Use of BE technique for Enterprise Social networking with Document security

Prof.A.V.Pande

Assistant Professor, Sipna College of Engineering and Technology, Amravati

Department of Computer Science and Engineering, Sant Gadge Baba Amravati University

ankita.pande2@gmail.com

Prof.Y.A.Thakare

Assistant Professor, Sipna College of Engineering and Technology, Amravati

Department of Computer Science and Engineering, Sant Gadge Baba Amravati University

yugathakare@gmail.com

Abstract—**Enterprise social network sites (ESNSs) are increasingly being introduced into large multinational organizations .They offer attractive means for digital social interactions and information sharing but also raise a number of security and privacy issues. While social networks allow users to share data amongst themselves, they currently do not provide any mechanism about sharing secured data amongst the multiple users and also enforce concerns about the leakage of the confidential documents being shared. To this end, we propose an approach to secure the data being shared amongst multiple users and also formulate a technique to avoid leakage of the confidential documents of the company. We propose Broadcast Encryption technique to deliver encrypted content over a broadcast channel in such a way that only qualified users can decrypt the document. The group members will receive a unique group key on their registered email-id's which will be later used by them to decrypt the document. Another technique which we propose is Leakage Detection & Prevention. In this technique we generate a hash value of the uploaded document using Secure Hash Algorithm (SHA) which will produce a 160 bit hash value known as message digest – typically rendered as hexadecimal number. If any employee is trying to share any document leakage will get identified using hash value of the document and prevented by the system. Thus the main objective of our project is to enhance security of the content being shared across the multiple users and prevent leakage of the confidential doc's.**

Keywords— **Secure hash Algorithm(SHA), Enterprise social network sites (ESNSs), Broadcast Encryption technique, Cryptography, message digest**

I. Introduction

In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has become a critical feature for thriving networks and in military alike. Cryptography is a well-known and widely used technique that manipulates information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields they are used to protect military messages, E-mails, credit card information, corporate data, personal files, etc.

We propose Broadcast Encryption technique to deliver encrypted content over a broadcast channel in such a way that only qualified users can decrypt the document. The group members will receive a unique group key on their registered email-id's which will be later used by them to decrypt the document. Another technique that we propose is Leakage Detection & Prevention. In this technique, we generate a hash value of the uploaded document using Secure Hash Algorithm (SHA), which will produce a 160-bit hash value known as message digest – typically rendered as hexadecimal number. If any employee is trying to share, any document leakage will get identified using hash value of the document and prevented by the system.

Enterprise social network sites (ESNSs) are increasingly being introduced into large multinational organizations .They offer attractive means for digital social interactions and information sharing but also raise a number of security and privacy issues. While social networks allow users to share data amongst themselves, they currently do not provide any mechanism about sharing secured data amongst the multiple users and enforce concerns about the leakage of the confidential documents being shared. To this end, we propose an approach to secure the data being shared amongst multiple users and formulate a technique to avoid leakage of the confidential documents of the company.

To achieve this we have used Broadcast encryption technique in our project. Broadcast encryption. Broadcast encryption is the cryptographic problem of delivering encrypted content over a broadcast channel in such a way that only qualified users can decrypt the content. This algorithm will be used to encrypt and decrypt documents.

Another algorithm that we have used is, SHA algorithm .This algorithm will be used to find out hash value of uploaded document.

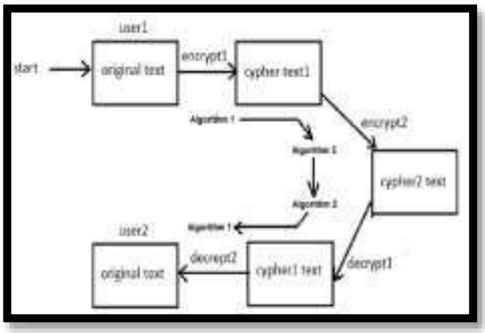


Fig. 1.1: Flow Diagram for Basic Encryption and Decryption Operation

1.1 Objective

The main goal of this project is to develop an accessible and secure web application so that to enhance document security and provide leakage detection.

- To develop online enterprise social networking application for company.
- To implement broad cast encryption technique for document security.
- To develop a leakage detection & prevention system.

II. LITERATURE REVIEW

A literature survey is a discussion of the literature in a given area of the study. It is concise overview of what has been studied, argued and established about a topic, and it is usually organized chronologically or thematically. Following is the listing of the things that were required to be studied for our project.

In previous paper, presenting a new block based symmetric cryptography algorithm. In this technique using a random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Basically In this technique a block based substitution method will use. In the present technique, they provide for encrypting message multiple times. The proposed key blocks contains all possible word comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key blocks will depend on text key entered by the user. Our proposed system using 512 bit key size to encrypt a text message. It wills us very difficult to find out two same massages using this parameter.

To decrypt any file one has to know exactly what the key blocks is and to find the random blocks theoretically one has to apply 2256 trial run and which is intractable. Initially that technique is only possible for some files such as Microsoft word file, excel file, text file.

2.1 Encryption Approach Used:

The symmetric encryption approach is divide in two type one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here we are choosing block cipher type because its efficiency and security. In the proposed technique, we have a common key between sander and receiver, which is known as private key. PrivateKey concept is the symmetric key concepts where plain text is converting into encrypted text known as cipher text using private key where cipher text decrypted by same private key into plane text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain private information. Basic concept of symmetric cryptography is shown in the following figure.

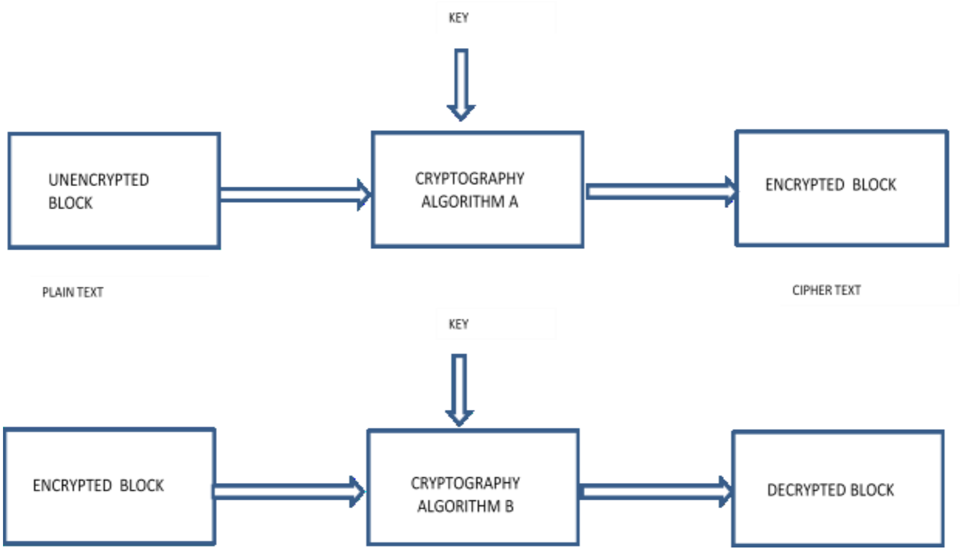


Fig. 2.1: Basic Concept for Symmetric Cryptography

2.2 Data Encryption Standard (DES):

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography Researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure (Known as a feistel network).As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time5 (be they plaintext or cipher text). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. The least significant bit of each byte is used either for parity (odd for DES) or for set arbitrarily and does not increase the security in any way. All blocks are numbered from left to right which makes the eight bit of each byte the parity bit. Once a plain-text message is received to be encrypted, it is arranged into 64-bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. Multiple permutations and substitutions are incorporated throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. However, it is generally accepted that the initial and final permutations offer little or no contribution to the security of DES and in fact some software implementations omit them.

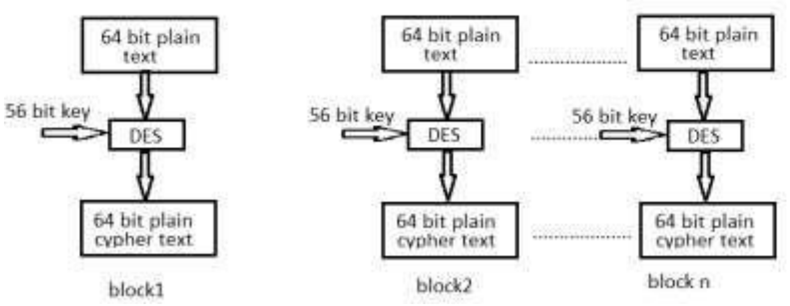


Fig. 2.2: Conceptual working of DES

Figure 2.2 shows the sequence of events that occur during an encryption operation. DES performs an initial permutation on the entire 64-bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a Round of which there are 16 (the subscript i in Li and Ri indicates The current round). Each of the rounds are identical and the effects of increasing their Number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly, these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the cipher text and either the plaintext or key. At the end of the16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation the output of this final permutation is the 64 bit cipher text.

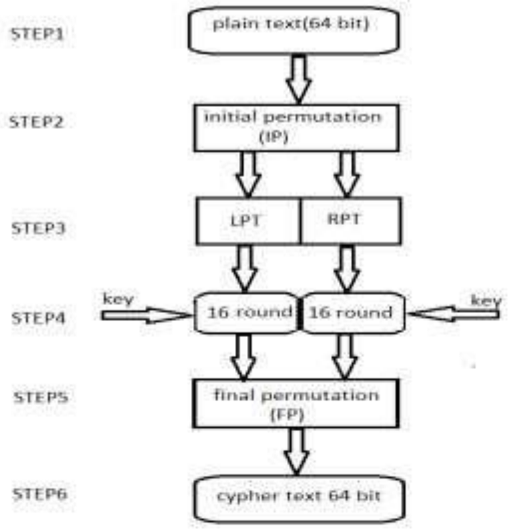


Fig. 2.3: Broad level Steps in DES

2.3 SHA:

SHA is a cryptographic hash function designed by National Security Agency (NSA) and published by NIST as US Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. The three SHA algorithms are structured differently and are distinguish as SHA-0, SHA-1 and SHA-2.

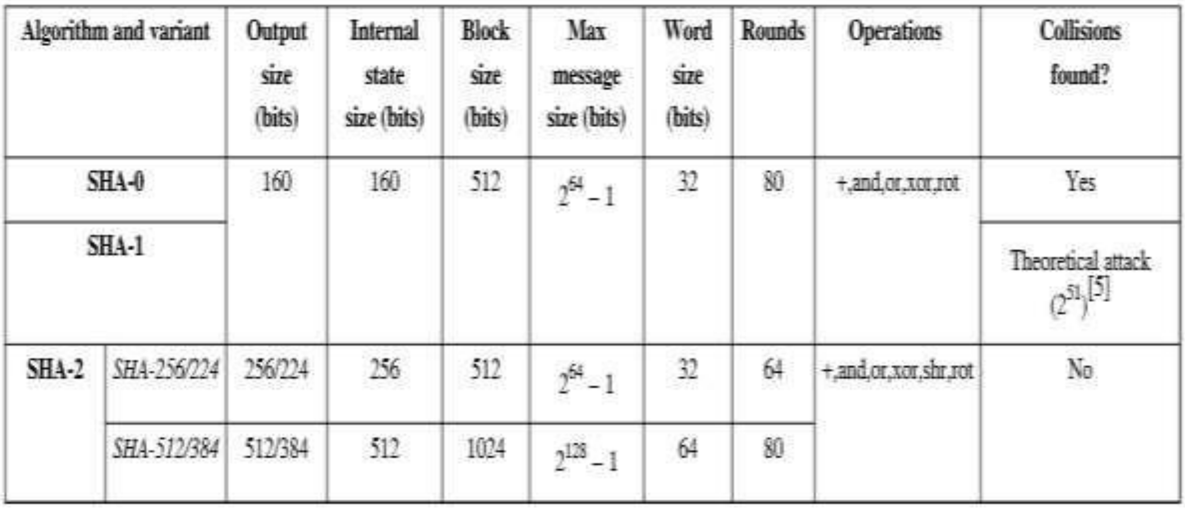
For a hash function for which L is the number of bits in the message digest, finding a message that corresponds to a given message digest can always be done using a brute force search in approximately 2^L evaluations. This is called a preimage attack and may or may not be practical depending on L and the particular computing environment. However, a collision, consisting of finding two different messages that produce the same message digest, requires on average only about 1.2 × $2^{L/2}$ evaluations using a birthday attack. Thus, the strength of a hash function is usually compared to a symmetric cipher of half the message digest length. SHA-1, which has a 160-bit message digest, was originally thought to have 80-bit strength.

In 2005, cryptographers Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu produced collision pairs for SHA-0 and have found algorithms that should produce SHA-1 collisions in far fewer than the originally expected 2 evaluations.

Some of the applications that use cryptographic hashes, like password storage, are only minimally affected by a collision attack. Constructing a password that works for a given account requires a preimage attack, as well as access to the hash of the original password, which may or may not be trivial. Reversing password encryption (e.g. to obtain a password to try against a user's account elsewhere) is not made possible by the attacks. (However, even a secure password hash cannot prevent brute-force attacks on weak passwords.)

In the case of document signing, an attacker could not simply fake a signature from an existing document: The attacker would have to produce a pair of documents, one innocuous and one damaging, and get the private key holder to sign the innocuous document. There are practical circumstances in which this is possible; until the end of 2008, it was possible to create forged SSL certificates using an MD5 collision.

Due to the block and iterative structure of the algorithms and the absence of additional final steps, all SHA functions (except SHA-3) are vulnerable to length-extension and partial-message collision attacks. These attacks allow an attacker to forge a message signed only by a keyed hash SHA (message || key) or SHA (key || message)—by extending the message and recalculating the hash without knowing the key. A simple improvement to prevent these attacks is to hash twice: SHA(message) = SHA (SHA (0^b || message)) (the length of 0^b, zero block, is equal to the block size of the hash function).



Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operations	Collisions found?
SHA-0		160	160	512	$2^{64}-1$	32	80	+,and,or,xor,rot	Yes
SHA-1									Theoretical attack (2^{51})[5]
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64}-1$	32	64	+,and,or,xor,shr,rot	No
	SHA-512/384	512/384	512	1024	$2^{128}-1$	64	80		

Fig. 2.4: Characteristics of SHA algorithms

III.IMPLEMENTATION

Systems implementation is the construction of the new system and the delivery of that system into production. The development process has started with the definition of set of system requirements, main functionalities and the analysis of possible development approaches.

3.1 Proposed Work:

Enterprise social network sites (ESNSs) are increasingly being introduced into large multinational organizations .They offer attractive means for digital social interactions and information sharing but also raise a number of security and privacy issues. While social networks allow users to share data amongst themselves, they currently do not provide any mechanism about sharing secured data amongst the multiple users and enforce concerns about the leakage of the confidential documents being shared. To this end, we propose an approach to secure the data being shared amongst multiple users and formulate a technique to avoid leakage of the confidential documents of the company.

We propose Broadcast Encryption technique to deliver encrypted content over a broadcast channel in such a way that only qualified users can decrypt the document. The group members will receive a unique group key on their registered email-id is which will be later used by them to decrypt the document. Another technique, which we propose, is Leakage Detection & Prevention. In this technique, we generate a hash value of the uploaded document using Secure Hash Algorithm (SHA), which will produce a 160-bit hash value known as message digest – typically rendered as hexadecimal number. If any employee is trying to share, any document leakage will get identified using hash value of the document and prevented by the system.

3.1.1 Reasons for Use these Approaches for Encryption and Decryption:-

- Each trading partner can use the same encryption algorithm no need to develop and exchange secret algorithms.
- Security is dependent on the length of the key.
- High rates of data throughput.
- Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms.
- Symmetric-key and asymmetric-key ciphers can be composed to produce stronger ciphers.

3.2. Role of Module

There are five roles of application which are as follows:-

3.2.1. Company admin:-Company Admin performs following tasks:

- Login/logout
- Create new branches
- Create branch manager login
- Create groups

- Accept employee’s group joining request
- View group member’s details
- View branch log

The company admin is the first user of the system and having highest autority. Company Adin can do all the tasks mention above. Company Admin can create groups and even can destroy it. He is having the power of creating new branvches in the company if required. He is having access to all the group member details.

3.2.2. Social activities management:-This module is responsible for the following tasks:

- Group management
  - Create new group
  - Delete group
  - Accept group joining requests
  - group key generation and notification
- If any user wants to create a group, his higher authority must approve the group .
- If higher authority declines the group creation request, the group will be deleted.
- Send group joining request to group admin.
- Polling
- Post updates
- Reply to updates posted by other user
- View group communication
- Get group key on email
- Every user will receive different key for his group
- Share documents for group
- Decrypt group documents

3.2.3. BE (Broadcast Encryption) algorithm

Following is the BE (Broadcast Encryption) algorithm in the system that we have used:

Step 1: Read file into byte array b[].
Step 2: Generate group and group member’s attributes as per the access permission.
Step 3: Generate key to encrypt attributes k.
Step 4: Generate key K to encrypt document.
Step 5: Include K in attributes.
Step 6: Encrypt attributes using key k
Step 7: EncA[]=A[]^k.
Step 8: Encrypt b[] using key K.
Step 9: Encb[]=b[]^K.
Step 10: Merge EncA[] and Encb[].
Step 11: EncDoc=EncA[] U Encb[].
Step 12: Store EncDoc[] in file .
Step 13: Store encrypted file on server.

3.2.4. Broadcast encryption technique

- Any user wants to share any document with particular group/ subgroup, he can share the same using BE technique.
- In BE technique, group member’s will receive their group key on registered email id respectively.
- At the time of file decryption, group member have to specify his group key.
- If specified group key is valid, system will verify session parameters to confirm that the user belongs to the specified group.
- If user’s identity satisfied, he can download the decrypted document.

3.2.5. Broadcast decryption technique

- Decrypt header of the requested document using group key specified by the employee
- Check whether the employee have access permission or not
- If employee attributes match with header attributes, document key will be extracted from document header
- Using document key, the document will be decrypted and deliver it to user

3.2.6. Broadcast decryption Algorithm:-Following is the decryption algorithm in the system that we have used:

```
Step 1: Read encrypted document into bytes docb[]
Step 2: Initialize Encheader[]=docb[0-headerlen]
Step 3: Decrypt request document header Encheader[]
Step 4: Generate header key k
Step 5: Header[]= EncHeader[]^k
Step 6: If (user attribute exist in Header[]) then
            o   Initialize K= Header[Dockey]
            o   Initialize Encdocb[]=docb[docb.len-headerlen]
Step 7: Decrypt Encdocb[] using key K
Step 8: DecDoc[]=Encdocb[]^K
Step 9: Convert DecDoc[] into file
Step 10: Deliver decrypted file to user
```

3.2.7. Upload / Download Working:

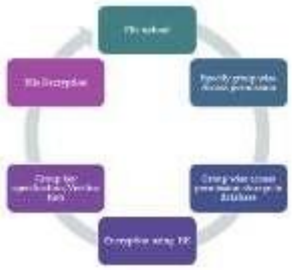


Fig. 3.1: Upload/download working

3.2.8. Group Management Working:

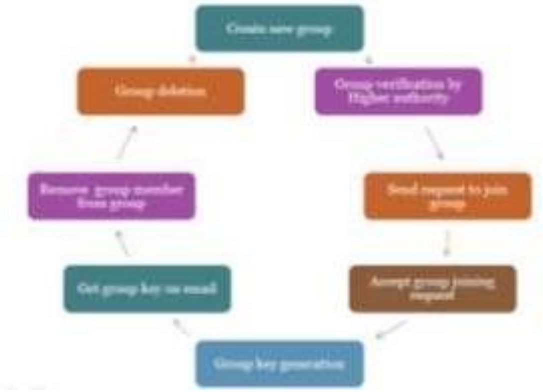

Create new group
Group verification by Higher authority
Send request to join group
Accept group joining request
Group key generation
Get group key on email
Remove group member from group
Group deletion

Fig. 3.2: Group Management Working

3.2.9. Leakage Detection & Prevention:

- If any employee is trying to share any document leakage will get identified using hash value of that document and prevented by system
- When leakage found by system, complaint report will be automatically posted to higher authority
- Higher authority will take legal action against the leaker.

IV. CONCLUSION

The final output of “Enterprise Social Networking with Broadcast Encryption & Document Leakage Detection System” is that you get a high-level encryption as well as decryption for crucial data such as secretes documents and authorized files that are used in various companies. The system allows its clients to encrypt or decrypt by uploading the required file. the “Enterprise Social Networking with Broadcast Encryption & Document Leakage Detection System” is a online repository of all the type of document generated every day by an organization storing these document on local storage has many limitations. Less security chance of getting document damage, accessibility of document lack of availability hybrid cryptography system overcomes the above limitations.

Thus, the “Enterprise Social Networking with Broadcast Encryption & Document Leakage Detection System” instills higher-level security for the crucial data and can be commercialized for further use in future.

REFERENCES

[1] Y. Zheng, “Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption,” master’s thesis, Worcester Polytechnic Inst., 2011.

[2] Vishwagupta, GajendraSingh ,Ravindra Gupta, "Advance cryptography algorithm for improving data security," Network,ijarcsse , Volume 2, Issue 1, January 2012 .

[3] S. Jahid, P. Mittal, and N. Borisov, “Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2011.

[4] J.OrlinGrabbe:”The DES Algorithm Illustrated”, [Online], Available:http://orlingrabbe.com/des.html

[5] William Stalling “Network Security essentials” ,Fourth edition, Pearson,pp. 27-57.

[6] Atulkahate ”cryptography and network security “,Tata McGraw hillPublication,2003.

[7] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[8] Yan Wang and Ming Hu “Timing evaluation of the known cryptographic algorithms “2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09© 2009 IEEE DOI 10.1109/CIS.2009.81.

[9] International journal of technology enhancements and emerging engineering research, vol 2, issue 4 63 issn 2347-4289

[10] Dripto Chatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 © 2011 IEEE.

[11] Dennis Hofheinz Eike Kiltz “Secure Hybrid Encryption from Weakened Key Encapsulation”,Advances in Cryptology CRYPTO '07, Lecture Notes in Computer Science Vol. 4622, A. Menezes ed., Springer-Verlag, 2007.

[12] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, EUROCRYPT'99, volume 1592 of LNCS, pages 223{238. Springer- Verlag, Berlin, Germany, May 1999.

[13] Dennis Hofheinz Eike Kiltz,” secure hybrid encryption from weakened key encapsulation”, advance in cryptography CRYPTO-07.Springer.pp-553-571.