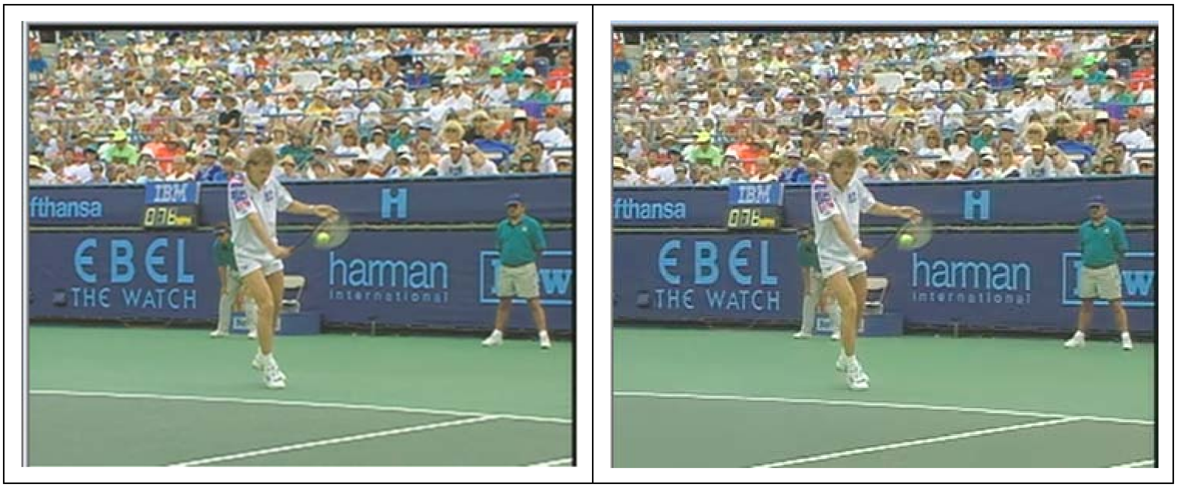


Figure 9 : Reconstruction quality per frame in terms of PSNR for the City video based on the $\text{Bisection Algorithm} - \text{A1}$

Considering the "Stefan" video a sample frame reconstructed using the $QIVST$ model and the $BisectionAlgorithm - A1$ is shown in figure 10 of this paper. The per frame $PSNR$ computed depicting the quality of reconstruction is shown in Figure 11 and 12. From the reconstruction results considering the "Stefan" video shown in this paper it is clear that the $QIVST$ model provides better quality in video delivery over wireless networks when compared to the $Bisection\ Algorithm - A1$.



b b

Figure 10 : A sample reconstructed frame at the receiver for the "Stefan" video considering the **a.** QIVST model proposed and **b.** Bisection Algorithm – A1

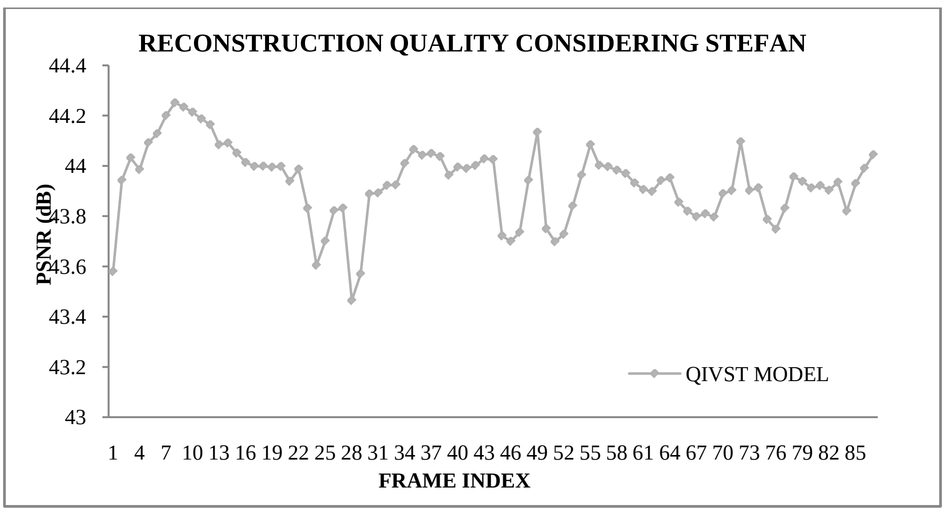


Figure 11 : Reconstruction quality per frame in terms of PSNR for the Stefan video based on the QIVST model

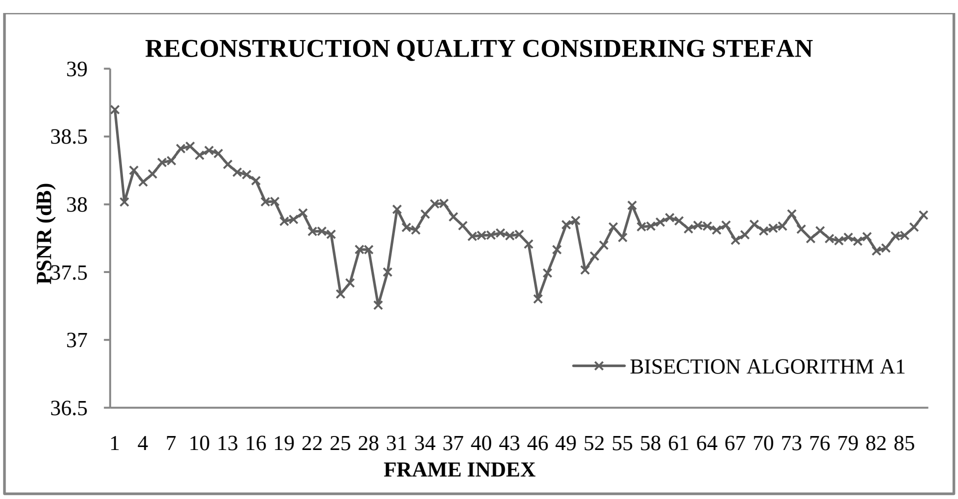


Figure 12 : Reconstruction quality per frame in terms of PSNR for the Stefan video based on the Bisection Algorithm – A1

The experimental study presented in this paper prove that the cross layer design based $QIVST$ model proposed is robust and adaptable proved in terms of lower $BER's$ observed. The $QIVST$ model induces an additional overhead due to the novel encoding scheme (proved by higher system utility observations) and improves the quality of video transmissions in wireless networks. The results also prove the proposed model superiority when compared to the state of art video delivery algorithm the $Bisection\ Algorithm - A1$.

V. Conclusion

High bandwidth requirements, delay sensitive nature and QoS measures of multimedia data delivery on wireless networks put forth numerous challenges. The use of SVC encoded streams on cross layer architectures have been proposed by researchers. The existing mechanisms fail to address the tradeoff between QoS and data delivery delays that exists. In this paper the QIVST model is introduced that adopts a cross layer design. The SVC video data considered in the QIVST model is further encoded at the MAC layer based on the physical layer conditions and the QoS achievable, to address the tradeoff issue highlighted. The distortion observed based on the QIVST model is presented. Based on the pending packet queues observed optimization of the routing layer is considered in the QIVST to minimize the end to end delay. The extensive results presented in the experimental study considering SVC video traces prove the robustness and efficiency of the proposed QIVST model when compared to the state of art existing system.

References Références Referencias

1. Jenq-Neng Hwang, Multimedia Networking: from Theory to Practice , Cambridge University Press, 2009
2. Baiocchi, Andrea; Cuomo, Francesca, "Infotainment services based on push-mode dissemination in an integrated VANET and 3G architecture," Communications and Networks, Journal of , vol.15, no.2, pp.179,190, April 2013
3. Changqiao Xu; ShijieJia; LujieZhong; Hongke Zhang; Muntean, G.-M., "Ant-Inspired Mini-Community-Based Solution for Video-On-Demand Services in Wireless Mobile Networks," Broadcasting, IEEE Transactions on , vol.60, no.2, pp.322,335, June 2014
4. Daewon Song and Chang Wen Chen. 2008. Maximum-throughput delivery of SVC-based video over MIMO systems with time-varying channel capacity. J. Vis. Comun. Image Represent. 19, 8 (December 2008), 520-528.
5. WassimHamidouche, Clency Perrine, YannisPousset, Christian Olivier, A solution to efficient power allocation for H.264/SVC video transmission over a realistic MIMO channel using precoder designs, Journal of Visual Communication and Image Representation, Volume 22, Issue 6, August 2011, Pp 563-574.
6. GK Srinivasa Gowda, CV Srikrishna& Kashyap D Dhruve,"Wireless Measurement Scheme for Bandwidth Estimation in Multihop Wireless AdhocNetwork",Global Journal of Computer Science and Technology, vol.13, no.5, pp 1-11, April 2013
7. "ISO/IEC 14492-2 (MPEG-4 Visual)", Coding of audio-visual objects—Part 2: Visual,
8. "ITU-T Rec. H.264 and ISO/IEC 14496-10 (MPEG-4 AVC)", Advanced Video Coding for Generic Audiovisual Services,
9. Wang, C.-Y.; Chen, Y.; Wei, H.-Y.; Liu, K.J.R., "Scalable Video Multicasting: A Stochastic Game Approach with Optimal Pricing," Wireless Communications, IEEE Transactions on , vol.PP, no.99, pp.1,1
10. Schwarz, H.; Marpe, D.; Wiegand, T., "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," Circuits and Systems for Video Technology, IEEE Transactions on , vol.17, no.9, pp.1103,1120, Sept. 2007
11. Zhao, M.; Gong, X.; Liang, J.; Wang, W.; Que, X.; Cheng, S., "QoE-Driven Cross-Layer Optimization for Wireless Dynamic Adaptive Streaming of Scalable Videos Over HTTP," Circuits and Systems for Video Technology, IEEE Transactions on , vol.25, no.3, pp.451,465, March 2015
12. Yuanzhang Xiao; van der Schaar, M., "Optimal Foresighted Multi-User Wireless Video," Selected Topics in Signal Processing, IEEE Journal of , vol.9, no.1, pp.89,101, Feb. 2015
13. Xu, C.; Li, Z.; Li, J.; Zhang, H.; Muntean, G., "Cross-layer Fairness-driven Concurrent Multipath Video Delivery over Heterogenous Wireless Networks," Circuits and Systems for Video Technology, IEEE Transactions on , vol.PP, no.99, pp.1,1
14. Kwanghyun Lee; Sungjin Lee; Sanghoon Lee, "Optimization of Delay-Constrained Video Transmission for Ad Hoc Surveillance," Vehicular Technology, IEEE Transactions on , vol.63, no.4, pp.1855,1869, May 2014
15. Xiang Chen; Jenq-Neng Hwang; Chung-Nan Lee; Shih-I Chen, "A Near Optimal QoE-Driven Power Allocation Scheme for Scalable Video Transmissions Over MIMO Systems," Selected Topics in Signal Processing, IEEE Journal of , vol.9, no.1, pp.76,88, Feb. 2015

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Encryption Algorithm AES-RFWKIDEA32-1 based on Network RFWKIDEA32-1

By Gulom Tuychiev
National University of Uzbekistan, Uzbekistan

Abstract- In this article we developed a new block encryption algorithm based on network RFWKIDEA32-1 using of the transformations of the encryption algorithm AES, which is called AES-RFWKIDEA32-1. The block's length of this encryption algorithm is 256 bits, the number of rounds are 10, 12 and 14. The advantages of the encryption algorithms are that, when encryption and decryption process used the same algorithm. In addition, the encryption algorithm AES-RFWKIDEA32-1 encrypts faster than AES.

Keywords: advanced encryption standard, feystel network, lai-massey scheme, round function, round keys, output transformation, multiplica- tion, addition, multiplicative inverse, additive inverse.

GJCST-E Classification : C.2.1

The Encryption Algorithm AES-RFWKIDEA32-1 based on Network RFWKIDEA32-1

Gulom Tuychiev

Abstract- In this article we developed a new block encryption algorithm based on network RFWKIDEA32-1 using of the transformations of the encryption algorithm AES, which is called AES-RFWKIDEA32-1. The block's length of this encryption algorithm is 256 bits, the number of rounds are 10, 12 and 14. The advantages of the encryption algorithms are that, when encryption and decryption process used the same algorithm. In addition, the encryption algorithm AES-RFWKIDEA32-1 encrypts faster than AES.

Keywords: advanced encryption standard, feystel network, lai-massey scheme, round function, round keys, output transformation, multiplica- tion, addition, multiplicative inverse, additive inverse.

I. Introduction

In September 1997 the National Institute of Standards and Technology issued a public call for proposals for a new block cipher to succeed the Data Encryption Standard [41]. Out of 15 submitted algorithms the Rijndael cipher by Daemen and Rijmen [13] was chosen to become the new Advanced Encryption Standard in November 2001 [28]. The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three diferent key lengths: 128 bits, 192 bits, and 256 bits. Encrypting a 128-bit block means transforming it in n rounds into a 128-bit output block. The number of rounds n depends on the key length: n =10 for 128-bit keys, n =12 for 192-bit keys, and n=14 for 256-bit keys. The 16-byte input block (t_0, t_1, . . . , t_{15}) which is transformed during encryption is usually written as a 4x4 byte matrix, the called AES State.

t_0	t_4	t_8	t_{12}
t_1	t_5	t_9	t_{13}
t_2	t_6	t_{10}	t_{14}
t_3	t_7	t_{11}	t_{15}

The structure of each round of AES can be reduced to four basic transfor-mations occurring to the elements of the State. Each round consists in applying

a) *Lecture Notes in Computer Science: Authors' Instructions*

successively to the State the SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations. The first round does the same with an extra AddRoundKey() at the beginning whereas the last round excludes the Mix-Columns() transformation.

The SubBytes() transformation is a nonlinear byte substitution that operates independently on each byte of the State using a substitution table (S-box). Figure 1 illustrates the SubBytes() transformation on the State.

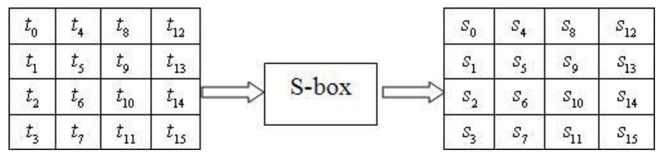


Figure 1: SubBytes() transformation

In the ShiftRows() transformation operates on the rows of the State; it cyclically shifts the bytes in each row by a certain o_set. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by o_sets of two and three respectively. Figure 2 illustrates the ShiftRows() transformation.

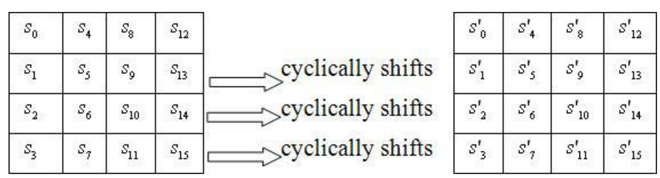


Figure 2 : ShiftRows() transformation

The MixColumns() transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x^4 +1 with a fixed polynomial a(x), given by a(x) = $3x^2 + x^2 + x + 2$. Let p = a(x) $\otimes s'$:

$$\begin{bmatrix} p_{4i} \\ p_{4i+1} \\ p_{4i+2} \\ p_{4i+3} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} s'_{4i} \\ s'_{4i+1} \\ s'_{4i+2} \\ s'_{4i+3} \end{bmatrix}, \ i = \overline{0...3}$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

Figure 3 . illustrates the MixColumns() transformation

$$y_{4i} = (\{02\} \bullet s'_{4i}) \oplus (\{03\} \bullet s'_{4i+1}) \oplus s'_{4i+2} \oplus s'_{4i+3}$$

$$y_{4i+1} = s'_{4i} \oplus (\{02\} \bullet s'_{4i+1}) \oplus (\{03\} \bullet s'_{4i+2}) \oplus s'_{4i+3}$$

$$y_{4i+2} = s'_{4i} \oplus s'_{4i+1} \oplus (\{02\} \bullet s'_{4i+2}) \oplus (\{03\} \bullet s'_{4i+3})$$

$$y_{4i+4} = (\{03\} \bullet s'_{4i}) \oplus s'_{4i+1} \oplus s'_{4i+2} \oplus (\{02\} \bullet s'_{4i+3}).$$

Author: National University of Uzbekistan, Republic of Uzbekistan, Tashkent. e-mail: blasterjon@gmail.com

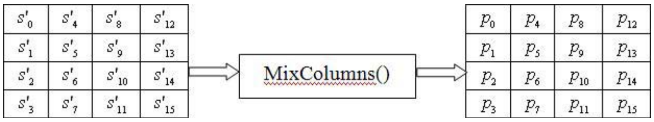


Figure 3 : MixColumns() transformation

II. Analysis of AES, PES and Idea

The first attack is a SQUARE attack suggested in [15] which uses $2^{128} - 2^{119}$ chosen plaintexts and 2120 encryptions. The second attack is a meet-in-the- middle attack proposed in [16] that requires 2^{32} chosen plaintexts and has a time complexity equivalent to almost 2^{128} encryptions. Recently, another at- tack on 7-round AES-128 was presented in [1]. The new attack is an impossible differential attack that requires $2^{117:5}$ chosen plaintexts and has a running time of 2^{121} encryptions. Similar results, but with better attack algorithms and lower complexities were reported in [42]. The resulting impossible diferential attack on 7-round AES-192 has a data complexity of 292 chosen plaintexts and time complexity of 2^{162} encryptions, while the attack on AES-256 uses $2^{116:5}$ chosen plaintexts and running time of $2^{247:5}$ encryptions.

There are several attacks on AES-192 [1, 14, 15, 24, 29, 42]. The two most no-table ones are the SQUARE attack on 8-round AES-192 presented in [15] that requires almost the entire code book and has a running time of 2^{188} encryptions and the meet in the middle attack on 7-round AES-192 in [14] that requires 2^{34+n} chosen plaintexts and has a running time of 2^{208}-^{n} + 2^{82+n} encryptions. Legitimate values for n in the meet in the middle attack on AES-192 are 94 i n i 17, thus, the minimal data complexity is 2^{51} chosen plaintexts (with time complexity equivalent to exhaustive search), and the minimal time complexity is 2^{146} (with data complexity of 2^{97} chosen plaintexts). AES-256 is analyzed in [1,14, 15, 24, 42]. The best attack is the meet in the middle attack in [14] which uses 2^{32} chosen plaintexts and has a total running time of 2^{209} encryptions. Finally, we would like to note the existence of many related-key attacks on AES-192 and AES-256. As the main issue of this paper is not related-key attacks, and as we deal with the single key model, we do not elaborate on the matter here, but the reader is referred to [43] for the latest results on related-key impossible di_er-ential attacks on AES and to [20] for the latest results on related-key rectangle attacks on AES.

The strength of AES with respect to impossible di_erentials was challenged several times. The first attack of this kind is a 5-round attack presented in [4]. This attack is improved in [11] to a 6-round attack. In [29], an impossible diferential attack on 7-round AES-192 and AES-256 is presented. The latter attack uses 2^{92} chosen plaintexts (or $2^{92:5}$ chosen plaintexts for AES-256) and has a running time of 2186 encryptions (or $2^{250:5}$ encryptions for AES-256). The tim 4 Lecture Notes in Computer Science: Authors' Instructions for AES-192. In [1] a new 7-round impossible diferential attack was presented. The new attack uses a diferent impossible diferential, which is of the same general type as the one used in previous attacks (but has a slightly diferent structure). Using the new impossible diferential leads to an attack that requires $2^{117:5}$ chosen plaintexts and has a running time of 2^{121} encryptions. This attack was later improved in [2, 42] to use $2^{115:5}$ chosen plaintexts with time complexity of 2^{119} encryptions.

The last application of impossible diferential cryptanalysis to AES was the extension of the 7-round attack from [1] to 8-round AES-256 in [42]. The ex-tended attack has a data complexity of 2116:5 chosen plaintexts and time com-plexity of $2^{247:5}$ encryption. We note that there were three more claimed impossible diferential attacks on AES in [8{10]. However, as all these attacks are awed [7]. In paper [25] present a new attack on 7-round AES-128, a new attack on 7-round AES-192, and two attacks on 8-round AES-256. The attacks are based on the attacks proposed in [1, 29] but use additional techniques, including the early abort technique and key schedule considerations.

The best attack we present on 8-round AES-256 requires $2^{89:1}$ chosen plain-texts and has a time complexity of $2^{129:7}$ memory accesses. These results are significantly better than any previously published impossible diferential attack on AES. We summarize results along with previously known results in Table 1.

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

Table 1: A Summary of the Attacks on AES

Number of rounds	complexity		Attack type
	Data (CP)	Time	
AES-128			
7	2^{128} - 2^{119}	2^{120}	Square [15]
7	$2^{117.5}$	2^{121}	Impossible Differential [15]
7	$2^{117.5}$	2^{119}	Impossible Differential [2, 42]
7	2^{32}	2^{128}	Meet in the middle [16]
7	$2^{112.2}$	$2^{117.2}$ MA	Impossible Differential [25]
AES-192			
7	2^{32}	2^{184}	Square [24]
7	$19{*}2^{32}$	2^{155}	Square [15]
7	2^{92}	$2^{186.2}$	Impossible Differential [29]
7	$2^{115.5}$	2^{119}	Impossible Differential [42]
7	2^{92}	2^{162}	Impossible Differential [42]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [14]
8	$2128 - 2119$	2^{188}	Square [15]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [25]
7	$2^{91.2}$	$2^{139.2}$	Impossible Differential [25]
AES-256			
7	2^{32}	2^{200}	Square [24]
7	$21{*}2^{32}$	2^{172}	Square [15]
7	$2^{92.5}$	$2^{250.5}$	Impossible Differential [29]
7	2^{32}	2^{208}	Meet in the middle [14]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [14]
7	$2^{115.5}$	2^{119}	Impossible Differential [42]
8	$2^{116.5}$	$2^{247.5}$	Impossible Differential [42]
8	$2^{128} - 2119$	2^{204}	Square [15]
8	2^{32}	2^{209}	Meet in the middle [14]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [25]
7	2^{92}	2^{163} MA	Impossible Differential [25]
8	$2^{111.1}$	$2^{227.8}$ MA	Impossible Differential [25]
8	$2^{89.1}$	$2^{229.7}$ MA	Impossible Differential [25]

The Proposed Encryption Standard (PES) is a 64-bit block cipher, using a 128-bit key, designed by Lai and Massey in 1990 (see [22]) and was a predecessor to IDEA (International Data Encryption Algorithm) [21]. IDEA was originally called IPES (Improved PES). PES iterates eight rounds plus an output trans- formation. The cryptanalysis of PES and IDEA presented on Table 2 and Table 3.

Table 2: A Summary of the Attacks on IDEA

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [26]	1993	2	32	210	242
Differential [12]	1993	2.5	32	210	232
Differential [26]	1993	2.5	96	210	2106
Related-Key Differential [18]	1996	3	32	6	6 * 232
Differential-Linear [6]	1996	3	32	230	244
Differential [5]	1996	3	32	230	0.75 * 244
Truncated Differential [19, 6]	1997	3.5	48	256	267
Miss-in-the-middle [3]	1998	3.5	64	238.5	253
Miss-in-the-middle [3]	1998	4	69	237	270

Related-Key Differential-Linear [17]	1998	4	15	38.3	-
Miss-in-the-Middle [3]	1998	4.5	80	264	2112
Square attack [27]	2000	2.5	77	3 * 216	262 + 247
Square attack [27]	2000	2.5	31	232	262
Square [27]	2000	2.5	31	248	279
Related-Key Square [27]	2001	2.5	32	2	241

Table 3 : A Summary of the Attacks on PES

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [23]	1991	7	96	264	2160
Square [27]	2000	2.5	31	217	247
Square [27]	2001	2.5	31	232	263
Related-Key Square [27]	2001	2.5	32	2	241

On the basis of encryption algorithm IDEAnd scheme Lai-Massey developed the networks IDEA32-1 and RFWKIDEA32-1, consisting from one round function [30, 31]. In the networks IDEA32-1 and RFWKIDEA32-1, similarly as in the Feistel network, when it encryption and decryption using the same algorithm. In the networks used one round function having 16 input and output blocks and as the round function can use any transformation.

Using transformation SubBytes(), ShiftRows(), MixColumns(), AddRound-Key() AES encryption algorithm as a round function networks IDEA8-1 [32], RFWKIDEA8-1 [32], PES8-1 [33], RFWKPES8-1 [34], IDEA16-1 [35], created encryption algorithms AES-IDEA8-1 [36], AES-RFWKIDEA8-1 [37], AES-PES8-1 [38], AES-RFWKPES8-1 [39], AES-IDEA16-1 [40].

In this paper developed block encryption algorithm AES-RFWKIDEA32-1 based network RFWKIDEA32-1 using transformation of the encryption algorithm AES. The length of block of the encryption algorithms is 256 bits, the number of rounds n equal to 10, 12, 14 and the length of key is variable from 256 bits to 1024 bits in steps 128 bits, i.e., key length is equal to 256, 384, 512,640, 768, 896 and 1024 bits.

III. The Encryption Algorithm AES-RFWKIDEA32-1

a) The structure of the encryption algorithm AES-RFWKIDEA32- 1

In the encryption algorithm AES-RFWKIDEA32-1 as the round function used SubBytes(), ShiftRows(), MixColumns() transformation encryption algorithm AES. The scheme n-rounded encryption algorithm AES-RFWKIDEA32-1 shown in Figure 4, and the length of subblocks X^0, X^1, ..., X^{31}, length of round keys $K_{32(i-1)}$, $K_{32(i-1)+1}$, ..., $K_{32(i-1)+31}$,, i = 1…n + 1 and K_{32n+32}, K_{32n+33}, ..., K_{32n+95} are equal to 8-bits.

Consider the round function of the encryption algorithm AES-RFWKIDEA32-1. Initially 32-bit subblocks t_0, t_1, . . . , t_{15} are written into the State array and are executed the above transformations SubBytes(), ShiftRows(), MixColumns(). After the AddRoundKey() transformation we obtain 8-bits subblocks y_0, y_1, ..., y_{15}.

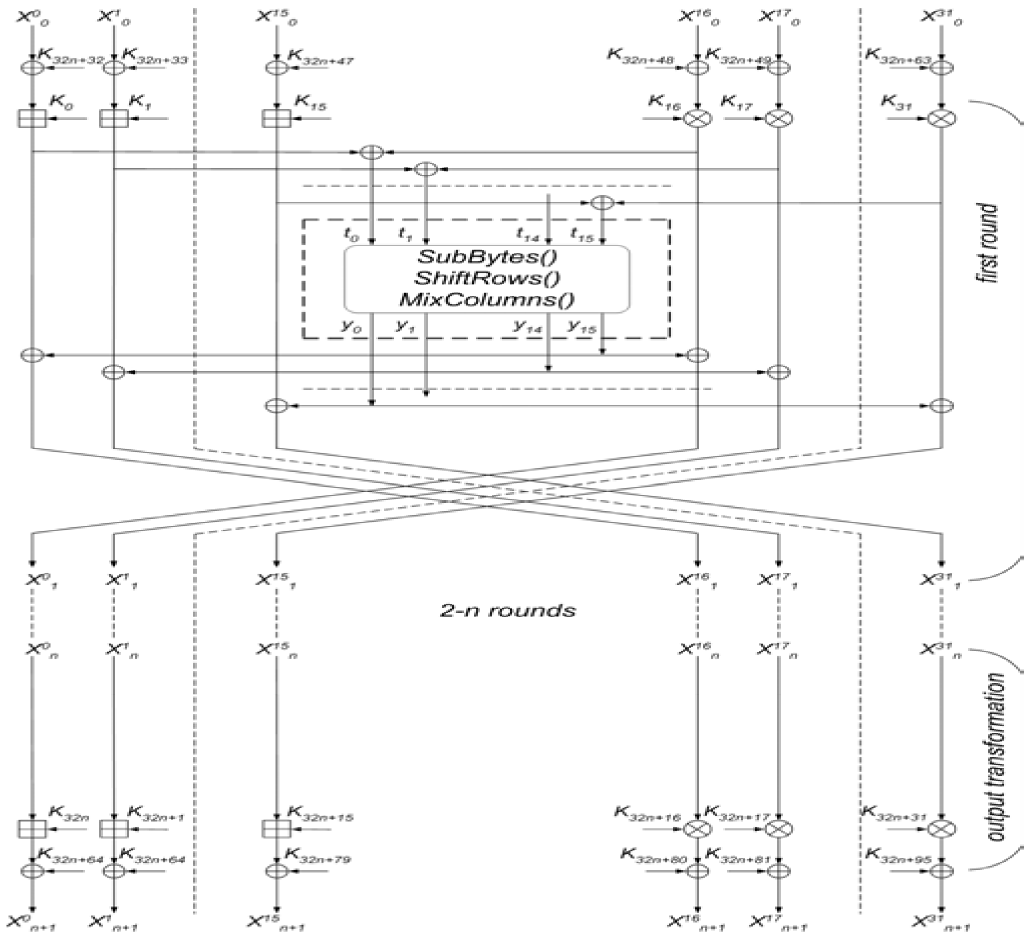


Figure 4: The scheme n-rounded encryption algorithm AES-RFWKIDEA32-1

The S-box SubBytes() transformation shown in Table 1 and is the only non-linear transformation. The length of the input and output blocks S-box is eight bits. For example, if the input value the S-box is equal to 0xE7, then the output value is equal 0x79, i.e. selected elements of intersection row 0xE and column 0x7.

Table 1 : The S-box of encryption algorithm AES-RFWKIDEA32-1

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x87	0x1C	0x05	0x06	0x13	0x86	0x84	0xC9	0x3F	0xEF	0x85	0xA6	0x10	0x41	0xA2	0x15
0x1	0xD2	0xF3	0xCA	0x0C	0x12	0x4E	0xC5	0x1B	0xA8	0x59	0xB3	0xA0	0x78	0xB9	0x17	0xDB
0x2	0x21	0x08	0x63	0xB5	0x35	0x24	0x01	0xD8	0x3D	0xA9	0x89	0x0B	0x0F	0x5A	0x2F	0x6D
0x3	0xFD	0xC1	0xA7	0xC3	0x7E	0x71	0xED	0x72	0xE5	0x77	0xFB	0x93	0x82	0xA5	0x33	0x0D
0x4	0xEE	0xE3	0xBC	0x76	0x66	0x94	0x56	0xBB	0x57	0x26	0x51	0x23	0xAE	0x83	0xA4	0xF9
0x5	0x47	0x4B	0xFF	0x88	0xBF	0x18	0x2B	0x46	0x96	0xC2	0x30	0x2E	0xD6	0xDC	0x5E	0xC0
0x6	0x5B	0x80	0xB2	0x02	0xC7	0xCC	0x27	0xE9	0xCD	0x0A	0xF7	0x04	0x5F	0x3C	0x60	0xBA
0x7	0x4F	0xA3	0xDF	0xE0	0x73	0x68	0x3E	0x09	0x38	0x31	0x52	0xAF	0x7F	0x00	0x03	0x53
0x8	0xC8	0xFC	0x67	0x98	0x44	0x61	0xDD	0x65	0xD9	0xA1	0x14	0x2C	0x9D	0x4C	0x6E	0x07
0x9	0x9F	0xEB	0xC4	0x58	0xB7	0xB6	0x7B	0xFA	0xD5	0x90	0x3A	0x7D	0x50	0x54	0xE6	0x42
0xA	0x9B	0x37	0x36	0xF6	0xCE	0xF5	0xBD	0x5C	0xD3	0x43	0xB8	0x97	0x6B	0x69	0x99	0x0E
0xB	0x81	0xDA	0x25	0x8C	0xE8	0x49	0xD4	0xAA	0x9C	0x55	0x19	0x92	0x8D	0x16	0xB0	0xFE
0xC	0x32	0x1E	0xAD	0xB4	0x7C	0xB1	0x39	0xD1	0x9A	0x48	0x1D	0x64	0xC6	0x28	0xE2	0xF2
0xD	0x1F	0x34	0x29	0x95	0xDE	0xE7	0x11	0xF4	0x8F	0x2D	0x45	0x2A	0xF1	0xCB	0x6C	0x70
0xE	0x8B	0x1A	0x7A	0x6F	0x8E	0x4A	0xF0	0x79	0x62	0x74	0xE1	0x8A	0xD0	0x4D	0xBE	0x40
0xF	0xF8	0xAB	0xEA	0xEC	0x20	0x91	0xD7	0x9E	0xCF	0x6A	0xAC	0xE4	0x3B	0x5D	0x22	0x75

Consider the encryption process of encryption algorithm AES-RFWKIDEA32-1. Initially the 256-bit plaintext X partitioned into subblocks of 8-bits $X_0^0, X_0^1, \ldots, X_0^{31}$, and performs the following steps:

1. subblocks $X_0^0, X_0^1, \ldots, X_0^{31}$ summed by XOR respectively with round key K_{32n+32}, K_{32n+33}, ..., K_{32n+63}:

$$X_0^j = X_0^j \oplus K_{32n+32+j},\ j = \overline{0...31}.$$

2. subblocks $X_0^0, X_0^1, \ldots, X_0^{31}$ multiplied and summed respectively with the round keys $K_{32(i-1)}$, $K_{32(i-1)+1}$, . . . , $K_{32(i-1)+31}$ and calculated 8-bit sub- blocks t_0, t_1, . . . , t_{15}. This step can be represented as follows:

$$t_0 = (X_{i-1}^0 + K_{32(i-1)}) \oplus (X_{i-1}^{16} \cdot K_{32(i-1)+16}),$$
$$t_1 = (X_{i-1}^1 \cdot K_{32(i-1)+1}) \oplus (X_{i-1}^{17} + K_{32(i-1)+17}),$$
$$t_2 = (X_{i-1}^2 + K_{32(i-1)+2}) \oplus (X_{i-1}^{18} \cdot K_{32(i-1)+18}),$$
$$t_3 = (X_{i-1}^3 \cdot K_{32(i-1)+3}) \oplus (X_{i-1}^{19} + K_{32(i-1)+19}),$$
$$t_4 = (X_{i-1}^4 + K_{32(i-1)+4}) \oplus (X_{i-1}^{20} \cdot K_{32(i-1)+20}),$$
$$t_5 = (X_{i-1}^5 \cdot K_{32(i-1)+5}) \oplus (X_{i-1}^{21} + K_{32(i-1)+21}),$$
$$t_6 = (X_{i-1}^6 + K_{32(i-1)+6}) \oplus (X_{i-1}^{22} \cdot K_{32(i-1)+22}),$$
$$t_7 = (X_{i-1}^7 \cdot K_{32(i-1)+7}) \oplus (X_{i-1}^{23} + K_{32(i-1)+23}),$$
$$t_8 = (X_{i-1}^8 + K_{32(i-1)+8}) \oplus (X_{i-1}^{24} \cdot K_{32(i-1)+24}),$$
$$t_9 = (X_{i-1}^9 \cdot K_{32(i-1)+9}) \oplus (X_{i-1}^{25} + K_{32(i-1)+25}),$$
$$t_{10} = (X_{i-1}^{10} + K_{32(i-1)+10}) \oplus (X_{i-1}^{26} \cdot K_{32(i-1)+26}),$$
$$t_{11} = (X_{i-1}^{11} \cdot K_{32(i-1)+11}) \oplus (X_{i-1}^{27} + K_{32(i-1)+27}),$$

$$t_{12} = (X^{12}_{i-1} + K_{32(i-1)+12}) \oplus (X^{28}_{i-1} \cdot K_{32(i-1)+28}),$$
$$t_{13} = (X^{13}_{i-1} \cdot K_{32(i-1)+13}) \oplus (X^{29}_{i-1} + K_{32(i-1)+29}),$$
$$t_{14} = (X^{14}_{i-1} + K_{32(i-1)+14}) \oplus (X^{30}_{i-1} \cdot K_{32(i-1)+30}),$$
$$t_{15} = (X^{15}_{i-1} \cdot K_{32(i-1)+15}) \oplus (X^{31}_{i-1} + K_{32(i-1)+31}), \, , i = 1.$$

3. performed SubBytes(), ShiftRows(), MixColumns() transformation. Output subblocks of the round function of the encryption algorithm are y_0, y_1, . . . ,y_{31}.

4. subblocks y_0, y_1, . . . , y_{31} are summed to XOR with subblocks $X^0_{i-1}, X^1_{i-1}, \dots, X^{31}_{i-1}$, i.. $X^j_{i-1} = X^j_{i-1} \oplus y_{15-j}$, $X^{j+16}_{i-1} = X^{j+16}_{i-1} \oplus y_{15-j}$, $j = \overline{0...15}$, $i = 1$.

5. at the end of the round subblocks X^j_{i-1} and X^{31-j}_{i-1}, $j = \overline{1...\quad}$ 15 swapped, i..,

$$X^0_i = X^0_{i-1},\ X^1_i = X^{30}_{i-1},\ X^2_i = X^{29}_{i-1},\ X^3_i = X^{28}_{i-1},$$
$$X^3_i = X^{27}_{i-1},\ X^5_i = X^{26}_{i-1},\ X^6_i = X^{25}_{i-1},\ X^7_i = X^{24}_{i-1},$$
$$X^8_i = X^{23}_{i-1},\ X^9_i = X^{22}_{i-1},\ X^{10}_i = X^{21}_{i-1},\ X^{11}_i = X^{20}_{i-1},$$
$$X^{12}_i = X^{19}_{i-1},\ X^{13}_i = X^{18}_{i-1},\ X^{14}_i = X^{17}_{i-1},\ X^{15}_i = X^{16}_{i-1},$$
$$X^{16}_i = X^{15}_{i-1},\ X^{17}_i = X^{14}_{i-1},\ X^{18}_i = X^{13}_{i-1},\ X^{19}_i = X^{12}_{i-1},$$
$$X^{20}_i = X^{11}_{i-1},\ X^{21}_i = X^{10}_{i-1},\ X^{22}_i = X^{9}_{i-1},\ X^{23}_i = X^{8}_{i-1},$$
$$X^{24}_i = X^{7}_{i-1},\ X^{25}_i = X^{6}_{i-1},\ X^{26}_i = X^{5}_{i-1},\ X^{27}_i = X^{4}_{i-1},$$
$$X^{28}_i = X^{3}_{i-1},\ X^{29}_i = X^{2}_{i-1},\ X^{30}_i = X^{1}_{i-1},\ X^{31}_i = X^{31}_{i-1},$$
$i = 1$.

6. repeating steps 2-5 n times, i.e., i = 2...n obtain subblocks $X^0_n,\ X^1_n,\ \dots, X^{31}_n$.

7. in output transformation round keys are multiplied and summed into sub-blocks, i.e.

$$X^0_{n+1} = X^0_n + K_{32n},\ X^1_{n+1} = X^{30}_n \cdot K_{32n+1},$$
$$X^2_{n+1} = X^{29}_n + K_{32n+2},\ X^3_{n+1} = X^{28}_n \cdot K_{32n+3},$$
$$X^4_{n+1} = X^{27}_n + K_{32n+4},\ X^5_{n+1} = X^{26}_n \cdot K_{32n+5},$$
$$X^6_{n+1} = X^{25}_n + K_{32n+6},\ X^7_{n+1} = X^{24}_n \cdot K_{32n+7},$$
$$X^8_{n+1} = X^{23}_n + K_{32n+8},\ X^9_{n+1} = X^{22}_n \cdot K_{32n+9},$$
$$X^{10}_{n+1} = X^{21}_n + K_{32n+10},\ X^{11}_{n+1} = X^{20}_n \cdot K_{32n+11},$$
$$X^{12}_{n+1} = X^{19}_n + K_{32n+12},\ X^{13}_{n+1} = X^{18}_n \cdot K_{32n+13},$$
$$X^{14}_{n+1} = X^{17}_n + K_{32n+14},\ X^{15}_{n+1} = X^{16}_n \cdot K_{32n+15},$$
$$X^{16}_{n+1} = X^{15}_n \cdot K_{32n+16},\ X^{17}_{n+1} = X^{14}_n + K_{32n+17},$$
$$X^{18}_{n+1} = X^{13}_n \cdot K_{32n+18},\ X^{19}_{n+1} = X^{12}_n + K_{32n+19},$$
$$X^{20}_{n+1} = X^{11}_n \cdot K_{32n+20},\ X^{21}_{n+1} = X^{10}_n + K_{32n+21},$$
$$X^{22}_{n+1} = X^{9}_n \cdot K_{32n+22},\ X^{23}_{n+1} = X^{8}_n + K_{32n+23},$$
$$X^{24}_{n+1} = X^{7}_n \cdot K_{32n+24},\ X^{25}_{n+1} = X^{6}_n + K_{32n+25},$$
$$X^{26}_{n+1} = X^{5}_n \cdot K_{32n+26},\ X^{27}_{n+1} = X^{4}_n + K_{32n+27},$$
$$X^{28}_{n+1} = X^{3}_n \cdot K_{32n+28},\ X^{29}_{n+1} = X^{2}_n + K_{32n+29},$$
$$X^{30}_{n+1} = X^{1}_n \cdot K_{32n+30},\ X^{31}_{n+1} = X^{31}_n + K_{32n+31},$$

8. subblocks $X^0_{n+1},\ X^1_{n+1},\ \dots,\ X^{31}_{n+1}$ are summed
K K
to XOR with the roundkey $\overline{key}$ $_{32n+64}$, $_{32n+65}$, $\dots$, K_{32n+95}: $X^j_{n+1} = X^j_{n+1} \oplus K_{32n+64+j}$, $j = 0...31$. As ciphertext plaintext X receives the combined 16-bit subblocks $X^0_{n+1}||X^1_{n+1}||...||X^{31}_{n+1}$.

b) Key generation of the encryption algorithm AES-RFWKIDEA32-1

In n-round encryption algorithm AES-RFWKIDEA32-1 in each round we applied sixteen (32) round keys of the 8-bit and output transformation sixteen (32) round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen (32) round keys of 8-bits. Total number of 8-bit round keys is equal to 32n+96. In Figure 4 encryption used encryption round keys K^c_i instead of K_i, while decryption used decryption round keys K^d_i . If n=10 then need 416 to generate round keys, if n=12, you need to generate 480 round keys and if n=14 need 544 to generate round keys.

When generating round keys like the AES encryption algorithm uses an array Rcon: Rcon=[0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80].

The key encryption algorithm K of length l (256 $\leq l \leq$1024) bits is divided into 8-bit round keysK^c_0, K^c_1 ,..., $K^c{}_{Lenght-1}$, Lenght $= l/$ 8, here K = $\{k_0, k_1, ..., k_{l-1}\}$, $K^c_0 = \{k_0, k_1, ..., k_7\}$, $K^c_1 = \{k_8, k_9, ..., k_{15}\}$,..., $K^c_{Lenght-1} = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ 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 0xC5, i.e. $K_L = \mathrm{0xC5}$.

When generating a round keys K^c_i, $i = \overline{Lenght...32n+95}$, we used transforma- tion SubBytes() and RotWord8(), here SubBytes()-is transformation 8-bit sub-block into S-box and RotWord8()-cyclic shift to the left of 1 bit of the 8-bit subblock. When the condition imod3 = 1 is true, then the round keys are com- puted as K^c_i = SubBytes $(K^c_{i-Lenght+1}) \oplus$ SubBytes(RotWord8 $K^c_{i-Lenght})) \oplus$ Rcon[imod8]$\oplus K_L$ otherwise K^c_i = SubBytes $(K^c_{i-Lenght}) \oplus SubBytes(K^c_{i-Lenght+1}) \oplus K_L$. 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 output transformation associate with of en- cryption round keys as follows:

$$(K^d_{32n}, K^d_{32n+1}, K^d_{32n+2}, K^d_{32n+3}, K^d_{32n+4}, K^d_{32n+5}, K^d_{32n+6}, K^d_{32n+7},$$
$$K^d_{32n+8}, K^d_{32n+9}, K^d_{32n+10}, K^d_{32n+11}, K^d_{32n+12}, K^d_{32n+13}, K^d_{32n+14}, K^d_{32n+15},$$
$$K^d_{32n+16}, K^d_{32n+17}, K^d_{32n+18}, K^d_{32n+19}, K^d_{32n+20}, K^d_{32n+21}, K^d_{32n+22},$$
$$K^d_{32n+23}, K^d_{32n+24}, K^d_{32n+25}, K^d_{32n+26}, K^d_{32n+27}, K^d_{32n+28}, K^d_{32n+29},$$
$$K^d_{32n+30}, K^d_{32n+31}) = (-K^c_0, (K^c_1)^{-1}, -K^c_2, (K^c_3)^{-1}, -K^c_4, (K^c_5)^{-1},$$
$$-K^c_6, (K^c_7)^{-1}, -K^c_8, (K^c_9)^{-1}, -K^c_{10}, (K^c_{11})^{-1}, -K^c_{12}, (K^c_{13})^{-1}, -K^c_{14},$$
$$(K^c_{15})^{-1}, (K^c_{16})^{-1}, -K^c_{17}, (K^c_{18})^{-1}, -K^c_{19}, (K^c_{20})^{-1}, -K^c_{21}, (K^c_{22})^{-1},$$
$$-K^c_{23}, (K^c_{24})^{-1}, -K^c_{25}, (K^c_{26})^{-1}, -K^c_{27}, (K^c_{28})^{-1}, -K^c_{29}, (K^c_{30})^{-1}, -K^c_{31}).$$

$$(K_{320}^d, K_{321}^d, K_{322}^d, K_{323}^d, K_{324}^d, K_{325}^d, K_{326}^d, K_{327}^d, K_{328}^d, K_{329}^d, K_{330}^d, K_{331}^d, K_{332}^d, K_{333}^d, K_{334}^d, K_{335}^d, K_{336}^d, K_{337}^d, K_{338}^d, K_{339}^d, K_{340}^d, K_{341}^d, K_{342}^d, K_{343}^d, K_{344}^d, K_{345}^d, K_{346}^d, K_{347}^d, K_{348}^d, K_{349}^d, K_{350}^d, K_{351}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, -K_8^c, (K_9^c)^{-1}, -K_{10}^c, (K_{11}^c)^{-1}, -K_{12}^c, (K_{13}^c)^{-1}, -K_{14}^c, (K_{15}^c)^{-1}, (K_{16}^c)^{-1}, -K_{17}^c, (K_{18}^c)^{-1}, -K_{19}^c, (K_{20}^c)^{-1}, -K_{21}^c, (K_{22}^c)^{-1}, -K_{23}^c, (K_{24}^c)^{-1}, -K_{25}^c, (K_{26}^c)^{-1}, -K_{27}^c, (K_{28}^c)^{-1}, -K_{29}^c, (K_{30}^c)^{-1}, -K_{31}^c).$$

For example, if the number of rounds is 10 the formula is as follows:

Decryption round keys of the first round associates with the encryption round keys as follows:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d, K_{24}^d, K_{25}^d, K_{26}^d, K_{27}^d, K_{28}^d, K_{29}^d, K_{30}^d, K_{31}^d) = (-K_{32n}^c, (K_{32n+1}^c)^{-1}, -K_{32n+2}^c, (K_{32n+3}^c)^{-1}, -K_{32n+4}^c, (K_{32n+5}^c)^{-1} -K_{32n+6}^c, (K_{32n+7}^c)^{-1}, -K_{32n+8}^c, (K_{32n+9}^c)^{-1}, -K_{32n+10}^c, (K_{32n+11}^c)^{-1}, -K_{32n+12}^c, (K_{32n+13}^c)^{-1}, -K_{32n+14}^c, (K_{32n+15}^c)^{-1}, (K_{32n+16}^c)^{-1}, -K_{32n+17}^c, (K_{32n+18}^c)^{-1}, -K_{32n+19}^c, (K_{32n+20}^c)^{-1}, -K_{32n+21}^c, (K_{32n+22}^c)^{-1}, -K_{32n+23}^c, (K_{32n+24}^c)^{-1}, -K_{32n+25}^c, (K_{32n+26}^c)^{-1}, -K_{32n+27}^c, (K_{32n+28}^c)^{-1}, -K_{32n+29}^c, (K_{32n+30}^c)^{-1}, -K_{32n+31}^c).$$

Likewise, the decryption round keys of the second, third and n{round associates with the encryption round keys as follows:

$$(K_{32(i-1)}^d, K_{32(i-1)+1}^d, K_{32(i-1)+2}^d, K_{32(i-1)+3}^d, K_{32(i-1)+4}^d, K_{32(i-1)+5}^d, , K_{32(i-1)+6}^d, K_{32(i-1)+7}^d, K_{32(i-1)+8}^d, K_{32(i-1)+9}^d, K_{32(i-1)+10}^d, K_{32(i-1)+11}^d, K_{32(i-1)+12}^d, K_{32(i-1)+13}^d, K_{32(i-1)+14}^d, K_{32(i-1)+15}^d, K_{32(i-1)+16}^d, K_{32(i-1)+17}^d, K_{32(i-1)+18}^d, K_{32(i-1)+19}^d, K_{32(i-1)+20}^d, K_{32(i-1)+21}^d, K_{32(i-1)+22}^d, K_{32(i-1)+23}^d, K_{32(i-1)+24}^d, K_{32(i-1)+25}^d, K_{32(i-1)+26}^d, K_{32(i-1)+27}^d, K_{32(i-1)+28}^d, K_{32(i-1)+29}^d, K_{32(i-1)+30}^d, K_{32(i-1)+31}^d) = (-K_{32(n-i+1)}^c, (K_{32(n-i+1)+30}^c)^{-1}, -K_{32(n-i+1)+29}^c, (K_{32(n-i+1)+28}^c)^{-1}, -K_{32(n-i+1)+27}^c, (K_{32(n-i+1)+26}^c)^{-1}, -K_{32(n-i+1)+25}^c, (K_{32(n-i+1)+24}^c)^{-1}, -K_{32(n-i+1)+23}^c, (K_{32(n-i+1)+22}^c)^{-1}, -K_{32(n-i+1)+21}^c, (K_{32(n-i+1)+20}^c)^{-1}, -K_{32(n-i+1)+19}^c, (K_{32(n-i+1)+18}^c)^{-1}, -K_{32(n-i+1)+17}^c, (K_{32(n-i+1)+16}^c)^{-1}, (K_{32(n-i+1)+15}^c)^{-1}, -K_{32(n-i+1)+14}^c, (K_{32(n-i+1)+13}^c)^{-1}, -K_{32(n-i+1)+12}^c, (K_{32(n-i+1)+11}^c)^{-1}, -K_{32(n-i+1)+10}^c, (K_{32(n-i+1)+9}^c)^{-1}, -K_{32(n-i+1)+8}^c, (K_{32(n-i+1)+7}^c)^{-1}, -K_{32(n-i+1)+6}^c, (K_{32(n-i+1)+5}^c)^{-1}, -K_{32(n-i+1)+4}^c, (K_{32(n-i+1)+3}^c)^{-1}, -K_{32(n-i+1)+2}^c, (K_{32(n-i+1)+1}^c)^{-1}, -K_{32(n-i+1)+31}^c),\ i = \overline{2...n}$$

Decryption round keys applied to the _rst round and after the output transformation associated with the encryption round keys as follows: $K_{32n+32+\ j}^d = K_{32n+64+j}^c$, $K_{32n+64+j}^d = K_{32n+32+j}^c$, $j = \overline{0...31}$.

IV. RESULTS

Using the transformations SubBytes(), ShiftRows(), MixColumns() of the encryption algorithm AES as the round function network RFWKIDEA32-1 we developed encryption algorithm AES-RFWKIDEA32-1. In the algorithm, the number of rounds of encryption and key's length is variable and the user can select the number of rounds and the key's length in dependence of the degree of secrecy of information and speed encryption.

As in the encryption algorithms based on the Feistel network, the advantages of the encryption algorithm AES-RFWKIDEA32-1 are that, when encryption and decryption process used the same algorithm. In the encryption algorithm AES-RFWKIDEA32-1 in decryption process encryption round keys are used in reverse order, thus on the basis of operations necessary to compute the inverse. For example, if the round key is multiplied by the subblock, while decryption is is necessary to calculate the multiplicative inverse, if summarized, it is necessary to calculate the additive inverse.

It is known that the resistance of AES encryption algorithm is closely associated with resistance S-box, applied in the algorithm. In the S-box's encryption algorithm AES algebraic degree of nonlinearity deg = 7, nonlinearity NL = 112, resistance to linear cryptanalysis $\lambda = 32 = 256$, resistance to diferential cryptanal ysis $\delta =$ $= 4/256$, strict avalanche criterion SAC = 8, bit independence criterion BIC = 8.

Global Journal of Computer Science and Technology (E) Volume XV Issue IV Version I Year 2015

In the encryption algorithm AES-RFWKIDEA32-1 resistance S-box is equal to resistance S-box's encryption algorithm AES, i.e., deg = 7, NL = 112, _ = 32=256, _ = 4=256, SAC= BIC=8.

V. Conclusions

It is known that as a network-based algorithms Feystel the resistance algorithm based on network RFWKIDEA32-1 closely associated with resistance round function. Therefore, selecting the transformations SubBytes(), ShiftRows(), Mix-Columns() of the encryption algorithm AES, based on round function network RFWKIDEA32-1 we developed relatively resistant encryption algorithm.

References Références Referencias

1. Bahrak B., Reza A.M. A Novel Impossible Di_erential Cryptanalysis of AES // proceedings of the Western European Workshop on Research in Cryptology 2007, Bochum, Germany, 2007.
2. Bahrak B., Reza A.M. Impossible Di_erential Attack on Seven-Round AES-128 // IET Information Security journal, Vol. 2, Number 2, pp. 2832, IET, 2008.
3. Biham E., Biryukov A., Shamir A.. Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre // 6th Fast Software Encryption Workshop, LNCS 1636, L.R. Knud-sen,Ed., Springer-Verlag, 1999, pp. 124138.
4. Biham E., Keller N. Cryptanalysis of Reduced Variants of Rijndael // unpublished manuscript, 1999.
5. Borst J. Di_erential-Linear Cryptanalysis of IDEA // Department of Electrical Engineering, ESATCOSIC Technical Report 96/2, 14 pages.
6. Borst J., Knudsen L., Rijmen V. Two Attacks on Reduced IDEA (extended abstract) // Advances in Cryptology, Eurocrypt97, LNCS 1233, W. Fumy, Ed.,Springer-Verlag, 1997, pp. 113.
7. Chen J. Personal communications, August 2008.
8. Chen J., Hu Y., Wei Y. A New Method for Impossible Di_erential Cryptanalysis of 7-round Advanced Encryption Standard // Proceedings of International Conference on Communications, Circuits and Systems Proceedings 2006, Vol. 3, pp. 1577-1579, IEEE, 2006.
9. Chen J., Hu Y., Wei Y. A New Method for Impossib le Di_erential cryptanalysis of 8-Round Adanced Encryption Standard // Wuhan Univeristy Journan of NationalSciences, vol. 11, number 6, pp. 1559-1562, 2006. Lecture Notes in Computer Science: Authors' Instructions 13\
10. Chen J., Hu Y., Zhang Y. Impossible di_erential cryptanalysis of Advanced Encryption Standard // Science in China Series F: Information Sciences, vol. 50, number 3, pp. 342350, Springer-Verlag, 2007.
11. Cheon J., Kim M., Kim K., Lee J-Y., Kang S. Improved Impossible Di_erential Cryptanalysis of Rijndael and Crypton // proceedings of Information Security and Cryptology ICISC 2001, Lecture Notes in Computer Science 2288,pp. 3949, Springer, 2002.
12. Daemen J., Govaerts R. , J. Vandewalle. Cryptanalysis of 2.5 Rounds of IDEA (Extended Abstract) // Department of Electrical Engineering, ESATCOSIC Technical Report 93/1, Mar. 1993, pp. 16.
13. Daeman J., Rijmen V. AES proposal: Rijndael, version 2, 1999. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
14. Demirci H, Selcuk A. A Meet-in-the-Middle Attack on 8-Round AES // proceedings of Fast Software Encryption 15, Lecture Notes in Computer Science 5806,pp. 116126, Springer, 2008.
15. Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D. Improved Cryptanalysis of Rijndael // proceedings of Fast Software Encryption 7, Lecture Notes in Computer Science 1978, pp. 213230, Springer-Verlag, 2001.
16. Gilbert H., Minier M. A collision attack on 7 rounds of Rijndael // proceedings of the Third AES Candidate Conference (AES3), pp. 230241, New York, USA, 2000.
17. Hawkes P. Di_erential-LinearWeak Key Classes of IDEA // Advances in Cryptology,Eurocrypt98, LNCS 1403, K. Nyberg, Ed., Springer-Verlag, 1998, pp. 112126.
18. Kelsey J., Schneier B., Wagner D. Key-Schedule Cryptanalysis of IDEA, GDES,GOST, SAFER and Triple-DES // Advances in Cryptology, Crypto96, LNCS 1109,N. Koblitz, Ed., Springer-Verlag, 1996, pp. 237251.
19. Knudsen L.R., Rijmen V. Truncated Di_erentials of IDEA // Department of Electrical Engineering, ESATCOSIC Technical Report 97/1.
20. Kim J., Hong S., Preneel B. Related-Key Rectangle Attacks on Reduced AES-192 and AES-256 // Proceedings of Fast Software Encryption 14, Lecture Notes in Computer Science 4593, pp. 225241, Springer-Verlag, 2007.
21. Lai X. On the Design and Security of Block Ciphers // Hartung-Gorre Verlag, Konstanz, 1992.
22. Lai X., Massey J.L. A Proposal for a New Block Encryption Standard // Advances in Cryptology, Eurocrypt90, LNCS 473, I.B. Damgard, Ed., Springer-Verlag, 1990, pp. 389404.
23. Lai X., Massey J.L., Murphy S. Markov Ciphers and Di_erential Cryptanalysis // Advances in Cryptology, Eurocrypt91, LNCS 547, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 1738.

24. Lucks S. Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys // proceedings of the Third AES Candidate Conference (AES3), pp. 215229, New York, USA, 2000.
25. Lu J., Dunkelman O., Keller N., Kim J. New Impossible Di_erential Attacks on AES
26. Meier W. On the Security of the IDEA Block Cipher // Advances in Cryptology,Eurocrypt93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 371385.
27. Nakahara J., Paulo S.L.M. Barreto, Preneel B., Vandewalle J., Kim Y. SQUARE Attacks on Reduced-Round PES and IDEA Block Ciphers.
28. National Institute of Standards and Technology. Announcing the Advanced Encryption Standard (AES), 2001. Federal Information Processing Standards Pub-14 Lecture Notes in Computer Science: Authors' Instructions lication 197. http:// csrc.nist.gov/publications/fips/fips197/fips-197.pdf
29. Phan R. Ch-W. Impossible Di_erential Cryptanalysis of 7-round Advanced Encryption Standard (AES) // Information Processing Letters, Vol. 91, Number 1, pp. 33-38, Elsevier, 2004.
30. Tuychiev G.N. About networks IDEA328, IDEA324, IDEA322, IDEA321, created on the basis of network IDEA3216 // Infocommunications: Networks Technologies- Solutions. Tashkent, 2014. 2 (30), pp. 4550.
31. Tuychiev G.N. To the networks RFWKIDEA3216, RFWKIDEA328, RFWKIDEA324, RFWKIDEA322 and RFWKIDEA321, based on the net- work IDEA3216 // International Journal on Cryptography and Information Security (IJCIS), Vol. 5, No. 1, March 2015, pp. 9-20
32. Tuychiev G.N. About networks IDEA8-2, IDEA8-1 and RFWKIDEA8-4, RFWKIDEA8-2, RFWKIDEA8-1 developed on the basis of network IDEA8-4 // Uzbek mathematical journal, {Tashkent, 2014, 3, pp. 104{118
33. Tuychiev G.N. About networks PES8-2 and PES8-1, developed on the basis of network PES8-4 // Transactions of the international scientific conference Modern problems of applied mathematics and information technologies {Al {Khorezmiy 2012, Volume II, { Tashkent, 2014, pp. 28{32.
34. Tuychiev G.N. About networks RFWKPES8{4, RFWKPES8{2, RFWKPES8{1, developed on the basis of network PES8{4 // Transactions of the international scientific conference Modern problems of applied mathematics and information technologies {Al {Khorezmiy 2012, Volume 2, { Tashkent, 2014, pp. 32{36
35. Tuychiev G.N. 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 {Tashkent, 2014
36. Tuychiev G. New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1-6
37. Tuychiev G. New encryption algorithm based on network RFWKIDEA8-1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security, 2015, Vol. 3, NO. 2, pp. 43-47
38. Tuychiev G. New encryption algorithm based on network PES8-1 using of the transformations of the encryption algorithm AES // International Journal of Mul-tidisciplinary in Cryptology and Information Security, 2015, vol.4., 1, pp. 1-5
39. Tuychiev G. New encryption algorithm based on network RFWKPES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2014, vol.3., 6, pp. 31-34
40. Tuychiev G. New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Information Technology, 2015, Volume 3, Issue 1, pp. 6-12
41. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology. Data Encryption Standard (DES), 1979. Federal Information Pro-cessing Standards Publication 46-3, http:// csrc.nist.gov/publications/fips/fips46-3/fips 46- .pdf
42. Zhang W., Wu W., Feng D. New Results on Impossible Di_erential Cryptanalysis of Reduced AES // proceedings of ICISC 2007, Lecture Notes in Computer Science 4817, pp. 239250, Springer-Verlag, 2007.
43. Lecture Notes in Computer Science: Authors' Instructions 15 Zhang W., Wu W., Zhang L. Dengguo Feng, Improved Related-Key Impossible Di_erential Attacks on Reduced-Round AES-192 // Proceedings of Selected Areas in Cryptography 2006, Lecture Notes in Computer Science 4356, pp. 1527, Springer-Verlag, 2007.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards “FARSC” title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

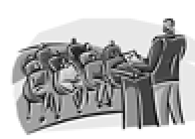
- The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

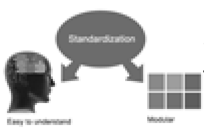


You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.



The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

Auxiliary Memberships

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

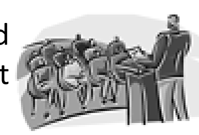
The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

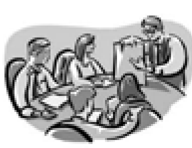
The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.



The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

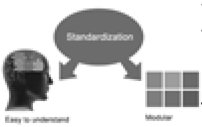


The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.



After nomination of your institution as “Institutional Fellow” and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

MANUSCRIPT STYLE INSTRUCTION **(Must be strictly followed)**

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, “Abstract” word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript’s Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation)
by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350