A PROPOSAL TO IMPROVE DENIABLE ENCRYPTION METHOD BASE ON PROBABILISTIC BLOCK CIPHERS

Nguyen Duc Tam*
Academy of Crytography Techniques – Vietnam Government Information Security Commission

***Abstract*—** The paper proposes a deniable encryption probability pseudo-block ciphers method based on the improvement of the deniable encryption block ciphers method proposed in [11] [13], and presents the proof of the correctness, security and deniability of the proposed method. The proposed method is based on a combination of block ciphers that are standardized and widely used today with a system of linear congruence equations.

***Keywords*—** Deniable encryption, probabilistic block ciphers, pseudo-probabilistic block ciphers.

I. MOTIVATION

Deniable encryption (DE) is a special cryptographic technique that is intended to defend against coercive attack. The scenario of a coercive attack is when a coercer has the ciphertext on a public channel, then coercing the sender or receiver or both parties to present the plaintext, secret key, encryption algorithm or decryption algorithm. The main purpose of denial encryption is to make it impossible for a coercer to find the secret message without the proper encryption key (or proper decryption algorithm). The most important feature of deniable encryption is when decrypting a ciphertext yields two different plausible plaintext [1].

Several deniable encryption schemas have been theoretically studied based on public key cryptosystems [5], [6], [8-10] and secret key system [2-4], [7]. However, most of the research on deniable encryption is theoretical or encrypting algorithms implemented by bit only illustrate the proposed method without having any practical application.

The classification of deniable encryption schemas is based on: encryption key used, the encryption algorithm used by the parties, the location of the party being forced by the coercive, the denial characteristics, including: Shared-key deniable encryption schema and public-key deniable encryption schema; Sender-deniable encryption schema, Receiver-deniable encryption schema, Sender or receiver deniable encryption schema, Bi-deniable encryption schema and, Off-the-record deniable encryption schema; Plan-ahead deniable encryption schema and Ad-hoc deniable encryption schema; Fully-deniable encryption schema and Flexible- deniable encryption schema [1].

In the papers [11], [13] have proposed a deniable encryption method base on block ciphers, the method has two encryption phases that combine block ciphers and algorithm to solve the system of congruent equations. the proposed method has proved the correctness, security, and deniability.

This paper proposes a deniable encryption probability pseudo-block ciphers method based on the improvement of the deniable encryption block ciphers method proposed in [11], [13]. The proposed method ensures computationally indistinguishable between the ciphertext generated from the probabilistic block ciphers and the pseudo probabilistic block ciphers deniable encryption.

In the paper, Part II describes the communication model and attack scenario. Part III introduces the proposed method in detail. Part IV proof the properties of the proposed method. Part V conclusion.

II. COMMUNICATION MODEL AND ATTACK SCENARIO

It is assumed that after ciphertext has been sent the adversary has possibility to force both the sender and the receiver to open the following:

1. The plaintext corresponding to the ciphertext;
2. Encryption and decryption algorithms;
3. The encryption key with which encryption of the opened message yields all bits of the ciphertext.

Thus, in the considered model of the coercive attack the sender and the receiver are coerced to open parameters and algorithm of the ciphering procedure with which each bit of the sent ciphertext has been produced depending on the opened message (plaintext).

Security against the described attack can be provided using the symmetric deniable encryption algorithm that produces the ciphertext like cryptogram produced as result of probabilistic encryption of the fake message with fake key. This idea leads to an encryption method that can be called pseudo-probabilistic encryption. Correspondingly, the ciphers performing pseudo-

Contact: Nguyen Duc Tam,
Email: nguyenductamkma@gmail.com
Received: 31/10/2020, Revised: 26/12/2020, Accepted: 15/3/2021.

probabilistic encryption can be called pseudo-probabilistic ciphers.

To have the above properties, for constructing symmetric pseudo-probabilistic ciphers we have used the following design criteria:

- symmetric deniable encryption should be performed as simultaneous encryption of two messages, secret one and fake one, using secret and fake keys (which are shared by sender and receiver);
- a probabilistic encryption algorithm should be associated with the symmetric deniable encryption algorithm;
- the associated probabilistic encryption algorithm should transform the fake message with the fake key into the same ciphertext that is produced by the symmetric deniable encryption algorithm;
- using the fixed-size shared keys should provide performing secure symmetric deniable encryption of messages having arbitrary length.

The use of pseudo-probabilistic encryption is attractive to provide security of the communication session to coercive attacks, since the parties of secure communication protocol can chart plausible that they use the probabilistic encryption to get higher resistance to potential cryptographic attacks.

III. DENIABLE ENCRYPTION METHOD BASE ON PROBABILISTIC BLOCK ENCRYPTION

Probabilistic encryption is the use of randomness in an encryption algorithm, so that when encrypting the same message several times it will, in general, yield different ciphertexts. The term "probabilistic encryption" is typically used in reference to public key encryption algorithms. To be semantically secure, that is, to hide even partial information about the plaintext, an encryption algorithm must be probabilistic.

A commonly used technique for probabilistic encryption is the addition of a random element R with the message M as input to the encryption process. The input message of encryption process is (M,R), when encrypting the same message M with different random R several times it will, in general, yield different ciphertexts $c = E(M,R)$. R is intentionally replaced by an encryption function $T: f_k(T)$ (where $f_k(T)$ is a cryptographic function with a random probability distribution), $f_k(T)$ will act as the random parameter R set to hide the secret message T. With M is a fake message to take the input of the encoding process is $(M, f_k(T))$. If the probability distribution of the ciphertext $E_k(M, f_k(T))$ and the probability distribution of the ciphertext $E_k(M,R)$ are computationally indistinguishable, then the probabilistic encryption method becomes a pseudo-probabilistic encryption. And now, pseudo-probabilistic encryption method becomes a deniable encryption method, where, depending on each case, the communicating parties decrypt the secret message T or the fake message M.

The necessary and sufficient conditions to implement the deniable encryption based on probabilistic encryption are:

1. The parties install and recover exactly secret messages T from the random parameters R in the probabilistic encryption protocol.

2. Probability distributions of functions $f_k(T)$ and R are computability indistinguishable, makes the probability distribution of set of ciphertexts $E_k(M, f_k(T))$ and set of ciphertexts $E_k(M,R)$ are computationally indistinguishable.

The deniable encryption method proposed by the paper is based on two algorithms:

- *The first algorithm* is "**pseudo-probabilistic deniable encryption block ciphers algorithm**", this is a secret algorithm and use for secret mode. Algorithm uses a system of two-unknown congruence equations to combine two pairs of data blocks, each pair consists of a half-block of secret message T and a half-block of fake message M, creating two intermediate cipher blocks. Then two intermediate blocks are chained back to form a block and put into the block cipher to encryp create an output block C.
- *The second algorithm* is "**probabilistic block ciphers algorithm**", it is a fake algorithm and uses for deniable mode. It is used to present to the coercer when under a coercive attack, with a fake message M and random R as inputs.

3.1 Pseudo-probabilistic deniable encryption block ciphers algorithm (secret algorithm)

To increase the randomness of the output ciphertext of the probabilistic block ciphers while ensuring that the output ciphertext space of the probabilistic block ciphers method is equal to the ciphertext space of the pseudo-probabilistic block ciphers. The deniable encryption method in [11], [13] is proposed to improve in detail as shown in *Figure 1.*P_C below:

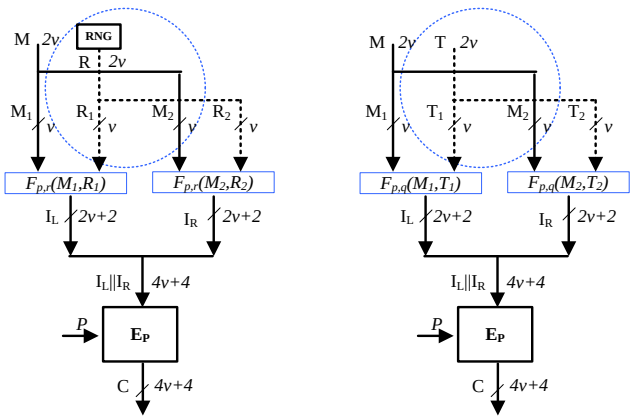

Figure 1.P_T *Probabilistic block ciphers*

Figure 1.P_C *Pseudo-probabilistic deniable encryption block ciphers*

Figure 1. Probabilistic block ciphers and Pseudo-probabilistic deniable encrytion block ciphers

A and B need to transmit a secret message T, camouflaged by a fake message M with the same $2v$-bits size, the detailed encrypting process is as follows:

Step 1:

First, separate the secret message block T and the fake message block M into two equal parts of v bit size: (T_1,T_2) and (M_1,M_2);

Then, use the secret values p *and* q *to combine two bit block pairs* $(M_1,T_1),(M_2,T_2)$ *into the output intermediate cipher blocks* (I_L,I_R), *where* (I_L,I_R) *is the solution of the following two systems of congruent equations:*

$$\begin{cases} I_L \equiv M_1 \bmod p & (a) \\ I_L \equiv T_1 \bmod q & (b) \end{cases} \quad (1)$$

$$\begin{cases} I_R \equiv M_2 \bmod p & (a) \\ I_R \equiv T_2 \bmod q & (b) \end{cases} \quad (2)$$

where p,q satisfy: p is a prime v+1 bit number, and q is a v+1 bit random integer. Then output (I_L,I_R) in the general case is in $2v+2$ bit. According to the Chinese congruent theorem, the solutions of the systems (1), (2) are:

$$I_L = F_{p,q}(M_1,T_1)=[M_1q(q^{-1} \bmod p)+T_1p(p^{-1} \bmod q)] \bmod pq \quad (3)$$

$$I_R = F_{p,q}(M_2,T_2)=[M_2q(q^{-1} \bmod p)+T_2p(p^{-1} \bmod q)] \bmod pq \quad (4)$$

where $(q^{-1} \bmod p)$ is the inverse element of q modulo p, $(p^{-1} \bmod q)$ is the inverse element of p modulo q.

Step 2:

Using block cipher E with encrypt key *P,* to encrypt the message block $I=(I_L \| I_R)$ (where || is the symbol that join trwo bit strings) produces a output cipher bock $4v+4$ bit size: $C=E_P(I)$. Block cipher $E_P()$ is used with the following *assumption 1*:

Assumption 1*:* $E_P()$ *is a secure block cipher and the output ciphertext of* $E_P()$ *has a uniform random distribution.*

This assumption is acceptable and practical, because the most commonly used block ciphers now satisfy the standard of random distribution of the output ciphertext [14].

The key of the encryption and decryption process is (p,q) for the congruent system of equations and the key P for the block cipher *E.* Where (p,P) is fixed, q changes after each communication, (q is randomly chosen and distributed. advance to the two sides and act as session key).

Algorithms of the encrypting process and decrypting process are as follows:

The encryption process:

Algorithm Enc_P*C* Encrypting in Pseudo-probabilistic deniable encryption block ciphers algorithm *(in secret mode)*

INPUT: M,T,P,p,q

OUTPUT: C

1. $M_1 \leftarrow Left(M,v)$;
2. $M_2 \leftarrow Right(M,v)$;
3. $T_1 \leftarrow Left(T,v)$;
4. $T_2 \leftarrow Right(T,v)$;
5. $I_L \leftarrow [M_1q(q^{-1} \bmod p)+T_1p(p^{-1} \bmod q)] \bmod pq$;
6. $I_R \leftarrow [M_2q(q^{-1} \bmod p)+T_2p(p^{-1} \bmod q)] \bmod pq$;
7. $I \leftarrow I_L \| I_R$;
8. $C \leftarrow E_P(I)$;
9. return C.

The decryption process:

Algorithm Dec_P*C* Decrypting in Pseudo-probabilistic deniable encryption block ciphers algorithm *(in secret mode)*

INPUT: C,P,p,q

OUTPUT: M

1. $I \leftarrow E_P^{-1}(C)$;
2. $I_L \leftarrow Left(I,2v+2)$;
3. $I_R \leftarrow Right(I,2v+2)$;
4. $T_1 \leftarrow I_L \bmod q$;
5. $T_2 \leftarrow I_R \bmod q$;
6. $T \leftarrow T_1 \| T_2$;
7. return T.

3.2 Probabilistic block ciphers algorithm (fake algorithm)

The probabilistic block ciphers agorithm (fake algorithm) used to present to the coercer (*firgure.*P_T) is similar.

Step 1:

The algorithm is explained to the coerver that, because the block cipher E does not guarantee semantic security in some cases (eg: ECB block ciphers mode), and in order to counteract the potential risks of type "trapdoor" in block cipher *E,* the algorithm adds random bit-blocks $R_1,R_2<2^v$ R and a random integer $2^v \le r < 2^{v+1}$, then the intermediate cipher blocks are computed against the congruence systems:

$$\begin{cases} I_L \equiv M_1 \bmod p & (a) \\ I_L \equiv R_1 \bmod r & (b) \end{cases} \quad (5)$$

$$\begin{cases} I_R \equiv M_2 \bmod p & (a) \\ I_R \equiv R_2 \bmod r & (b) \end{cases} \quad (6)$$

According to the Chinese congruent theorem, the solutions of the systems (5), (6) are:

$$I_L = F_{p,r}(M_1,R_1)=[M_1r(r^{-1} \bmod p)+R_1p(p^{-1} \bmod r)] \bmod pr \quad (7)$$

$$I_R = F_{p,r}(M_2,R_2)=[M_2r(r^{-1} \bmod p)+R_2p(p^{-1} \bmod r)] \bmod pr \quad (8)$$

Step 2:

the intermediate cipher block $I=I_L \| I_R$ is encrypted using block cipher E: $C = E_P(I)$.

The added random values (R,r) are not stored in the computer's memory during the probabilistic encrypting process, they are added under the following *assumption 2:*

Assumption 2*: The random values (R,r) add to the probabilistic block ciphers agorithm, are generated during each encryption execution and are not stored in the computer's memory.*

Algorithms of the encrypting process and decrypting process are as follows:

The encryption process:

Algorithm Enc_P$_T$ Encrypting in Probabilistic block ciphers algorithm *(in deniable mode)*

(This is a fake algorithm presented when under a coercive attack, the two sides keep secret parameter q)

INPUT: M, R, P, p, r

OUTPUT: C

1. $M_1 \leftarrow Left(M, v)$;
2. $M_2 \leftarrow Right(M, v)$;
3. $R_1 \leftarrow Left(R, v)$;
4. $R_2 \leftarrow Right(R, v)$;
5. $I_L \leftarrow [M_1 r(r^{-1} \bmod p) + R_1 p(p^{-1} \bmod r)] \bmod pr$;
6. $I_R \leftarrow [M_2 r(r^{-1} \bmod p) + R_2 p(p^{-1} \bmod r)] \bmod pr$;
7. $I \leftarrow I_L \,||\, I_R$;
8. $C \leftarrow E_P(I)$;
9. return C.

The decryption process:

Algorithm Dec_P$_T$ *Decrypting in Probabilistic block ciphers algorithm (in deniable mode)*

(This is a fake algorithm presented when under a coercive attack, the two sides keep secret parameter q)

INPUT: C, P, p, r

OUTPUT: M

1. $I \leftarrow E_P^{-1}(C)$;
2. $I_L \leftarrow Left(I, 2v+2)$;
3. $I_R \leftarrow Right(I, 2v+2)$;
4. $M_1 \leftarrow I_L \bmod p$;
5. $M_2 \leftarrow I_R \bmod p$;
6. $M \leftarrow M_1 \,||\, M_2$;
7. return M.

How to defend against coercive attack: When the parties are coercived, the parties will present to the coercer: the fake algorithm **Probabilistic block ciphers algorithm** and parameters: (P, p, r), and they are completely consistent with the ciphertext C in the hands of the coercer (where C is the ciphertext encrypted by A using the secret algorithm **Pseudo-probabilistic deniable encryption block ciphers algorithm** and sent to B).

IV. CORRECTNESS, SECURITY AND DENIABILITY OF PROPOSED METHOD

4.1 Definition share-key flexible bi-deniable encryption

The method of performing encryption can be denied as described in section III using pre-shared key sharing and using two algorithms, one actually uses (the one that is dishonest with the coercer), a fake algorithm that exposes when under a coercive attack (the algorithm is honest with the coercer). From the concepts of Canetti et al. In [1], the proposed method takes the form of a share-key flexible bi-deniable encryption method.

Based on the definitions in [1], including definition 4 of a share-key sender-deniable encryption protocol, definition 3 of a public key flexible-sender-deniable encryption protocol, definition 10 public key bi-deniable encryption protocol. The definition of share-key flexible bi-deniable encryption stated as [1], [13]:

With symbols:

- m_1 is the secret transmitted message, m_2 is the fake massage, k is the share-key, r_A is the sender A's random input, r_B is the receiver B's random input, c is a transcript ò the conversation between A and B for transmitting m_1, faking algorithm ϕ used inputs: secret massage m_1, fake massage m_2, ciphertext c and randoms input r_A, r_B to recreate fake randoms input and fake share-key: $(\tilde{k}, \tilde{r}_A) = \phi_A(m_1, k, r_A, c, m_2)$, $(\tilde{k}, \tilde{r}_B) = \phi_B(m_1, k, r_B, c, m_2)$.

- $COM_\pi(P, m, k, r_A, r_B)$ denote the communication between A and B for transmit m, when A has random input r_A and B has random input r_B, with share-key k and preserve-bit P.

- $COM_\pi(P, m, k)$ denote the random variable description $COM_\pi(P, m, k, r_A, r_B)$ when r_A and r_B are uniformly and independently chosen.

<u>Definition 1</u>: share-key flexible bi-deniable encryption protocol

A protocol π with sender A and receiver B, binary Preserve parameter P (with two values P_T, P_C) is ashare-key flexible bi-deniable encryption protocol if:

Correctness*: The receiver always decrypts and recovers the plaintext from the sender and transmits it*

Security*: For any m_1, m_2 of plaintext space M and for anny $P \in \{P_T, P_C\}$ and random share-key k, we have:*

$$COM_\pi(P, m_1, k) \approx^c COM_\pi(P, m_2, k)$$

(encryption of m_1, m_2 are indistinguisable independent of P)

Deniability*: There exits two efficients "faking" algorithm ϕ_A, ϕ_B having the following property with respect to any $m_1, m_2 \in M$. Let k, r_A, r_B, r_A', r_B' be uniformly*

chosen random input of A and B, respectively let $c = COM_\pi(P_C, m_1, k, r_A, r_B)$, *and* $(\tilde{k}, \tilde{r}_A) = \phi_A(m_1, k, r_A, c, m_2)$, $(\tilde{k}, \tilde{r}_B) = \phi_B(m_1, k, r_B, c, m_2)$, *Then, the random variables:*

$(m_2, \tilde{k}, \tilde{r}_A, \tilde{r}_B, c) \approx^c (m_2, k, r_A^{'}, r_B^{'}, COM_\pi(P_T, m_2, k, r_A^{'}, r_B^{'}))$.

(where $\approx^c$: is the computationally indistinguishable sign of the two probability distributions).

4.2 Proof the correctness, security and deniability of proposed method

Clause 1*: The pseudo-probabilistic deniable encryption block ciphers method described in Section III is a share-key flexible bi-deniable encryption protocol as described in Definition 1.*

Proof:

We have:

- When $P = P_C$: the algorithm that the two sides use at this time is the algorithm that is dishonest to the coercer, that is, the two sides use "**pseudo-probabilistic deniable encryption block ciphers algorithm**" (the encryption algorithm is *Enc_P*$_C$, the algorithm decoded is *Dec_P*$_C$).

- When $P = P_T$: the algorithm both sides use now is the algorithm that is honest with the coercer, that is, the two sides use "**probabilistic block ciphers algorithm**" (the encryption algorithm is *Enc_P*$_T$, the decryption algorithm is *Dec_P*$_T$).

*** Correctness:**

With ciphertext C generated from the *Enc_P*$_C$ encryption algorithm:

+ In secret mode, B uses the *Dec_P*$_C$ secret algorithm, which correctly recovers the secret message T using key (P, q).

The decrypting process *Dec_P*$_C$ is in secret mode:

$E_p^{-1}(C) \to I_L \| I_R \to (I_L \bmod q) \| I_R \bmod q) \to T_1 \| T_2 \to T$

+ In deniable mode, B uses the *Dec_P*$_T$ fake algorithm, which correctly recovers the fake message M using key (P, p).

The decrypting process *Dec_P*$_T$ is in deniable mode:

$E_p^{-1}(C) \to I_L \| I_R \to (I_L \bmod p) \| I_R \bmod p) \to M_1 \| M_2 \to M$

*** Security:**

Apply the parameters according to Definition 1, $m_1 = (M, T), m_2 = (M, R), k = (P, p)$.

The encryption process:

The process of forming the output ciphertext according to Figure 1 is illustrated:

+ When $P = P_T$, in deniable mode:

$COM_\pi(P_T, m_1, k) = [M \to F_{p,r}(M_1, T_1) \| F_{p,r}(M_2, T_2) \to E_p(F_{p,r}(M_1, T_1) \| F_{p,r}(M_2, T_2))]$

$= E_p(F_{p,r}(M_1, T_1) \| F_{p,r}(M_2, T_2))$

$COM_\pi(P_T, m_2, k) = [M \to F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2) \to E_p(F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2))]$

$= E_p(F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2))$

+ When $P = P_C$, in secret mode:

$COM_\pi(P_C, m_1, k) = [M \to F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2) \to E_p(F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2))]$

$= E_p(F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2))$

$COM_\pi(P_C, m_2, k) = [M \to F_{p,q}(M_1, R_1) \| F_{p,q}(M_2, R_2) \to E_p(F_{p,q}(M_1, R_1) \| F_{p,q}(M_2, R_2))]$

$= E_p(F_{p,q}(M_1, R_1) \| F_{p,q}(M_2, R_2))$

With:

$F_{p,r}(M_1, T_1) = [M_1 r(r^{-1} \bmod p) + T_1 p(p^{-1} \bmod q)] \bmod pr$

$F_{p,r}(M_2, T_2) = [M_2 r(r^{-1} \bmod p) + T_2 p(p^{-1} \bmod q)] \bmod pr$

$F_{p,r}(M_1, R_1) = [M_1 r(r^{-1} \bmod p) + R_1 p(p^{-1} \bmod q)] \bmod pr$

$F_{p,r}(M_2, R_2) = [M_2 r(r^{-1} \bmod p) + R_2 p(p^{-1} \bmod q)] \bmod pr$

$F_{p,q}(M_1, T_1) = [M_1 q(q^{-1} \bmod p) + T_1 p(p^{-1} \bmod q)] \bmod pq$

$F_{p,q}(M_2, T_2) = [M_1 q(q^{-1} \bmod p) + T_2 p(p^{-1} \bmod q)] \bmod pq$

$F_{p,q}(M_1, R_1) = [M_1 q(q^{-1} \bmod p) + R_1 p(p^{-1} \bmod q)] \bmod pq$

$F_{p,q}(M_2, R_2) = [M_1 q(q^{-1} \bmod p) + R_2 p(p^{-1} \bmod q)] \bmod pq$

We have: according to *Assumption 1*, the output of the encryption process is the output of the block cipher E_p with a uniformly distributed, thus:

The probability distribution of $COM_\pi(P_T, m_1, k) và COM_\pi(P_T, m_2, k)$ is uniformly random;

The probability distribution of $COM_\pi(P_C, m_1, k) và COM_\pi(P_C, m_2, k)$ is uniformly random.

The decryption process:

Since the way of retrieving the spoof M message in the two algorithms (the secret algorithm and the fake algorithm) is identical, the decryption process is in the opposite sequence to the encryption process shown in *Figure 1* described as:

+ When $P = P_T$, in deniable mode:

$COM_\pi(P_T, m_1, k) = COM_\pi(P_T, m_2, k) =$

$= [E_p^{-1}(C) \to I_L \| I_R \to (I_L \bmod p) \| I_R \bmod p) \to M_1 \| M_2 \to M] = M$

+ When $P = P_C$, in secret mode:

$COM_\pi(P_C, m_1, k) = COM_\pi(P_C, m_2, k) =$

$= [E_p^{-1}(C) \to I_L \| I_R \to (I_L \bmod p) \| I_R \bmod p) \to M_1 \| M_2 \to M] = M$

therefoce:

$COM_\pi(P_T, m_1, k) \approx^c COM_\pi(P_T, m_2, k)$;

$COM_\pi(P_C, m_1, k) \approx^c COM_\pi(P_C, m_2, k)$

*** Deniability:**

+ Apply the parameters according to Definition 1:

$m_1 = (M, T); m_2 = (M, R)$;

$k = \tilde{k} = p$;

$r_A = r_B = q$;

$\tilde{r}_A = r_A^{'} = \tilde{r}_B = r_B^{'} = r$;

A encrypt message T with the secret algorithm *Enc_P$_C$ (Figure 1.P$_C$)*, the process of forming the output ciphertext of the E_P encryption is described:

$$COM_\pi(P_C, m_1, k, r_A, r_B) = [M \to F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2) \to E_P(F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2))]$$
$$= E_P(F_{p,q}(M_1, T_1) \| F_{p,q}(M_2, T_2))$$

A encrypt message M with the fake algorithm *Enc_P$_T$ (Figure 1.P$_T$)*, the process of forming the output ciphertext of the E_P encryption is described:

$$COM_\pi(P_T, m_2, k, r_A^{'}, r_B^{'}) = [M \to F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2) \to E_P(F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2))]$$
$$= E_P(F_{p,r}(M_1, R_1) \| F_{p,r}(M_2, R_2))$$

According to *Assumption 1*, the output of the encryption process is the output of the block cipher E_P with a uniformly distributed and by choosing the parameters (p, q, r), we have the probability distribution of:

$(m_2, \tilde{k}, \tilde{r}_A, \tilde{r}_B, COM_\pi(P_C, m_1, k, r_A, r_B))$ and

$(m_2, k, r_A^{'}, r_B^{'}, COM_\pi(P_T, m_2, k, r_A^{'}, r_B^{'}))$

is uniformly random, therefore the two probability distributions are computationally indistinguishable.

Comment

The cryptographic security of the Pseudo-probabilistic deniable encryption block ciphers method depends on the security of the block cipher functions E used to encrypt input blocks of data. The most efficient and easy to execute is the use of standard block ciphers (standard block ciphers) that have been tested for safety in practice. The paper proposes to use TripleDES block ciphers algorithm with data block size $4v+4=64$ bits [12], or AES block ciphers algorithm with data block size $4v+4=128$ bits [12].

In the general case, two encrypted messages are divided into z blocks of data of equal size $2v$-bit: $M=(M_1, M_2, \ldots, M_z)$ and $T=(T_1, T_2, \ldots, T_z)$, then the corresponding pairs of (M_i, T_i) are encrypted consecutively with the same set of session keys (P, p, q).

V. CONCLUSION

The proposed method in the paper uses the algorithm to solve the system of congruent equations, chaining the two halves of the secret message and the two halves of the fake message block into two intermediate cipher blocks, then two intermediate cipher blocks are chained and input to a block ciphers (standardized and widely used) to encrypt an output cipher block. The proposed method ensures the correctness in encrypting and decrypting, it is a bi- deniable encryption method. With fake messages being generated right after encryption, the proposed method is a plan ahead-deniable encryption method. The output ciphertexts of the pseudo-probabilistic deniable encryption block ciphers algorithm to have a random probability distribution same to that of the ciphertext generated by the probabilistic deniable encryption block ciphers algorithm on the same space of the ciphertext. With the use of the secret message as an additional random source of probabilistic block ciphers, the proposed method is implemented as a pseudo-probabilistic block ciphers method.

REFERENCES

[1] Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky, "Deniable Encryption," Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, pp. 90-104, 1997.

[2] Truecrypt: Free open-source on-the-fly encryption. [Online]. http://truecrypt.org.

[3] Roger Needham, and Adi Shamir Ross Anderson, "The steganographic file system. In Information Hiding," Springer, pp. 73-82, 1998.

[4] AndrewD. McDonald and MarkusG. Kuhn. Stegfs, "A steganographic file system for linux. In Andreas Pfitzmann, editor, Information," Springer Berlin Heidelberg, pp. 463–477, 2000.

[5] B. Meng, "A Secure Internet Voting Protocol Based on Non-interactive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext," Journal of Networks, pp. 370–377, 2009.

[6] I. Yu, E. Kushilevits, and R. Ostrovsky, "Efficient Non-interactive Secure Computation," Advances in Cryptology -- EUROCRYPT 2011. Lectute Notes in Computer Science. Springer – Verlag. Berlin, Heidelberg, New York, pp. 406-425, 2011.

[7] C. Wang and J.A. Wang , "Shared-key and Receiver-deniable Encryption Scheme over Lattice," Journal of Computational Information Systems, pp. 747-753, 2012.

[8] N.A. Moldovyan, A.A. Moldovyan, and A.V. Shcherbacov, "Deniable-encryption protocol using commutative transformation," Workshop on Foundations of Informatics, pp. 285-298, 2016.

[9] N.A. Moldovyan, A.N. Berezin, A.A. Kornienko, and A.A. Moldovyan, "Bi-deniable Public-Encryption Protocols Based on Standard PKI," Proceedings of the 18th FRUCT & ISPIT Conference, Technopark of ITMO University, Saint-Petersburg, Russia. FRUCT Oy, Finland, pp. 212-219, 2016.

[10] A.A. Moldovyan, N.A. Moldovyan, and V.A. Shcherbakov, "Bi-Deniable Public-Key Encryption Protocol Secure Against Active Coercive Adversary," Buletinul Academiei de Stiinte a Republicii Moldova. Mathematica, pp. 23-29, 2014.

[11] Moldovyan Nikolay Andreevich, Moldovyan Alexander Andreevich, Tam Nguyen Duc, Hai Nguyen Nam, Manh Cong Tran, Minh Nguyen Hieu, "Pseudo-probabilistic block ciphers and their randomization" in Journal of Ambient Intelligence and Humanized Computing (volume 10).: Springer International, 2019, pp. 1977-1984.

[12] J. Pieprzyk, T. Hardjono and J. Seberry, Fundamentals of computer security, Springer-Verlag, 2003.

[13] Nguyễn Đức Tâm, Nguyễn Nam Hải, Nguyễn Hiếu Minh, "Chứng minh tính đúng đắn, an toàn và chối từ của phương pháp mã hóa theo khối giả xác suất có thể chối từ", Tạp chí nghiên cứu KH&CN Quân sự (Số 65), 02 2020, pp. 175-185.

[14] J. Soto and L. Bassham, "Randomness testing of the advanced encryption standard finalist candidates", NIST IR 6483, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6483.pdf, 2000.

MỘT ĐỀ XUẤT CẢI TIẾN PHƯƠNG PHÁP MÃ HÓA CÓ THỂ CHỐI TỪ DỰA TRÊN MÃ KHỐI XÁC SUẤT

***Tóm tắt*—** Bài báo đề xuất một phương pháp mã khối giả xác suất có thể chối từ dựa trên cải tiến phương pháp mã hóa theo khối có thể chối từ đã được đề xuất trong [11][13], đồng thời trình bày các chứng minh về tính đúng đắn, an toàn và chối từ của phương pháp đề xuất. Phương pháp đề xuất dựa trên sự kết hợp của các mã khối đã được chuẩn hóa và sử dụng rộng rãi hiện nay với hệ phương trình đồng dư tuyến tính

***Từ khóa*—**Mã hóa có thể chối từ, mã hóa theo khối xác suất, mã hóa theo khối giả xác suất.

AUTHOR's BIOGRAPHY
Nguyễn Đức Tâm
Born in 1974 in Bac Giang provice. Graduated in Academy of Cryptography Techniques. Currently working at Academy of Cryptography Techniques. Research scope: deniable encryption.
Email: nguyenductamkma@gmail.com