Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme

By Gorti VNKV Subba Rao & Dr. Garimella Uma
*Sree Dattha Institutions, India*

*Abstract -* In MANETs the nodes are capable of roaming independently. The node with inadequate physical protection can be easily captured, compromised and hijacked. Due to this huge dependency's on the nodes, there are more security problems. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer. In this paper we look at the current scheme to transmit the data in MANETs. We then propose a new scheme for secure transmission of message in MANETs as Alternative scheme for DF's new Ph and DF's additive and multiplicative PH. Here we also provide the computational cost of the homomorphic encryption schemes. We also provide the implementation issues of our new scheme in MANETs. For the entire message to be recoverd by the attacker, the attacker needs to compromise atleast g nodes, one node from each group g and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network.

*GJCST-E Classification :* *E.3*

AN EFFICIENT SECURE MESSAGE TRANSMISSION IN MOBILE AD HOC NETWORKS USING ENHANCED HOMOMORPHIC ENCRYPTION SCHEME

*Strictly as per the compliance and regulations of:*

# An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme

Gorti VNKV Subba Rao [α] & Dr. Garimella Uma [σ]

*Abstract* - In MANETs the nodes are capable of roaming independently. The node with inadequate physical protection can be easily captured, compromised and hijacked. Due to this huge dependency's on the nodes, there are more security problems. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer. In this paper we look at the current scheme to transmit the data in MANETs. We then propose a new scheme for secure transmission of message in MANETs as Alternative scheme for DF's new Ph and DF's additive and multiplicative PH. Here we also provide the computational cost of the homomorphic encryption schemes. We also provide the implementation issues of our new scheme in MANETs. For the entire message to be recoverd by the attacker, the attacker needs to compromise atleast *g* nodes, one node from each group *g* and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network.

## I. Gorti's-Enhanced Homomorphic Cryptosystem (EHC)

A new Enhanced homomorphic Cryptosystem (EHC) for homomorphic Encryption / Decryption with IND-CCA secure. Homomorphic encryption schemes allow operations to be performed on the encrypted data as if the operations are performed on the plaintext. Homomorphic encryption has numerous applications in real time. The computer will perform the computation on the encrypted data, hence without knowing anything of its real value. Finally, it will send back the result, and that will be decrypted. For coherence, the decrypted result has to be equal to the intended computed value if performed on the original data. For this reason, the encryption scheme has to present a particular structure [23].By keeping the all the industry demands we proposed new scheme exhibit better performance than existing schemes mainly in processing speed, memory and power consumption. Our scheme is a non deterministic and exhibits addition, multiplication, mixed addition and mixed multiplication operations. Our Construction. A large prime number 'p', another prime number 'q' such that q < p are taken and a random number 'r' has taken to make the scheme non deterministic. Consider the set of clear text data *Zp* and the set of clear text operations *{+, -,*, / and mixed}* consisting respectively, of the addition, subtraction, multiplication and mixed multiplication modulo m, with *m= pq.* Let the cipher text data set be *Zc*. Define the encryption key k = (p, *q,m,r)* and Ek(X)=)(mod m). *Decryption will be done with the secret key* k = ( p ), X=Dk (Y ) = C mod p. But can be broken if *p* can be discovered but which is a very tough to solve. A computer can factor that number fairly quickly, but (although there are some tricks) it basically does it by trying most of the possible combinations. One can find two huge prime numbers, p and q that have 200 or may be 400 digits each. Q will be kept secret (It is secret key), and by multiplying them together to make a number m = pq. That number m is also a secret key to encrypt the data. It is relatively easy to get m by multiplying p and q. But if anybody know m, it is basically impossible to find p and q . To get them, you need to factor m, which seems to be an incredibly difficult problem finding the ' r ' also difficult as this value will be generated randomly. it is generally regarded that m should be at least 1024, if not 2048.

### a) *Operations Encryption/Decryption of EHC Scheme*

| Secretkeygen() |
|---|
| Chose large prime number ' p ' and another prime number ' q '<br>Calculate m = p * q<br>Generate a random number ' r '.<br>r,q and m Kept secret. Secret values r,q and |
| m Shared key : p |
| Encryption<br>Encrypt(X,m,p,q,r)<br>Assume $X \in Z_p$<br>Compute $Y = (X + r*p^q) \pmod{m}$<br>Output $Y \in Z_c$ |
| Decryption<br>Decrypt(Y,p)<br>input $Y \in Z_c$<br>compute X = Y mod p output $X \in Z_p$ |

Algorithm of EHC

*Author α : Vice Principal,Sree Dattha Institutions, Hyderabad.*
*E-mail : gvnkvsubbarao@yahoo.com*
*Author σ : Director & Professor, Teachers Academy, Hyderabad.*

In order to see that the scheme above deciphers correctly it is necessary to prove that decryption really outputs the original message M.

*Proof :* Encrypt the message X

$$E(X) = )(\text{mod } m)$$

Cipher text Y will be (X+rp)

Decrypt Y = X = Y mod p

= (X+rp) mod p

= rp mod p + X mod p

= X Plaintext

*b) Security of the Encryption Scheme*

We can support strongly our scheme is more secure when compare to existing schemes as follows :

1. Our scheme is very strong as it uses the secret keys q, m and r and sharing key p for encryption. So it is very difficult to find the secret keys.
2. Our scheme only shares the shared key p only between the sender and receiver so it is very difficult to find the q and r.
3. Random number 'r' will be generated randomly so that every time the same plaintext mapped to different cipher text so that it is very tough to track the plain text even with strong observation for opponent.
4. Opponent cannot get the secret value and random number.
5. Our scheme supports Addition, Multiplication, Mixed addition and Mixed multiplication.
6. As we are taking large prime number p the decryption circle will be more so that second multiplication also possible.
7. Is IND-CCA secured scheme which will be proved in the next section.
8. It is very faster than the existing schemes and consumes less power and memory.

*c) Non deterministic feature which enhances the security*

The random number 'r' gives the feature non deterministic means the plaintext will be converted into different cipher text with the change in the value r. We can better understand using the following example.

Let p=11 q=7 r=2 x1=5 x2=3 then m=77 cipher text Y1= 27 cipher text Y2= 25.

Now by changing the random number the same plain text will be mapped to another cipher texts Let p=11 q=7 r=4 x1=5 x2=3 then m=77 cipher text Y1= 49 cipher text Y2= 47.

## II. Introduction to MANETs

Mobile Ad-hoc network (MANETs) is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. By definition, MANETs differentiate themselves from existing networks by the fact that they rely on no fixed infrastructure [Zhou and Haas 1999]: the network has no base stations, access points, remote servers, etc. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1.1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

Technically and architecture wise if we see the MANETs environment consists of mobile nodes that communicate directly with each other in a peer to peer way. Mobile nodes that join together in on movement and they create a network on their own and each these node performs the basic operations like routing and packet forwarding without the help of an established infrastructure. All the available nodes can join together in the network and carry out network operation. Due to this huge dependency's on the each other nodes it is obvious to have more security problems. Other angle if we observe in MANETs, the nodes are capable of roaming independently so that the node with inadequate physical protection can be easily captured, may compromise and hijacked. Therefore the nodes in the network must be prepared to work in a mode that trusts no peer [12, 13].

Security is an important area for MANETS, especially for those comes under security-sensitive applications. To provide security in MANETs, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.[81] Mobile ad hoc networks are self configurable and autonomous systems, comprising of nodes, which are able to move and organize themselves arbitrarily without any infrastructure [1]. Without the support of infrastructure, it is very difficult to distinguish the insider and outsider nodes of the mobile ad hoc networks. Since the mobile adhoc network environment is defined in a unique way, by features such as frequently changing network topology, vulnerable wireless links, storage limitations, and constraints in computational and transmission aspects [2]. Due to the above-mentioned properties of MANETs, the inclusion and implementation of security infrastructure has been a real challenge.

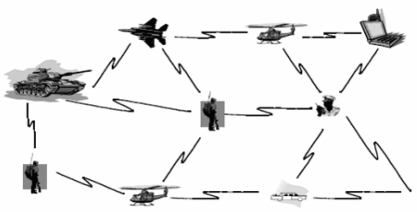


*Figure 1.1 :* Overview of Mobile Ad-hoc Network

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Wireless ad-hoc network have many advantages:

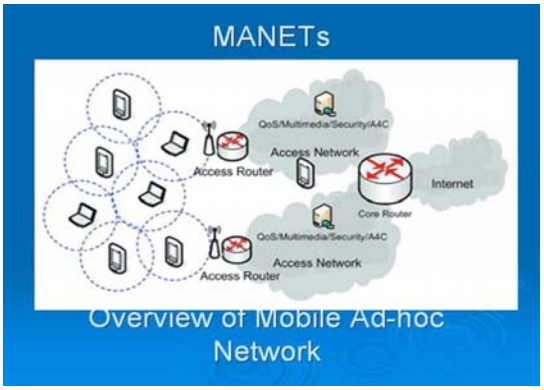
– *Low Cost of Deployment :* Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
– *Fast Deployment :* Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
– *Dynamic Configuration :* Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future in MANET, provision of secure communication protocol should satisfy the following security requirements [7, 8, 9].

1. *Mutual Authentication :* Ensures the authenticity of communicating nodes mutually.
2. *Confidentiality :* Ensures the secrecy of the message content is known only between the authenticated communicating nodes (or users).
3. *Data Integrity :* Ensures the receiver, that the received message is intact.
4. *Non–Repudiation :* Ensures the origin of the message cannot deny having sent the message.
5. *Non–Impersonation :* Ensures unauthorized users cannot pretend to be an authorized one to do malfunction. Proposed novel protocol achieves the above security requirements and also requires less computational power due to the deployment of elliptic curve cryptography and minimum transmission overhead due to less number of handshaking messages.

First we will discuss in detail the existing security solutions available for MANETs. Then we propose a new scheme for secure transmission of message in MANETs as an alternative for threshold cryptography (TC).

## III. Literature Survey




*Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that uses temporary network from existing network infrastructure or central point.* Each node participating in the network acts as host/a router and must forward to packets for other nodes. MANETs are completely different from other network because of their characteristics such as: self organizing capability, node mobility, provides large number of degree of freedom and dynamic topology. As mobile ad hoc networks edge closer toward wide-spread deployment, security issues have became a central concern and are increasingly important.

In fact, ad hoc networks cannot be used in practice if they are not secure, for example, in applications like emergency rescue and battlefield communication; if no security mechanism is used, an adversary can easily thwart the network establishment. Due to their inefficiency, asymmetric/public key cryptosystems, for example RSA, are unsuitable for ad hoc networks where there are constraints on computation and energy [10]. In fact, symmetric key systems, like DES, AES and keyed hash functions, are still the major tools for communication privacy and data authenticity in most networks. To provide secure communication for any group of nodes using symmetric key cryptography, these nodes need to share a common secret key1 By definition [30], an ad hoc network is peer-to-peer and does not rely on any fixed infrastructure.

A *mobile ad hoc network* (MANET) [1] is a collection of wireless mobile nodes that form a temporary network on the fly that operates without the support of any fixed network infrastructure. MANETs are created dynamically and they provide special challenges beyond those in standard data networks [2]. Some examples of the possible uses of ad hoc networking [3],[4] include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or

earthquake. In such networks, each mobile node operates not only as a host but also as a router and cooperates dynamically to establish routing among them to discover "multihop" paths through the network to any other node.

There are various issues related to ad hoc networks [5], [6]. Several protocols have been proposed for routing in such an environment.

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network.

Mobile Ad Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread application in military and civilian communications. Such a network is highly dependent on the cooperation of all of its members to perform networking functions.

## IV. Advantages of Manets

The following are some of the advantages of mobile ad hoc networks.

i. They provide access to information and service regardless of geographic position. This is applicable in military or police exercises, disaster relief operations, mine site operations, and urgent business meetings, where instant communication is needed.
ii. These networks can be setup at any place and time. They can be setup without wires or base stations and the nodes are free to move randomly and organize themselves arbitrarily; thus the networks wireless topology may change rapidly and unpredictably. Mobile devices in the network can freely leave or join the network at will.
iii. The networks work without any preexisting infrastructure. This makes MANETs cost effective for areas where there are no standard communication infrastructures. Owners of MANET equipped devices can communicate with each other, share data and streaming video.
iv. Low Power Consumption is another strong point for MANETs. Most devices used are battery powered; hence they are portable, making mobility easy and devices affordable. Examples are Bluetooth enables phones, laptops, palm tops, etc.

## V. Challenges of Mobile Ad-Hoc Networks

Some challenges mobile ad hoc networks face towards efficient delivery of service includes:

*a) Routing is a Most*

Required function in any network. In ad hoc networks, routing poses two specific challenges. Firstly, routing in traditional networks (examples: the Internet and cellular networks) aims to quickly propagate changes in topology or reach ability, hence creating stable networks, while in mobile ad hoc networks, the topology is constantly changing and is deemed unstable. Secondly, traditional routing solutions rely on some form of distributed routing databases, maintained by the operators in either the networks nodes or specialized management nodes. In mobile ad hoc networks, nodes cannot be assumed to have persistent data storage, and they cannot always be trusted [Hubaux, et al 2001].

*b) Mobility Management*

A network must manage the mobility of its terminals, and therefore be able to locate any of them. In particular, if a terminal wants to communicate with another, it will make use of the address of the latter; the network will have to locate it in some way. The simple solution of broadcasting a paging message to the whole network does not scale. For example, in cellular networks, the location of the mobile stations is stored in centralized servers. The self-organization of ad hoc networks precludes the existence of such servers, leading to mediate loss/trace of any node once outside the range of the immediate network.

*c) IP (Internet Protocol) Addresses*

For small mobile ad hoc networks, addresses are allocated in the traditional way, with an IP prefix identifying the mobile ad hoc network. For large-scale networks, the topology based address allocation currently used in the Internet may not be optimal. In contrast, a node address should be interpreted as a stable node identifier, which carries no specific topological information.

*d) Transport Layer*

Of ad hoc networks also requires attention. Transmission and Control Protocol (TCP) performance in ad hoc networks may be severely degraded, as TCP interprets losses as a signal of congestion and this adversely reduces its sending rate, whereas wireless links may temporarily exhibit high loss rates due to transmission errors not related to congestion.

*e) Radio Interface*

This can be engineered in different ways, based on the requirements of a specific system. Issues to be taken into account include:

i. The decrease in signal strength as the square of the distance.
ii. Some of the traditional multi-access protocols used for wire line LANs cannot be used; example: collision detection is not appropriate because a node is usually unable to listen while it is transmitting.
iii. Two terminals may unknowingly interfere at a third one.

*f) Security*

This is of critical importance for most networks, and mobile ad hoc networks are no exception. Several security features can be required, such as availability of service despite denial-of-service attacks, confidentiality, integrity, authentication, and non-repudiation. Guaranteeing these features is a major challenge.

*g) Power Management*

Is almost always a difficult issue in wireless networks. In the case of ad hoc networks, there are essentially two concerns:

i. Power has to be fine-tuned in order to maximize the throughput of the network: the higher the power, the larger the transmission ranges of the node, but also the higher the interference from other signals. Trade-off is obtained when there is on average exactly one packet in transit over each hop.
ii. Since the nodes are usually battery operated, it is important to minimize their consumption. A typical solution consists in turning the devices to a sleep or idle mode whenever they

## VI. Existing Security Solutions Available in the Area MANETs

1. Secure routing protocol
   a) Secure Routing Protocol (SRP) [9, 10].
   b) Secure link state protocol (SLSP) [11].
2. Secure data forwarding
   a) Secure Message Transmission (SMT) [12,13]
   b) Threshold Cryptography (TC) [14].

In detail we can see below.

*a) Secure routing protocol suggested for MANETs (SRP)*

There are various secure routing protocols suggested for routing packets in MANETs. One such routing protocol is Secure Routing Protocol (SRP) [9, 10]. In SRP, only the end nodes have to be securely associated, with no need for cryptographic operations at the intermediate nodes. SRP provides one or more route replies, whose correctness is verified by the route "geometry" itself, while compromised and invalid routing information is discarded. Another routing protocol is secure link state protocol (SLSP) [11] for MANETs. It uses the secure neighbor discovery and the use of neighbor lookup protocol (NLP) strengthens SLSP against attacks that attempt to exhaust network and node resources. Furthermore, SLSP can operate with minimal or no interactions with a key management entity, while the credentials of only a subset of network nodes are necessary for each node to validate the connectivity information provided by its peers.

*b) Secure Data Forwarding Suggested for MANETs*

We will see two major secure message transmission schemes such as Secure Message Transmission and Threshold Cryptography.

*c) Secure Message Transmission*

Secure routing is the pre-requisite for implementing secure data forwarding. The main concept here is forwarding data securily in MANETs in the presence of malicious /untrusted nodes after the discovering the route between the source and target. There are various schemes with various factors proposed for secure data forwarding such as data forwarding based on neighbor's rating, implementing currency system in network for packet exchange, and redundantly dividing and routing message over multiple network routes. For example, Secure Message Transmission (SMT) is a secure data forwarding scheme in which first the active paths are discovered between two nodes using secure routing protocol. Based on B active paths, the message is divided into B different parts such that any A parts can be used to recover this message. These B partial messages are then routed on the identified paths. The destination can recover a message when A or more partial messages are received. Thus, this scheme ensures that the message reaches the destination even if a few packets are dropped in transit. Both the above security solutions are essential to ensure that the MANETs survive even in the presence of malicious or untrusted nodes. Thus, by implementing the above solutions the nodes can communicate securely without relying on all nodes on only one route. The concept of dividing the message using SMT protocol is extended further in the Threshold Cryptography can be implemented to redundantly fragment the message into B parts such that using any T parts the message can be recovered [12, 13, 14]. Now we will see in detail about the this.

*d) Threshold Cryptography*

The main goal of threshold cryptography (TC) is to split a cryptographic operation among multiple users so that some predetermined number of users can perform the desired (cryptographic) operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and/or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key.

The power to sign should then be shared, to avoid abuse and to guarantee reliability. Main aim of TC is to make this possible. Both the schemes ECC and RSA are homomorphic. Therefore, threshold cryptography is applicable and cryptographic operations can be split among multiple users such that any subset comprising of *t* users can perform the desired operation, where *t* is a predefined number. In a *t* out of *n* scheme, any set of *t* users can perform the desired operation, while any set of (t-1) users or less cannot. A cryptographic scheme based on threshold cryptography is secure against an attacker as long as the attacker compromises no more than (t-1) nodes.

Threshold cryptography (TC) [13, 14, 15] involves sharing of a key by multiple individuals called shareholders engaged in encryption/decryption. The aim of this is to have distributed architecture in a hostile environment. Other than sharing keys or working in distributed manner, TC can be implemented to redundantly split the message into B parts such that with T or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over B multiple paths. Threshold schemes generally involve key generation, encryption, share generation, share verification, and share combining algorithms. The basic requirement of any TC scheme is Share generation, for data confidentiality and integrity. Threshold models can be broadly divided into two major First one is single secret sharing threshold e.g. Shamir's *t-out-of-n* scheme based on Lagrange's interpolation and later one is threshold sharing functions e.g. geometric based threshold. These schemes are being used to implement threshold variants of RSA, ElGamal,ECC and Privacy Homomorphism[13, 14]. RSA-TC and ECC-TC has been discussed in the papers [13, 14, 15]. It has been shown that RSA-TC using key sharing is unsuitable in resource constrained MANETs due to high storage, computation, and bandwidth requirements [13].

ECC-TC has been shown to be more efficient for resource constrained MANETs [14]. The authours in paper [14] has used variation of ECC implemented algorithms such as Diffie-Hellman (DH), Menezes Vanstone (MV) and L Ertaul in MANETs. They have performed various comparison tests in different scenarios between these different ECCs'. ECC-DH split before encryption has been proved to be better for resource constraint sender as the encryption timings are lowest. ECC-MV split before encryption has been proved to be best for decryption at the resource constraint receiver as the decryption time is lowest. The encryption and decryption time of ECC- MV and ECCDH has been shown to vary significantly for encryption before split and encryption after split. The encryption and decryption time of ECC-Ertaul has been proved to be more moderate for varying key sizes, T and B for both encryption before split and encryption after split. As a result ECC-Ertaul has been suggested as a best variation of ECC for MANETs in his experiment results [14]. We will show by our observations in our experiments how our Enhanced homomorphic encryption scheme can be used as an alternative for TC for performing the transmission the message securely in MANETs in the next section.

*e) MANETs – New Protocol by Implementing EHES*

In ECC based TC there is an overhead of message splitting using Lagrange Interpolation scheme. In our new scheme keeping the concept of threshold cryptography in mind, the message can be split and encrypt by the our Enhanced homomorphic encryption scheme removing the overhead discussed above by Lagrange Interpolation all together. In our scheme we increase the success rate as compared to RSA based TC. In our study we used the Elgamal, MMH along with our Enhanced Homomorphic encryption scheme to encrypt the message. We also tested their encryption times and execution times. Here we will discuss about our new protocol to transmit the encrypted message securely by using our Enhanced homomorphic encryption schemes. We show that even if a node is compromised, the node will not be able to determine the sensitive information. Even if certain number of nodes are compromised and not send the message, the destination can recover the message.

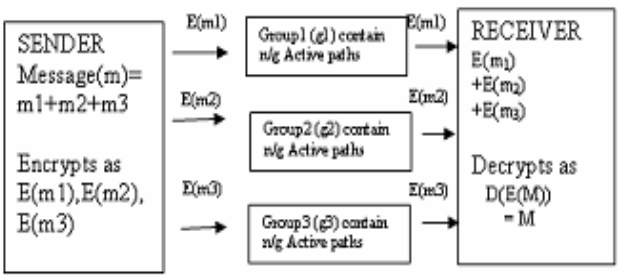



*Figure 1 :* New Protocol in MANETs

In our protocol we are only interested in secured message transmission securely on the already established path not in path establishment from the sender to the receiver. We assume that set of disjoint paths and the key (using any of the key distribution schemes.) have already been established from the sender to receiver by MANETs routing protocols [9, 10] between the sender and receiver.

To transmit the message securely, the idea is to group the set of *n* disjoint paths from sender to receiver into *g* groups, each group having at least *n/g* active disjoint paths. The message to be transmitted is split into number of messages equal to *g* and encrypted using homomorphic encryption schemes [2,3,4,5]. The encrypted split message is sent to each of the *g* groups so that the each group having only one encrypted split message. Each node (router) in the group also will have

the same split message and the entire message cannot get even if node compromised. As Homomorphic encryption schemes are used to encrypt the split message, by performing addition operation on the encrypted split messages the receiver can recover the entire encrypted message and decryption the entire recovered message. This scheme is illustrated in the *Figure 5.1.*

As we know, the nodes are always on the move in MAMETs. There will be scenarios where the intermediate node is out of range or may have been killed or out of the MANET all together. In such cases how would the receiver get all the split messages sent by the sender? It is the serious question. To ensure that the receiver gets all the split messages, the sender sends the same split messages to more than one disjoint paths. Let us assume that there are *n* disjoint paths and the disjoint paths getting the same split message belongs to one group. Let us assume that there are *g* groups of disjoint path, with each group having at least *n/g* disjoint paths. The sender splits a message into *g* splits, and sends each split to each group. The receiver recovers the entire message even if at most *(n/g)-1* disjoint paths are not active. A malicious node cannot recover the entire message as it gets only partial encrypted message. To ensure security the sender does not send more than one split message to the same group of nodes.

*f) Secure data forwarding protocol with EHES implementation results*

We simulated the MANETs environment using the programming language C in the Linix environment. It is done on a system having the Intel® Core™ 2 Duo CPU T5750@2GHz CPU and 3 GB system memory running the Linux kernel –2.6.25-14.fc9.i686 Fedora release -9.

The assumptions during implementation are that there is a sender, receiver and multiple forwarding nodes between them and set of active disjoint paths have already been established from the sender to receiver by the routing protocols. We also assume that the key for homomorphic encryption scheme has already been established between the sender and receiver by using any of the key distribution schemes. The Homomorphic encryption scheme used to encrypt the message at the sender are Enhanced Homomorphic encryption scheme, Mixed multiplicative homomorphism and Elgamal. Using our simulation system, We have tested all the schemes processing timing encryption timings. Here we also tested the following scenarios

1. By varying key sizes 512, 1024 and 2048 bits by keeping the message size fixed.
2. By varying message sizes 500, 1000, 2000 bits as on stream and 100, 250, 500 bits as in another streams with fixed key size ( 512,1024 and 2048 bits).
3. By varying d (splitting times) size 2,4,6,8,10 to find the best d value in the Network as the d is based on number of groups.
4. Here we have considered the following two
   – First one, encryption done after the splitting the message.
   – Second one, Encryption done first and then split the message.

In our simulation the active disjoint paths getting the same message are grouped as one group. Based on *n* active paths the groups *g* are determined. The sender splits the message and encrypts each split message with the one of the homomorphic encryption schemes. In our network, *n* and *g* are fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24})*. The proposed network rate of success is computed as ( *No. of recovered messages by the receiver/No. of sender sent message s*) ** 100 … (5.1)* The rate of success of the network with *n* and *g* fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24})* is determined by randomly killing the nodes. The nodes are killed randomly by using Exponential distribution provided by the function in GSL library [41].

In our implementation, the sender first splits the message into *g* partial messages where each partial message is sent to one of the *g* groups of the MANETs. Each of the partial messages are associated with a unique message split id. All the message split id's of the partial messages forming the entire message is summed up to set up the message split id sum. The message id, message split id, message spit id sum and encrypted partial text is placed in the buffer so that the receiver can recover the entire message from the partial encrypted message. To recover the entire message sent by the sender, the receiver follows two steps. In the first step the receiver adds up all the partial encrypted message whose message id's are same and message split id's sums up to message split id sum. In the second step the receiver decrypts the sum of all partial encrypted messages to recover the entire message. As the same encrypted partial message is sent to all the active paths in the group the receiver is likely to get the same redundant message. The redundant messages will be discarded by the receiver if they have the same message id and message split id. In the next section we look at the encrypted message buffer structure.

*g) The encrypted message buffer structure*

The size of the encrypted message buffer structure sent form sender to receiver varies from one homomorphic encryption to another.

*h) Elgamal*

In elgamal the size of the cipher text increases with the increase in the encryption split *"d"*. So the size of the buffer increases with the increase of the parameter *d* used in encryption.

*i) Mixed Multiplicative Homomorphism (MMH)*

Here also the size of the ciphertext increases with the increase in the encryption split *"d"*. So the size of the buffer increases with the increase of the parameter *d* used in encryption.

*j) Enhanced Homomorphic Encryption Scheme (EHES)*

In all the above mentioned schemes the *message id* field identifies different messages encrypted at the sender. The messages split at the sender is uniquely identified by *message split id*. The sum of all the *message split id* is included in *message split id sum*. The rest of the buffer is used to contain the size of the ciphertext and the ciphertext itself. The size of the ciphertext is essential in reading the ciphertext from the buffer. The receiver recovers the entire message by adding up all the cipher values with the same message id and whose *message split id's* adds up to *message split id sum.*

*k) Experimental Investigations*

We will see the performance results from our simulation.

In MANETs as we know that the nodes have low computational power, Less memory. In such cases we need to find best encryption scheme, which can compute fastly and occupies less memory. In our implementation we do various tests to find a relatively best encryption schemes among our scheme, Elgamal, MMH.

In our simulation we tested and determined the encryption timings of all above mentioned encryption schemes by varying the key size (512, 1024, 2048 bits) and keeping the message size fixed (512 bits). In another test we determined the execution timings of all these same encryption schemes by keeping the key size fixed (512 bits, 1024 bits, 2048 bits) and varying message size. The timings are determined over 200 runs.

*Figure 1* represents the execution timings of *Table 1* in a chart. From *Figure 1*, by observation we found clearly that our Scheme is much faster than other encryption schemes. We also observed that the encryption timings of Scheme MMH and Elgamal increases with the increase in encryption keys but in case of our Scheme the encryption timing remains almost the same with the

| Message size in bits | Elgamal | MMH | EHES |
|---|---|---|---|
| 250 | 89 | 21 | 9 |
| 500 | 105 | 21 | 11 |
| 1000 | 142 | 22 | 8 |

*Table 1 :* Encryption process time of Schemes μSec with key size 512 bit increase in the encryption key size

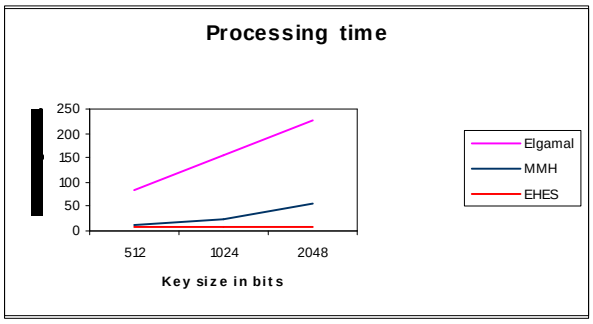



*Figure 1 :* Processing time of Schemes in micro seconds with varying key sizes and fixed message size 512 bits

*Table 1* represents the execution timing of above mentioned schemes in micro seconds by increasing the message size to 100, 250 and 500 bits and by keeping the key size fixed (512 bits). *Figure 1* graph represents the execution timings of *Table 1.* From *Figure 2*, it is very clear that our Scheme is much faster than other two Schemes. We also found that the encryption timing of other Schemes increases with the increase in message size we also observed that the Message size encryption timings of our Scheme remains almost the same with the increase in the message size.

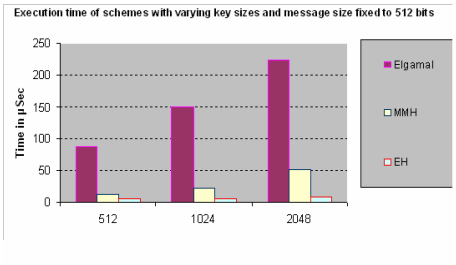



*Figure 2 :* Encryption process time of Schemes in μSec with key size 512 bit

*Table 3* represents the execution timings of the same encryption schemes in micro seconds by increasing the message size (250, 500 and 1000 bits ) and by keeping the key size fixed ( 1024 bits ). *Figure 3* graph represents the execution timings of *Table 37.*. From *Figure 5.4*, we can say that our Scheme is much faster than other schemes. We also observed that the encryption timings of Elgamal increases with the increase in message size and the encryption timings of our Scheme and MMH remains almost the same with the increase in the message size.

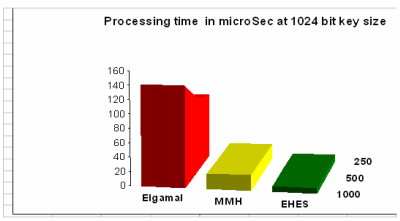


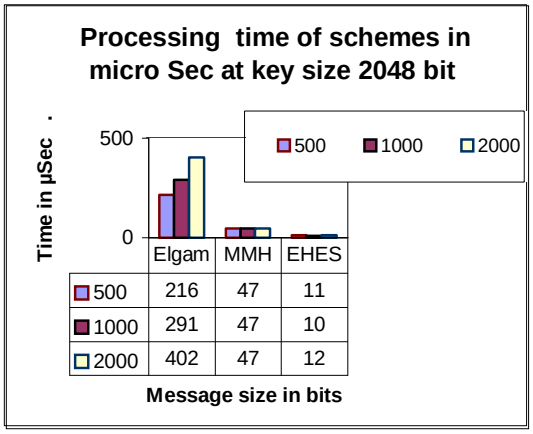

*Figure 3 :* Processing time of schemes in μSec at 1024 bit key size

*Table 3 :* Processing time of schemes in μSec at 1024 bit key size

| MESSAGE SIZE IN BITS | Elgamal | MMH | Our Scheme EHES |
|---|---|---|---|
| 100 | 72 | 11 | 7 |
| 250 | 76 | 11 | 7 |
| 500 | 87 | 11 | 7 |

We have also computed the execution timings of Schemes in micro seconds by increasing the message size (500, 1000 and 2000 bits) and by keeping the key size fixed (2048 bits). graph 4 shows the execution timings computed, it is observed that our Scheme is much faster than other schemes as shown in chart and that the encryption timings of Elgamal Schemes increases with the increase in message size and the encryption timings of our Scheme and MMH remains almost the same with the increase in the message size.

*Figure 4 :* Processing time of schemes in μSec at key size 2048 bit




From the graphs and corresponding *Tables* it is observed that our Scheme is much faster than other schemes. We also observed from graph (*Figure 2)* that the encryption timings of other Schemes increases with the increase in encryption keys but the encryption timing of our Scheme remains almost the same with the increase in the encryption key size. From graphs and corresponding *Tables* we also can say that the encryption timings of Elgamal Scheme increases with the increase in message size. However the encryption timings of MMH and our Schemes remains almost the same with the increase in the message size.

*I) Experimental Results of our New Protocol with our new scheme*

In MANETs we know that the nodes are always on the move and there may be scenarios where the active path may no longer be active with this result, the receiver may not receive all the packets sent by the sender. *Figure 5 graph* depicts the rate of success of the networks with *n* active paths and *g* groups fixed to *(12,{2,6,12})*, *(16,{2,8,16})* and *(24,{2,12,24}),* by randomly killing the nodes. The nodes in the networks are killed randomly by using Exponential distribution provided by the function in GSL library [41].

The networks with *n* and *g* fixed to *(12,{2,6,12})* defines 3 sets of networks with the I network having *12* active paths, *2* groups and 6 active paths in each group, II network with *12* active paths, 6 groups and *2* active paths in each group and III network with *12* active paths, *12* groups and *1* active path in each group. The networks with *n* and *g* fixed to *(16,{2,8,16})* defines 3 sets of networks with I network having *16* active paths, *2* groups and 8 active paths in one group and *8* active paths in another group, II network with *16* active paths, 8 groups and 2 active paths in one group and *2* active paths in remaining groups and III network with 16 active paths, *16* groups and *1* active path in each group. The networks with *n* and *g* fixed to *(24,{2,12,24})* defines 3 sets of networks with I network having *24* active paths, *2* groups and *12* active paths in each group, II network with *24* active paths, *12* groups and *2* active paths in each group and III network with *12* active paths, *24* groups and *1* active path in each group. From graph shown in the *Figure 5.7* it is clear that the rate of success increases by reducing the number of groups in the network. This is because by reducing the number of groups in the network we would increase the number of active paths in each group. Just one partial message from each group is enough to recover the entire message. From *Figure 5.7* we see that the rate of success is 100% with *g=2* and *n=12,16,24.* This is because by increasing the number of paths in each group, the probability of one path in each group remaining active is high and with it the probability of recovery of the message at the receiver is also high. The rate of success gradually decreases with the gradual increase in the number of groups in the network. With *g=n* we see that rate of success is lesser than 50%. Therefore to get the rate of success as 100% in the network it is better to reduce the number of groups, thus increasing the number of active paths in each group.

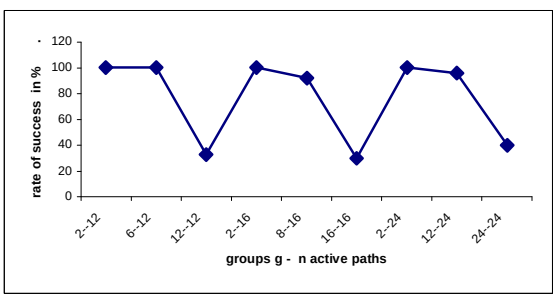



*Figure 5 :* Rate of success of the I,II & III Network

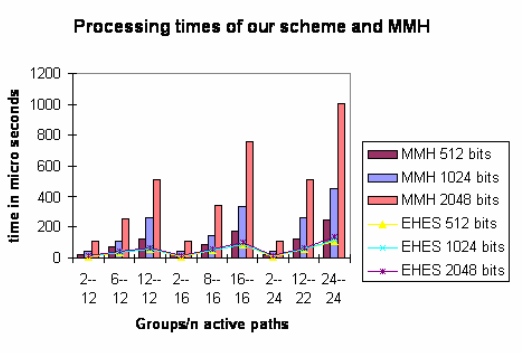



*Figure 6 :* Processing timing ( in micro seconds ) of our Scheme and MMH in micro Seconds varying key sizes 512, 1024 & 2048

*Table 4 :* Processing timing of our Scheme and MMH in micro Seconds varying key sizes 512, 1024 & 2048

| | **MMH Scheme** with key size in bits | | | **Our Scheme** with key size in bits | | |
|---|---|---|---|---|---|---|
| groups out of n active paths | 512 | 1024 | 2048 | 512 | 1024 | 2048 |
| 2—12 | 25 | 43 | 112 | 10 | 11 | 14 |
| 6—12 | 70 | 112 | 254 | 34 | 35 | 40 |
| 12—12 | 124 | 257 | 515 | 55 | 60 | 68 |
| 2—16 | 25 | 43 | 112 | 10 | 11 | 14 |
| 8—16 | 85 | 147 | 339 | 50 | 50 | 55 |
| 16—16 | 177 | 330 | 760 | 85 | 90 | 103 |
| 2—24 | 25 | 43 | 112 | 10 | 11 | 14 |
| 12—22 | 124 | 257 | 515 | 55 | 60 | 68 |
| 24—24 | 243 | 457 | 1008 | 112 | 115 | 140 |

In our proposed protocol in MANETs the sender splits the message with respect to the value *g*. The sender using the homomorphic encryption scheme then encrypts all the split messages. As the number of splits at the sender is equal to the value *g* the total encryption timing of all the split messages increase with the value *g*. *Figure 5.7 & 5.8* and the corresponding *Tables* represent the total encryption timings of all the split messages. From the *Figures* it is observed that the total encryption timing increases with the value *g*. Also from *Figures* we found that our Scheme is the much fastest encryption scheme, followed by other Schemes.

## VII. Discussion of Results

By using our proposed new scheme for secured transmission of message in the area MANETs as an alternative to TC, we eliminate the overhead of the schemes associated with Lagrange Interpolation Scheme. As MANETs are grouped mode even if one compromised the entire message would not be revealed. For this the attacker needs to compromise atleast *g* nodes to get full message for that he has to get one node from each group *g* and know the encryption keys to decrypt the message. The success rate of our proposed new scheme is 100% if there are more number of active paths in each group of the network. From our implementation results it is clear that our scheme is the fastest homomorphic encryption scheme in comparison with other schemes.

## References Références Referencias


1. J. Domingo-Ferrer. "A Provably Secure Additive and Multiplicative Privacy Homomorphism". Information Security Conference, LNCS 2433, pp 471–483, January 2002.
2. J. Domingo-Ferrer, "A new Privacy Homomorphism and Applications", Elsevier North-Holland, Inc, 1996.
3. J. Domingo-Ferrer and J. Herrera- Joancomarti. "A privacy homomorphism allowing field operations on encrypted data". I Jornades de Matematica Discreta I Algorismica, Universitat Politecnica de Catalunya, March 1998.
4. Hyungjick Lee, Jim Alves- Foss, Scott Harrison, "The use of Encrypted Functions for Mobile Agent Security", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.
5. J. Girao, D. Westhoff and M. Schneider. Concealed data aggregation in wireless sensor networks. ACM WiSe04 – poster, in conjunction with ACM MOBICOM 2004, October 2004.
6. J. Girao, D. Westhoff and M. Schneider. CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. 40th International conference on communications, IEEE ICC 2005, May 2005.
7. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans". On Information Theory, 1986.
8. William Stallings "Network Security Essentials", Second Edition, Prentice Hall 2006, pp.3.
9. P. Papadimitratos, Z. J. Haas "Secure Data Transmission in Mobile Ad Hoc Networks," ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.
10. Mithun Acharya, Joao Girao and Dirk Westhoff. "Secure comparison of encrypted data in wireless sensor networks". In 3rd Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Trentino, Italy, April 2005. WiOpt2005.
11. P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan. 27- 31, 2002.
12. P. Papadimitratos, Z. J. Haas, and P. Samar, "The Secure Routing Protocol (SRP) for Ad Hoc Networks," Internet Draft, draft papadimitratos-secure-routingprotocol-00.txt, Dec. 2002.

13. P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proceedings of the IEEE CS Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, Jan. 2003.
14. L. Ertaul, N. Chavan, "Security of Ad Hoc Networks and Threshold Cryptography", 2005 International Conference on Wireless Networks, Communications and Mobile Computing, Wirelesscom 2005, MobiWac 2005, June 2005, Maui, Hawaii.
15. L. Ertaul, N. Chavan, "Elliptic Curve Cryptography based Threshold Cryptography (ECCTC) Implementation for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, pp 48-61 April.
16. L. Ertaul, W. Lu, "ECC based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in Mobile Ad Hoc Networks (MANET) I", Proc. Of Networking 2005 International Conference, May 2005, University of Waterloo, Ontario, CA.
17. Makoto Yokoo, Koutarou Suzuki, "Secure Multi-agent Dynamic Programming based on Homomorphic Encryption and its Application to Combinatorial Auctions", Proceedings of the First International joint Conference on Autonomous Agents and Multiagent systems( AAMAS), 2002.
18. N. Koblitz, "ECC", Math. Of Computation, v. 48, 1987, pp. 203-209.
19. A. J. Menezes, D. B. Johnson, "ECDSA: An Enhanced DSA", Invited Talks – 7th Usenix Sec., Symp., Jan., 1998, pp. 33-43.
20. Certicom Corp., "Certicom ECC Tutorials".
21. Certicom Corp., "Remarks on the Security of the ECC systems", ECC White Papers, uly 2000.
22. K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, vol. 11, no.1, pp. 62-67, February 2004.
23. L. Ertaul, W. Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)", Proc. Of the Networking 2005 International Conf., May 2005, University of Waterloo, Ontario, CA.
24. L. Ertaul, "Cryptography Lecture Notes", California State University, East Bay, http://www.mcs.csueastbay.edu/~lertaul/
25. D. Wagner, "Cryptanalysis of an algebraic privacy homomorphism", In proceedings of the 6th information security conference (ISC03), Bristol, UK, October 2003.
26. William Stallings "Cryptography and Network Security", Third Edition, Chinese Remainder Theorem (CRT), pp. 245-247. Extended Euclid's Algorithm, pp. 119-220.
27. Jung Hee Cheon, Hyun Soon Nam, "A Cryptanalysis of the Original Domingo-Ferrer's Algebraic Privacy Homorphism", http://eprint.iacr.org/2003/221.pdf
28. William Stallings "Cryptography and Network Security", Third Edition, The RSA Algorithm, pp. 268-278.
29. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, Nov., 1976, pp. 644-654.
30. L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Comms of the ACM, v. 21-n.2, February 1978, pp. 120-126.
31. Yang Xiao. "Security in Sensor Networks", Auerbach Publications, 2007, pp. 275-290.
32. Dirk Westhoff, Joao Girao, Mithun Acharya. "Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution and routing adaptation". IEEE Transactions on Mobile Computing, October 2006.
33. R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms", in Foundations of Secure Computation, R. A. DeMillo et al., Eds. New-York: Academic Press, 1978, pp. 169-179.
34. Rakesh Agrawal., Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu: "Order-Preserving Encryption for Numeric Data". SIGMOD Conference 2004, pp 563-574.
35. J. Rissanen. "Stochastic complexity in statistical inquiry". World Scientific Publication, 1989.
36. L.Ertaul, Vaidehi, "Finding Minimum Optimal Path Securely Using Homomorphic Encryption Schemes in Computer Networks", The 2006 International Conference on Security & Management, SAM'06, June, Las Vegas.
37. P. Paillier. "Trapdooring Discrete Logarithms on Elliptic Curves over Rings". ASIACRYPT, pp 573–584, 2000.
38. Willian Stallings, "Cryptography and Network Security, Principles and Practices." Fourth Edition, Prentice Hall 2006, pp.312.
39. T. Okamoto and S. Uchiyama. "A New Public-Key Cryptosystem as Secure as Factoring". EUROCRYPT, pp 308–318, 1998.
40. GSL manual, http://www.gnu.org/software/gsl/manual/html_node/Random-Number-Distributions.html
41. Fork document, http://www.csl.mtu.edu/cs4411/www/NOTES/process/fork/create.html
42. W. Richard Stevens, "Unix Network Programming, Volume 2, Interprocess Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Message Queues, pp 75-126.
43. W. Richard Stevens, "Unix Network Programming, Volume 2, Inter process Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Shared memory, pp 325-342.

44. W. Richard Stevens, "Unix Network Programming, Volume 2, Interprocess Communication", Second Edition, Addison Wesley Longman Singapore Pte. Ltd 1999, Posix Semaphore, pp 219-279.
45. GMP manual, "http://gmplib.org/manual/".
46. Cohen S psychological models of the role of social support in the etiology physical disease. Health Psychology 7 (1988) 269-297.
47. Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). http://www.cms.hhs.gov/hipaaGenInfo.
48. R. Agrawal, D. Asonov, M. Kantarcioglu and Y. Li. Sovereign Joins. In *ICDE 2006,* page 26. IEEE Computer Society, 2006.
49. F. Emekc¸ i, D. Agrawal, A. E. Abbadi and A. Gulbeden. Privacy Preserving Query Processing Using Third Parties. In *ICDE 2006,* page 27. IEEE Computer Society, 2006.
50. Dan Boneh, Ran Canetti, Shai Halevi and Jonathan Katz. Chosenciphertext security from identity-based encryption. SIAM J. Comput., 36(5):1301{1328, 2007.
51. M. Naor, B. Pinkas and R. Sumner. Privacy Preserving Auctions and Mechanism Design. In *Electronic Commerce 1999,* pages 129–139. ACM, 1999.
52. BRUCE SCHNEIER, "Applied cryptography – Protocols, Algorithms and Source Code in C" Second Edition.
53. Levent ertaul and Weimin Lu, "ECC Based Thresold Cryptography for Secure Data forwarding and Secure Key Exchange in MANET(I)." IFIP International federation for Information Processing – Networking 2005, LNCS 3462, pp 102- 113, 2005.
54. Mikhail J. Atallah, Keith B. Frikken, Marina Blanton, "Private Combinatorial Group Testing" *ASIACC'* 08, March 18-20, Tokyo, Japan 2008 ACM 978-1-59593-979-1/08/0003.
55. Human gemome project. http://genomics.energy.gov.
56. I. Damg°ard, M. Fitzi, E. Kiltz, J. B. Nielsen, and T. Toft. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In Proceedings of the third Theory of Cryptography Conference, TCC 2006, volume 3876 of Lecture Notes in Computer Science, pages 285–304. Springer-Verlag, 2006.
57. *Dr. Abu Sayed Md. Latiful Hoque and Gahangir Hossain,* "PIR WITH PCACHE: ANEWPRIVATE INFORMATION RETRIEVAL PROTOCOL WITH IMPROVED PERFORMANCE" Malaysian Journal of Computer Science, Vol. 21(1), 2008.
58. Juan Ramón Troncoso-Pastoriza, Stefan Katzenbeisser Mehmet Celik," Privacy Preserving Error Resilient DNA Searching through Oblivious Automata" *CCS'07,* October 29–November 2, 2007, Alexandria, Virginia, USA.2007 ACM 978-1-59593-703-2/07/0011.
59. Zhiqiang Yang, Sheng Zhong, Rebecca N. Wright, "Towards Privacy Preserving Model Selection" Preproceedings version, PinKDD'07, August 12, 2007, San Jose, California, USA.
60. R. Agrawal and R. Srikant. Privacy preserving data mining. In *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 439–450. ACM Press, May 2000.
61. J. P. Prins, Z. Erkin, and R. L. Lagendijk, *"Research Article* Anonymous Fingerprinting with Robust QIM Watermarking Techniques" Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2007, Article ID 31340, 13 pages doi:10.1155/2007/31340.
62. C. Orlandi, A. Piva andM. Barni, *"Research Article* Oblivious Neural Network Computing via Homomorphic Encryption" Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2007, Article ID 37343, 11 Pages doi:10.1155/2007/37343.
63. Bart Goethals1, Sven Laur2, Helger Lipmaa2 and Taneli Mielik¨ainen1, "On Private Scalar Product Computation for Privacy-Preserving Data Mining" Helsinki University of Technology, Finland.
64. Thomas B. Pedersen, Erkay Savas and Yucel Saygin, "SECRET SHARING VS. ENCRYPTION-BASED TECHNIQUES FOR PRIVACYPRESERVING DATA MINING" Joint UNECE/Eurostat work session on statistical data confidentiality (Manchester, United Kingdom, 17-19 December 2007).
65. Mikhail J. Atallah, Florian Kerschbaum, "Secure and Private Sequence Comparisons "*WPES'03,* October 30, 2003, Washington, DC, USA. ACM \ 15811377 61/03/0010.
66. R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms" in R.A. DeMillo et al. eds., Foundations of Secure Computation (Academic Press, New York, 1978) 169-179.
67. E.F. Brickell and Y. Yacobi, "On privacy homomorphisms" in D. Chaum et al eds., Advances in Cryptology-Eurocrypt'87 (Springer, Berlin, 1988) 117- 125.
68. J. Domingo-Ferrer, "A new privacy homomorphism and applications" in Information Processing Letters, vol. 60, no. 5, pp. 277-282, Dec. 1996.
69. N. Ahituv, Y. Lapid and S. Neumann, "Processing encrypted data", Communications of the ACM, vol. 20, no. 9, pp. 777-780, Sep. 1987.
70. C. Ding, D. Pei and A. Salomaa, "Chinese remainder theorem," 1996.
71. J. Domingo-Ferrer and J. Herrera- Joancomarti, "A privacy homomorphism allowing field operations on encrypted data," *I Jornades de Matematica Discreta*

*i Igorismica, Universitat Politecnica de Catalunya*, 1998.
72. C. Negus, "Linux Bible: Boot Up to Fedora, KNOPPIX, Debian, SUSE, Ubuntu and 7 Other Distributions," 2006.
73. D. Westhoff, J. Girao and A. Sarma, "Security Solutions for Wireless Sensor Networks," *Nec Technical Journal*, vol. 1, 2006.
74. J. Girao, D. Westhoff, M. Schneider, N. E. C. E. Ltd, and G. Heidelberg, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," *Communications, 2005. ICC 2005. 2005 IEEE International Conference on,* vol. 5, 2005.
75. D. Integrity, P. Sakarindr and N. Ansari, "Security Services IN Group Communications OVER Wireless Infrastructure, Mobile Ad Hoc AND Wireless Sensor Networks," *IEEE Wireless Communications,* pp. 9, 2007.
76. Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, "Security Solutions for Wireless Sensor Networks" http://www.nec-display.com/products/model/lcd2180w _led/index.html
77. I. F. Blake, G. Seroussi and N. P. Smart. Elliptic curves in cryptography. Cambridge University Press, New York, NY, USA, 1999.
78. Alessandro Sorniotti, Laurent Gomez, Konrad Wrona and Lorenzo Odorico "Secure and Trusted innetwork Data Processing in Wireless Sensor Networks: a Survey" Journal of Information Assurance and Security 2 (2007) 189 –199.
79. Zhiqiang Yang1, Sheng Zhong2 and Rebecca N. Wright1, "Privacy- Preserving Queries on Encrypted Data⋆ In Proceedings of the 11th European Symposium On Research In Computer Security (Esorics), 2006.
80. **Mufutau Akinwande, "Advances in Homomorphic Cryptosystems"** *Journal of Universal Computer Science, vol. 15, no. 3 (2009), 506-522, 1/2/09 J.UCS.*
81. M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.
82. Brett Hemenawy and Rafail Ostrovsky, University of Michigan "On Homomorphic Encryption and Chosen-Cipher text Security" in the Proceedings of PKc 2012.
83. C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal,* vol. 28, pp. 656–715, 1949.
84. R. Rivest, L. Adleman and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.
85. R. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In Comm. of the ACM, 21:2, pages 120–126, 1978.
86. A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.
87. S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
88. T. ElGamal, "A prublic key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (CRYPTO '84), vol. 196 of Lecture Notes in Computer Science, pp. 10–18, Springer, New York, NY, USA, 1985.
89. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT'99), vol. 1592 of Lecture Notes in Computer Science, pp. 223–238, Springer, New York, NY, USA, 1999.
90. C. Fontaine, F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007, p.1-15, January 2007.
91. D. Micciancio and O. Regev. Post- Quantum Cryptography, chapter Lattice based Cryptography. Springer, 2008.
92. C. Gentry. Fully homomorphic encryption using ideal lattices. In Proc. of STOC, pages 169178. ACM, 2009.
93. N. P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. Lecture Notes in Computer Science, 2010, Volume 6056/2010, 420-443.
94. M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In Advances in Cryptology – Eurocrypt 2010, Springer LNCS 6110, 24–43, 2010.
95. Group Theory by "J S Milne" Version 3.12 April 9, 2012.
96. Brett Hemenway and Rafail Ostrovsky University of Michigan UCLA "On homomorphic Encryption and Chosen-Ciphertext Security".
97. Jibang Liu, Yung-Hsiang Lu, and Cheng-Kok Koh "Performance Analysis of Arithmetic Operations in Homomorphic Encryption".
98. Craig Gentry "A FULLY HOMOMORPHIC ENCRYPTION SCHEME".
99. Liangliang Xiao, Osbert Bastani, I-Ling Yen, "An Efficient Homomorphic Encryption Protocol for Multi-User Systems".