Deniable Encryption Protocols Based on Probabilistic Public-Key Encryption

Nikolay Moldovyan[1], Andrey Berezin[2],
Anatoly Kornienko[3], Alexander Moldovyan[1]

[1]Saint Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
[2]Saint Petersburg Electrotechnical University "LETI"
[3]Petersburg State Transport University
St. Petersburg, Russian Federation
nmold@mail.ru, a.n.berezin.ru@gmail.com, {kaa.pgups,maa1305}@yandex.ru

***Abstract*—The paper proposes a new method for designing deniable encryption protocols characterized in using RSA-like probabilistic public-key encryption algorithms. Sender-, receiver-, and bi-deniable protocols are described. To provide bi-deniability in the case of attacks perfored by an active coercer stage of entity authentication is used in one of described protocols.**

I. Introduction

The regular encryption schemes provide very high security against known-plaintext and chosen text attacks, therefore they are widely used to protect information sent via telecommunication channels from unauthorized access. However, in real world sometimes an adversary (coercer) has power to force a user to open encryption keys. Such attacks are called coercive. To provide security against such attacks it was introduced notion of *deniable encryption* (DE) [1]. The DE schemes are classified according to which party of the communication session may be coerced: sender-deniable, receiver-deniable, sender- and receive-deniable (bi-deniable) schemes in which coercer attacks the sender, the receiver, and the both parties, correspondingly. There are also considered shared-key DE protocols [2] and public key ones [2], [3]. Practical applications of the DE protocols relate to prevention of the vote buying in the internet-voting systems [4], [5], to providing secure multi-party computations [6], and to providing information secrecy with practical methods of the public-key deniable encryption [7], [8], [9], [10].

Resistance of the DE protocols to coercive attacks is provided due to potential possibility to decrypt the ciphertext c in different ways. The receiver can open the secret message t, but when being coerced he opens the fake message m. It should be mentioned the issue about time at which the attacked parties have to decide on the fake message. In the *plan-ahead* DE protocols the fake message is selected at time of encryption. There are known practical public-key DE schemes [11] and shared-key DE ones [2] in which the fake message is fixed and selected before or during the encryption process. From theoretic point of view the *flexible* DE protocols represent significant interest, in which the fake massage can be selected arbitrary at time of the coercive attack.

Possibility of the alternative decryption in the flexible public-key DE protocols is connected with using a random value r when encrypting the secret message t. The public-key encryption can be represented with the formula $c = E_P(t, r)$, where P is a public key. At time of the coercive attack the sender of the message can open a fake message m with another random value $r' \neq r$ such that $c = E_P(m, r')$. The fake random value r' can be computed with some faking algorithm F_P, parametrized with the public-key value P. The algorithm F_P is considered as a part of the DE scheme. Its input is the pair (c, m), i.e. $r' = F_P(c, m)$. The fake message can be selected arbitrary at time when the sender and/or the receiver of the ciphertext are coerced. Examples of such design of the DE protocols are presented in papers [12], [13]. In that protocols the secret message is encrypted consecutively bit by bit. Besides, each bit is sent in form of large pseudo-random number having size more than 1000 bits.

Present paper proposes a novel design of flexible public-key DE protocols in which the message is transformed as a single data block that provides significantly higher performance. Besides, the proposed protocols provide simple and very fast procedure (performing only one modulo multiplication operation) for computing the fake random input (which plays role of the local encryption key) connected with the fake message. The main feature of the proposed design is combining probabilist public-key encryption with the commutative encryption, the last being implemented without exchanging encryption keys (called local keys). The random values are generated independently of the secret and fake messages, therefore they are not saved in computer memory. The role of the random values used while performing the public-key encryption consists only in randomizing the ciphertexts. Due to such destination of the random values and due to lack of their connection with messages (secret and fake ones) it is supposed that at time of coercive attack the coercer demands opening the source message, the secret and private keys, including the local keys, but not values of the randomization parameter of the probabilistic public-key encryption algorithm.

The paper organized as follows. Section 2 describes the commutative encryption algorithm and RSA-like public-key encryption algorithms used in the proposed DE protocols. Section 3 describes the sender-deniable, receiver-deniable, and sender&receiver-deniable protocols in which the fake message is selected at time of attack. Section 4 describes a bi-deniable plan-ahead DE protocol. Section 5 presents discussion. Section 6 concludes the paper.

ISSN 2305-7254

II. Encryption algorithms used in frame of the proposed DE protocols

A. Commutative encryption

If some encryption function E satisfies the following condition

$$E_K[E_Q(M)] = E_Q[E_K(M)],$$

where K and Q are encryption keys and M is some plaintext, then it is called a commutative encryption function. Commutative encryption is used in Shamir's no key protocol (also called Shamir's three-pass protocol [14]) described as follows. Suppose Alice (sender) wishes to send the secret message M to Bob (receiver), using a public channel and no shared key. For this purpose they can use the following protocol that provides privacy:

1) Alice chooses a random key K and encrypts the message M using a commutative encryption function $E : C_1 = E_K(M)$, where C_1 is the produced ciphertext. Then she sends the ciphertext C_1 to Bob.

2) Bob chooses a random key Q and encrypts the ciphertext C_1 using the function E as follows: $C_2 = E_Q(C_1)$, where C_2 is the produced ciphertext. Then he sends the ciphertext C_2 to Alice.

3) Alice decrypts the ciphertext C_2 obtaining the ciphertext $C_3 : C_3 = E_K^{-1}(C_2)$. Then she sends the ciphertext C_3 to Bob.

Having received the ciphertext C_3 Bob computes the value $M' = E_Q^{-1}(C_3)$. Due to commutativity of the encryption function the values M' and M are equal, i.e. the protocol works correctly. Indeed, one has the following:

$$M' = E_Q^{-1}(C_3) = E_Q^{-1}[E_K^{-1}(C_2)] = E_Q^{-1}[E_K^{-1}[E_Q(C_1)]] = E_Q^{-1}[E_K^{-1}[E_Q(E_K(M))]] = E_Q^{-1}[E_K^{-1}[E_K(E_Q(M))]] = E_Q^{-1}[E_Q(M)] = M.$$

If the used encryption function E is secure to the know input text attack, then the described three-pass protocol provides security to passive attacks. However it does not provide authentication, i.e. it is not secure to active attacks. The mentioned security requirement is not actual for the DE protocols described in the next section, therefore we use simple commutative encryption function described as modulo multiplication of the message $M < n$ and the key $K < n$:

$$C = E_K(M) = MK \bmod n,$$

where n is an integer containing two large (1024 bits) prime factors and K is relatively prime to n. The decryption function is described as follows:

$$M = E_K^{-1}(C) = CK^{-1} \bmod n,$$

where integer number K^{-1} is such that $K^{-1}K \equiv 1 \bmod n$.

B. RSA-like public encryption algorithm

To perform probabilistic public-key encryption we will use a modification of the RSA algorithm [15] in which it is specified a prime $\pi = 2\mu+1$, where μ is equal to the following 128-bit prime number

$$338507469684516321177847385852415861521.$$

The RSA cryptoscheme [15] is used for performing the public encryption with Bob's public key (n_B, e_B) that is generated simultaneously with his private key d_B as follows. Bob selects two strong [16] primes p and q having large size (for example, 1024 bits). Then it is computed the value $n_B = pq$ and selected a random number e_B (of comparatively small size,for example, 32 bits) that is relatively prime to Euler phi function values $\phi(n_B) = (p-1)(q-1)$ and $\phi(\pi) = \pi-1$. The private key d_B is calculated as number $d_B = e_B^{-1} \bmod (p-1)(q-1)(\pi-1)$. Probabilistic public-key encryption of some message M (such that $M < n_B$) is performed as computing the ciphertext

$$C = (M||\rho)^{e_B} \bmod n_B\pi,$$

where $||$ denotes the concatenation operation; the parameter ρ is a uniformly random 128-bit string. Decryption of the ciphertext C is performed with the private value d as follows

$$M = \left(C^{d_B} \bmod n_B\pi\right) \text{ div } 2^{128}.$$

The parameter ρ takes on a random value that is at moment of performing the probabilistic public-key encryption operation, i.e. the values ρ are different at arbitrary two steps of performing the RSA-like encryption. Since the values ρ have no relation to the input message there is no need to save them in computer memory. The last explains why we assume that the coercer does not demand Alice (sender in communication session) and Bob (receiver of the message) to open the values ρ, like in other DE protocols [12], [13] opening some used random values is not supposed.

III. Flexible DE protocols

A. Sender-side public key DE protocol

The proposed flexible sender-deniable public-key encryption protocol (fig. 1) represents a three-pass DE scheme and is described as follows.

1) To send the secret message M, where $M < n_B$, Alice generates her local key K as a random value $K < n_B$ such that $\gcd(K, n_B) = 1$ and computes the value $C = MK \bmod n_B$ and the ciphertext

$$C_1 = (C||\rho)^{e_B} \bmod n_B\pi = ((MK \bmod n_B)||\rho)^{e_B} \bmod n_B\pi.$$

Then she sends the ciphertext C_1 to Bob.

2) Using his private key d_B Bob decrypts the ciphertext C_1: $C||\rho = C_1^{d_B} \bmod n_B\pi$, generates a random value $Q < n_B$ such that $\gcd(Q, n_B) = 1$ and computes the ciphertext

$$C_2 = CQ \bmod n_B = MKQ \bmod n_B.$$

Then he sends the value C_2 to Alice.

3) Alice computes the ciphertext

$$C_3 = ((C_2K^{-1} \bmod n_B)||\rho)^{e_B} \bmod n_B\pi = = ((MQ \bmod n_B)||\rho)^{e_B} \bmod n_B\pi\}$$

and sends the value C_3 to Bob.

Bob decrypts the ciphertext $C_3 : (MQ \bmod n_B)||\rho = (C_3)^{d_B} \bmod n_B\pi$ and discloses the secret message M as follows: $M = (MQ \bmod n_B)Q^{-1} \bmod n_B$.

Alice		Bob
$K \leftarrow_{\$} \mathbb{Z}_{n_B}$		
$\gcd(K, n_B) = 1$		
$C = MK \bmod n_B$		
$C_1 = (C\|\|\rho)^{e_B} \bmod n_B\pi$		
	$\xrightarrow{C_1}$	
		$C\|\|\rho = C_1^{d_B} \bmod n_B\pi$
		$Q \leftarrow_{\$} \mathbb{Z}_{n_B}$
		$\gcd(Q, n_B) = 1$
		$C_2 = CQ \bmod n_B$
	$\xleftarrow{C_2}$	
$C_3 = ((C_2K^{-1} \bmod n_B)\|\|$		
$\|\|\rho)^{e_B} \bmod n_B\pi$		
	$\xrightarrow{C_3}$	
		$M = (MQ \bmod n_B)$
		$Q^{-1} \bmod n_B$

Fig. 1. Flexible sender-side deniable public-key encryption protocol

The protocol resists the sender-side coercive attack at which it is supposed that some coercer intercepts the ciphertexts C_1, C_2, and C_3 sent during the communication session and after termination of the protocol he forces Alice to open the secret message and her local key. When being coerced Alice chooses some fake message M' such that $M' < n_B$ and such that $\gcd(M', n_B) = 1$, computes the fake local key $K' = MKM'^{-1} \bmod n_B$, and opens the fake values M' and K' as the real values that had been used at step 1 of the protocol. One should note that probability of the event $\gcd(M', n_B) \neq 1$ is negligibly small ($< 2^{-1000}$), due to large size of the both divisors of the number n_B.

From the ciphertext C_2 coercer is able to calculate the value $Q' = C_2M'^{-1}K'^{-1} \bmod n_B$ for which the following inequality holds $M'Q' \bmod n_B \neq MQ \bmod n_B$. However for the coercer it is computationally infeasible to disclose Alice's lie because of the probabilistic encryption performed at step 3. Indeed, the ciphertext C_3 depends on both the $M'Q' \bmod n_B$ and the value ρ, therefore to demonstrate inequality $M'Q' \bmod n_B \neq MQ \bmod n_B$ the coercer should show that inequality $C_3 \neq ((M'Q' \bmod n_B)||\rho)^{e_B} \bmod n_B\pi$ holds for all possible values of the parameter ρ. The last is computationally infeasible due to very large number (2^{128}) of the potentially possible values of the parameter ρ. Thus, the described protocol in sender-deniable one and its resistance is defined by security of the RSA-like public-key encryption algorithm, i.e. its resistance to sender-side coercive attack is sub-exponential.

B. Receiver-side public key DE protocol

The proposed flexible receiver-deniable public-key encryption protocol is characterized in using the public key of the sender (fig. 2), i.e. Alice's public key (n_A, e_A). It represents a three-pass DE protocol described as follows.

1) To send the secret message M, where $M < n_A$, Alice generates her local key K as a random value $K < n_A$ such that $\gcd(K, n_A) = 1$ and computes the ciphertext $C_1 = MK \bmod n_A$. Then she sends the ciphertext C_1 to Bob.

2) Bob generates a random value $Q < n_A$ such that $\gcd(Q, n_A) = 1$ and computes the ciphertexts $C_2' = C_1Q \bmod n_A = MKQ \bmod n_A$ and

$$C_2 = ((C_2')||\rho)^{e_A} \bmod n_A\pi.$$

Then he sends the value C_2 to Alice.

3) Alice decrypts the ciphertext $C_2 : C_2'||\rho = (MKQ \bmod n_A)||\rho = (C_2)^{d_A} \bmod n_A\pi$, where d_A is Alice's private key. Then she computes the ciphertext

$$C_3 = C_2'K^{-1} \bmod n_A = MQ \bmod n_A$$

and sends the last value to Bob.

Bob decrypts the ciphertext C_3 and gets the secret message: $M = C_3Q^{-1} \bmod n_A$.

Alice		Bob
$K \leftarrow_{\$} \mathbb{Z}_{n_A}$		
$\gcd(K, n_A) = 1$		
$C_1 = MK \bmod n_A$		
	$\xrightarrow{C_1}$	
		$Q \leftarrow_{\$} \mathbb{Z}_{n_A}$
		$\gcd(Q, n_A) = 1$
		$C_2' = C_1Q \bmod n_A$
		$C_2 = ((C_2')\|\|\rho)^{e_A}$
		$\bmod n_A\pi$
	$\xleftarrow{C_2}$	
$C_2'\|\|\rho = (C_2)^{d_A} \bmod n_A\pi$		
$C_3 = C_2'K^{-1} \bmod n_A =$		
$= MQ \bmod n_A$		
	$\xrightarrow{C_3}$	
		$M = C_3Q^{-1} \bmod n_A$

Fig. 2. Flexible receiver-side deniable public-key encryption protocol

The protocol resists the receiver-side coercive attack at which it is supposed that some coercer intercepts the ciphertexts C_1, C_2, and C_3 sent during the communication session and after termination of the protocol he forces Bob to open the message and his local key. When being coerced Bob chooses some fake message M' such that $M' < n_A$ and $\gcd(M', n_A) = 1$, computes the fake local key $Q' = MQM'^{-1} \bmod n_A$, and opens the fake values M' and Q' as the real values. Since probability of the event $\gcd(M', n_b) \neq 1$ is negligibly small ($< 2^{-1000}$), Bob can select arbitrary fake message $M' < n_A$ without checking condition $\gcd(M', n_A) = 1$.

From the ciphertext C_1 the coercive attacker is able to calculate the value $K' = C_1M'^{-1} \bmod n_A = MKM'^{-1} \bmod$

n_A for which the following inequality holds $M'K'Q' \bmod n_B \neq MKQ \bmod n_B$. However for the coercer it is computationally infeasible to disclose Bob's lie because of the probabilistic encryption performed at step 2. Indeed, the ciphertext C_2 depends on the random value ρ, therefore to demonstrate inequality $M'K'Q' \bmod n_B \neq MKQ \bmod n_B$ one should to compute 2^{128} different values $C_2^* = ((M'K'Q' \bmod n_B)||\rho)^{e_B} \bmod n_B\pi$ to show that for all possible values of the parameter ρ it always holds the inequality $C_2^* \neq C_2$.

Thus, the described protocol in receiver-deniable one and its resistance to coercive attack has the same order as computational difficulty of the problem of factoring modulus n_A.

C. Sender&receiver-side public key DE protocol

In the proposed sender-side and receiver-side public-key DE protocol there are used public keys of both the sender and the receiver (fig. 3), i.e. Alice's public key (n_A, e_A) and Bob's public key (n_B, e_B) that satisfy the condition $n_A > n_B$. The proposed DE scheme represents a three-pass protocol described as follows.

1) To send the secret message M, where $M < n_B$, Alice generates her local key K as a random value $K < n_B$ such that $\gcd(K, n_B) = 1$ and computes the value $C = MK \bmod n_B$ and the ciphertext

$$C_1 = (C||\rho)^{e_B} \bmod n_B\pi = ((MK \bmod n_B)||\rho)^{e_B} \bmod n_B\pi.$$

Then she sends the ciphertext C_1 to Bob.

2) Using his private key d_B Bob decrypts the ciphertext C_1: $C||\rho = C_1^{d_B} \bmod n_B\pi$, generates a random value $Q < n_B$ such that $\gcd(Q, n_B) = 1$ and computes the ciphertexts

$$C_2' = CQ \bmod n_B = MKQ \bmod n_B.$$

and

$$C_2 = ((C_2')||\rho)^{e_A} \bmod n_A\pi.$$

Then he sends the value C_2 to Alice.

3) Alice decrypts the ciphertext $C_2 : C_2'||\rho = (MKQ \bmod n_B)||\rho = (C_2)^{d_A} \bmod n_A\pi$, where d_A is Alice's private key. Then she computes the ciphertext

$$C_3' = C_2'K^{-1} \bmod n_B = MQ \bmod n_B$$

and

$$C_3 = (C_3')||\rho)^{e_B} \bmod n_B\pi = ((MQ \bmod n_B)\,||\rho)^{e_B} \bmod n_B\pi$$

and sends the last value to Bob.

Bob decrypts the ciphertext C_3 : $(MQ \bmod n_B)\,||\rho = (C_3)^{d_B} \bmod n_B\pi$ and discloses the secret message M as follows: $M = (MQ \bmod n_B)Q^{-1} \bmod n_B$.

This protocol combines the protocols from Subsections 3.1 and 3.2 and it is easy to see that the last protocol resists the sender-side and the receiver-side coercive attacks. However one should indicate that it does not resist attack at which Alice and Bob are coerced simultaneously since in this case they have to select the same fake message, otherwise their lie will be evident to the coercer. This is a common problem for flexible DE protocols [17], [18] that provide possibility to select arbitrary fake messages. Bi-deniability in the sense of resistance to attack at which sender and receiver are coerced simultaneously is provided with the plan-ahead public-key DE protocols described in papers [11], [3].

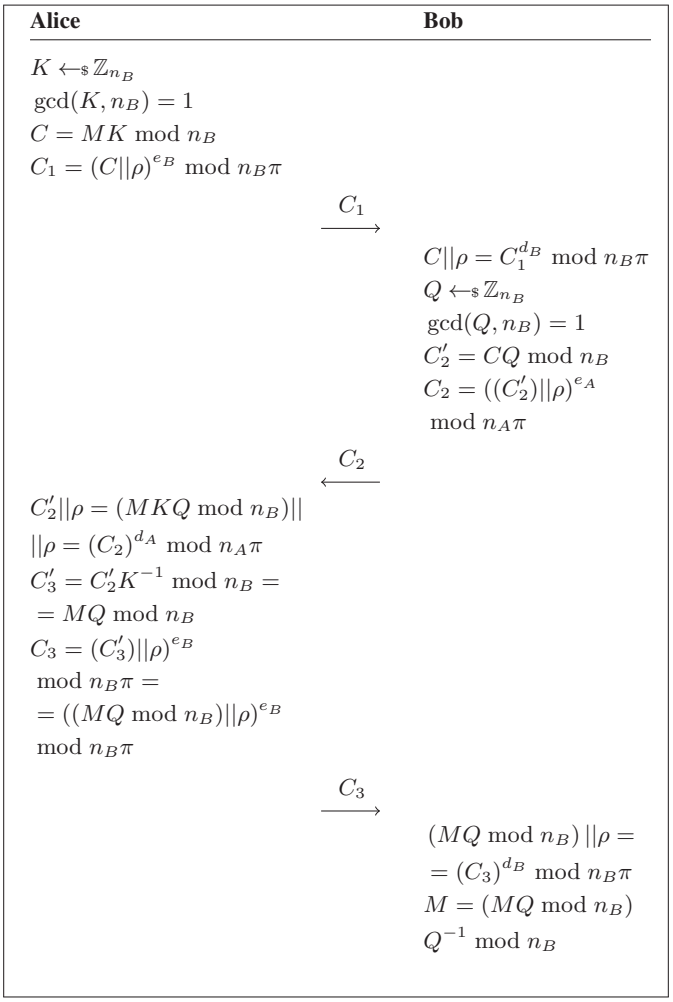

Fig. 3. Flexible receiver-side deniable public-key encryption protocol

To provide resistance to the attack in which sender and receiver are coerced simultaneously as well as to active coercive attacks we propose the plan-ahead public-key DE scheme described in next section.

IV. Plan-ahead public-key DE protocol

Suppose Alice and Bob are users of the RSA cryptosystem; the pair of numbers (n_A, e_A) is Alices public key; d_A is her private key; (n_B, e_B) is Bobs public key; d_B is his private key. Besides, Alices and Bobs public keys are such that the numbers $P_A = 2n_A + 1$ and $P_B = 2n_B + 1$ are primes and order of the number 7 is equal to $2n_A$ or n_A modulo P_A and is equal to $2n_B$ or n_B modulo P_B. Earlier primes with such structure were used in papers [19], [20]. To provide secure transmission of the secret message from Alice to Bob they can use the DE protocol that includes the following steps (see fig. 4 in which

the steps of generation and verification of digital signatures are omitted):

1) Alice selects a 512-bit random value k_A and computes $R_A = 7^{k_A} \bmod P_B$ and sends the value R_A to Bob as her random choice.

2) Bob selects a 512-bit random number k_B, calculates the value $R_B = 7^{k_B} \bmod P_B$ and his signature S_B to the sum $(R_A + R_B \bmod n_B)$:

$$S_B = (R_A + R_B)^{d_B} \bmod n_B.$$

Then he transmits the values R_B and S_B to Alice.

3) Alice verifies validity of Bobs signature to the value $(R_A+R_B \bmod n_B)$. If the signature S_B is false she terminates the protocol. If the signature S_B is valid, she computes her signature S_A to the value $(R_A + R_B \bmod n_B)$:

$$S_A = (R_A + R_B)^{d_A} \bmod n_A.$$

Then Alice select a fake message M, calculates the values

$$Z_A = R_B^{k_A} \bmod P_B, V = TZ_A \bmod n_B,$$
$$C_1 = (M + V)^{e_B} \bmod n_B, C_2 = V^{e_B} \bmod n_B.$$

Then Alice sends the ciphertext (C_1, C_2) and signature S_A to Bob.

4) Bob verifies validity of Alices signature to the value $(R_A+R_B \bmod n_B)$. If the signature S_A is false he terminates the protocol. If the signature S_A is valid, he computes the values

$$Z_B = R_A^{k_B} \bmod P_B; \quad V = C_2^{d_B} \bmod n_B.$$

Then Bob computes the value

$$T' = VZ_B^{-1} \bmod n_B$$

that is equal to T, i.e. he discloses the secret message T sent by Alice.

This protocol performs correctly. Correctness proof is as follows:

$$\left.\begin{array}{l} Z_B \equiv R_A^{k_B} \equiv 7^{k_A k_B} \bmod P_B \\ Z_A \equiv R_B^{k_1} \equiv 7^{k_B k_A} \bmod P_B \end{array}\right\} \Rightarrow Z_B = Z_A \Rightarrow$$
$$T' \equiv VZ_B^{-1} \equiv VZ_A^{-1} \equiv$$
$$\equiv TZ_AZ_A^{-1} \equiv T \bmod n_B$$
$$\Rightarrow T' \equiv T.$$

V. Discussion

A particular design feature of the protocols described in Section 3 is using commutative encryption function, like in the well known three-pass no-key protocols. Like in the lasts, in the proposed DE protocols the commutative encryption is performed with local keys selected by each party of the communication session independently. The local keys play the role of input randomness of the DE scheme which should be computed to provide relation of the selected fake message with the ciphertexts send during the communication session. Other significant feature of the proposed three-pass public-key DE protocols is performing *probabilistic* public-key encryption providing randomization of the ciphertexts that restricts significantly possibilities of the coercer. Due to these two design

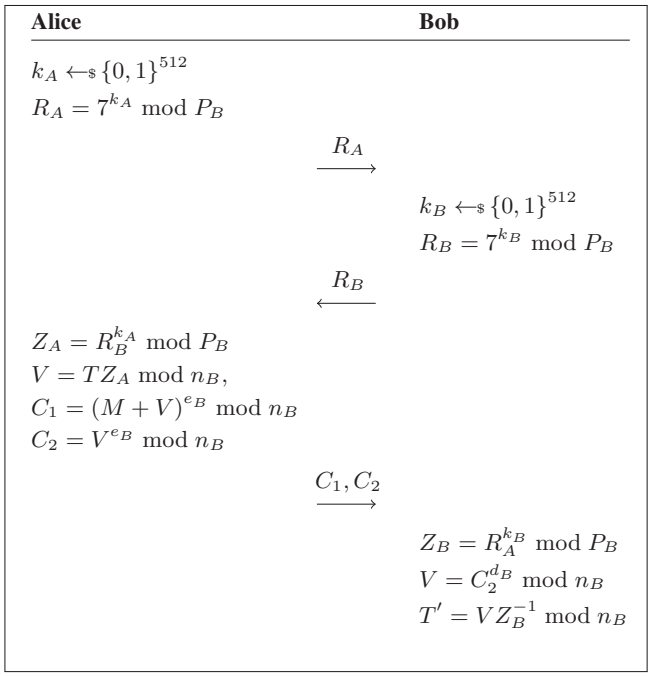

Fig. 4. Flexible receiver-side deniable public-key encryption protocol

features flexibility of the DE protocols has been provided together with the super-polynomial security against sender-side and receiver-side coercive attacks. Comparing the proposed DE protocols with the flexible DE scheme from papers [12], [21], [22] one can conclude that the first are more practical.

The protocols from Section 3 do not resist simultaneous coercion of the both parties of the communication session, i.e. the protocol from Subsection 3.3 is not fully bi-deniable. To provide full bi-deniability in the DE protocol from Section 4 it is used selection of the fake message at moment of performing the protocol. To provide resistance to active attacks of the potential coercer that protocol includes operations of the mutual entity authentication. If a party of the protocol is unable to confirm its validity the other party terminated the process of performing the protocol. At steps 2 and 3 Alice verifies validity of Bob and at steps 3 and 4 Bob verifies validity of Alice. Actually, the active coercer is detected before performing procedures connected directly with the deniable encryption.

Thus, security of the proposed protocol against active attacks is provided due to performing the authentication stage. Alice sends the ciphertext to Bob only after his proving ability to sign correctly the value $R_A + R_B \bmod n_B$ that depends on Alices random choice R_A. Correspondingly, Bob decrypts the ciphertext only after Alices proving her authenticity with her valid signature to the value $R_A + R_B \bmod n_B$ that depends on Bobs random choice R_B.

Besides serving as random requests, the values R_A and R_B are used by Alice and Bob to perform a hidden public key agreement procedure that allows them to compute the single-use shared key Z, the last being applied to encrypt the secret message T. Actually, the values R_A and R_B are computationally indistinguishable from uniformly random ones, therefore attacker is unable to show that these values play the role of the

single-use public keys computed depending on some single-use private keys k_A and k_B, correspondingly. The masked single-use public keys R_A and R_B are used for computing the single-use shared key $Z = Z_A = Z_B$. In its turn the single-use shared key Z is applied to compute some pseudo-random value $V = TZ \bmod n_B$ that contains the secret message T and is used for randomizing the encryption of the fake message M.

At time of bi-side simultaneous coercive attack Alice and Bob have possibility to declare plausible about their using the following probabilistic public-key encryption algorithm:

1) Generate a random number W,

2) Encrypt the message M as fallows: $C_1 = (M + W)^{e_2} \bmod n_2$,

3) Encrypt the value W as fallows: $C_2 = W^{e_2} \bmod n_2$.

It can be potentially selected the value W such that $W = V$, therefore the associated probabilistic encryption algorithm can potentially generate the ciphertext produced by the public-key DE protocol.

At time of coercive attack Bob opens to coercer both the message M and his private key d_B. However the coercer can open only the randomization parameter V that connects plausible the fake message M and the ciphertext (C_1, C_2). For an arbitrary plaintext T' there exists a single-use key Z' such that $V = T'Z' \bmod n_B$. To disclose the secret message coercer need to know at least one of the values k_A and k_B, i.e. he should compute the discrete logarithm $\log_7 R_1 \bmod P_B$ or $\log_7 R_B \bmod P_B$. It is supposed Alice and Bob generate their public keys so that the primes P_A and P_B have sufficiently large size: more than 1024 bits (2500 bits) in the case of providing 80-bit (128-bit) resistance to simultaneous bi-side coercive attack. One soul note that the number $P_B - 1$ contains large prime factors (numbers p and q), and number 7 has a large order ω ($\omega \geq p_B q_B$) for arbitrary values p_B and q_B with probability very close to 1. Due to large value ω, the discrete logarithm problem is computationally difficult and it is supposed the coercer is not able to find discrete logarithms modulo P_B.

VI. Conclusion

There have been proposed flexible sender-side, receiver-side, and sender&receiver-side DE protocols that are very attractive from practical point of view due to their providing super-polynomial resistance to coercive attacks and comparatively high performance. The proposed design can be potentially extended on the case of combining the commutative functions with probabilistic public-key encryption based on computational difficulty of the discrete logarithm problem on an elliptic curve. This case will give potentially exponential resistance to coercive attack. Besides, this research direction can give DE protocols more suitable for using standard public-key infrastructure, like plan-ahead public-key DE protocol introduced in paper [23].

It has been also proposed fully bi-deniable public encryption protocol with plan-ahead fake message, which is secure against active attacks. The last DE scheme includes steps of the entity mutual authentication in frame of which the parties of the protocol they hide execution of the procedure of exchanging the single-use public keys. The lasts are used to mask the ciphertext containing the secrete message.

References

[1] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption", *in Proc. Adv. in Cryptol.–CRYPTO'97*, vol. 1294, 1997, pp. 90-104.

[2] A.A. Moldovyan, N.A. Moldovyan, D.N. Moldovyan, V.A. Shcherbacov, "Stream Deiable-Encryption Algorithm Satisfying Criterion of the Computational Indistinguishability from Probabilistic Ciphering", *Comput. Sci. J. of Moldova*, vol. 24, no. 1, 2016, pp. 68-82.

[3] N.A. Moldovyan, A.A. Moldovyan, V.A. Shcherbacov, "Generating Cubic Equations as a Method for Public Encryption", *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, vol. 79, no. 3, 2015, pp. 60-71.

[4] 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", *J. of Netw.*, vol. 5, 2009, pp. 370-377.

[5] B. Meng, J. Wang, "An efficient receiver deniable encryption scheme and its applications", *J. of Netw.*, vol. 6, 2010, pp. 683-690.

[6] Y. Ishai, E. Kushilevitz, R. Ostrovsky, M. Prabhakaran, A. Sahai, "Efficient non-interactive secure computation", *Adv. in Cryptol.–EUROCRYPT 2011*, vol. 6632, 2011, pp. 406-425.

[7] A. ONeill, C. Peikert, B. Waters, "Bi-deniable public-key encryption", *in Adv. in Cryptol.–CRYPTO 2011*,, vol. 6841, 2011 pp. 525-542.

[8] B. Meng, J. Wang, "A receiver deniable encryption scheme", *in Int. Symp. on Inf. Proc. (ISIP09)*, 2009, pp. 254-257.

[9] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption", *in SOFSEM 2008: Theory and Pract. of Comput. Sci.*, 2008, pp. 599-609.

[10] M.H. Ibrahim, "Receiver-deniable public-key encryption", *Int. J. of Netw. Secur.*, vol. 2, 2009, pp. 159-165.

[11] A.A. Moldovyan, N.A. Moldovyan "Practical Method for Bi-Deniable Public-Key Encryption", *Quasigroups and related systems*, vol. 22, 2014, p. 277-282.

[12] M.T. Barakat, "A New Sender-Side Public-Key Deniable Encryption Scheme with Fast Decryption", *KSII T Internet Info*, vol. 8, no. 9, 2014, pp. 3231-3249.

[13] M.H. Ibrahim, "A method for obtaining deniable public-key encryption", *Int. J. of Netw. Secur.*, vol.1, 2009, pp. 1-9.

[14] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC press, 1996.

[15] R.L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Comm. of the ACM*, vol. 21, 1978, pp. 120-126.

[16] J. Gordon, "Strong primes are easy to find', *in Proc. Adv. in Cryptol.–EUROCRYPT 84*, 1984. pp. 216-223.

[17] D. Dachman-Soled "On minimal assumptions for sender-deniable public key encryption", *LNCS*, vol. 8383, 2014, pp. 574-591.

[18] D. Dachman-Soled "On the impossibility of sender-deniable public key encryption", *IACR Cryptol. ePrint Archive*, 2012:727, 2012.

[19] N.A. Moldovyan, "An approach to shorten digital signature length', *Comput. Sci. J. of Moldova*, vol. 14, no. 3(42), 2006,pp.390-396.

[20] A.A. Moldovyan , N.A. Moldovyan, V.A. Shcherbacov, "Short signatures from difficulty of the factoring problem', *Buletinul Academiei de Stiinte a Republicii Moldova. Matematica*, no. 2(72)-3(73), 2013, pp. 27-36.

[21] A. Sahai, B. Waters, "How to use indistinguishability obfuscation: Deniable encryption and more", *IACR Cryptol. ePrint Archive*, 2013:454, 2013.

[22] D. Markus, D.M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction", *in Proc. Adv. in Cryptol.–EUROCRYPT 2011*, 2011, vol. 6632, pp. 610-626.

[23] N.A. Moldovyan, A.N. Berezin, A.A. Kornienko, A.A. Moldovyan, "Bi-deniable public-encryption protocols based on standard PKI", *in Proc. 18th FRUCT ISPIT Conf.*, April 2016, pp. 212-219.