Quasigroups and Related Systems **22** (2014), 277 – 282

Practical method for bi-deniable public-key encryption

Nikolay A. Moldovyan and Alexander A. Moldovyan

Abstract. There is considered a practical method for public-key deniable encryption that is free from using any shared key. The method is based on using the public-key encryption algorithm producing the cryptogram that is computationally indistinguishable from the ciphertext produced by some probabilistic public-key encryption algorithm. The last is called probabilistic encryption algorithm associated with the deniable encryption. The proposed algorithm provides deniability when coercive adversary attacks both the party sending message and the party receiving message.

1. Introduction

The notion of *public-key deniable encryption* was introduced by Canett et al. in 1997 [1] as cryptographic primitive for using in cryptographic protocols providing security against so called coercive attacks. There are considered sender-deniable, receiver-deniable, and sender- and- receive-deniable (bi-deniable) schemes in which coercive adversary attacks the party sending message, the party receiving message, and the both parties, correspondingly. In the model of the coercive attack it is supposed that coercive adversary has power to force a party or the both parties simultaneously to open all the private information relating to the cryptogram (ciphertxt) after it has been sent, i.e. to open the message and private keys corresponding the public keys used while encrypting the message. The schemes proposed in [1] show potential possibility of providing security against coercive attacks, however they do not suite well for practical application because of their low performance. Potential practical applicability of the public-key deniable encryption for preventing vote buying in the internet-voting systems [5] and to provide secure multiparty computations [3] initiated a lot of investigations on developing secure and practical methods for the public-key deniable encryption [4,6,7]. The common feature of the deniable encryption schemes is possibility to decrypt the ciphertext c in different ways, while using the private key corresponding to the public key used for encryption of the secret message t. Such possibility is possible

2010 Mathematics Subject Classification: 11T71, 94A60, 94A62
Keywords:Cryptographic algorithms, public-key encryption, deniable encryption, probabilistic ciphering, hash-functions, discrete logarithm problem, entity authentication.
This work was financially supported by Government of Russian Federation, Grant 074-U01.

due to using local random value r in the encryption process. In the case of attack a fake message m is to be opened to coercive adversary and it is to be demonstrated that the public encryption of the message$m$ with using some random value $r' \neq r$ produces the ciphertext c (this is to be done by the sender) and decryption of the ciphertext c with using the private key produces the fake message$m$ (this is to be done by the receiver). In the case of bi-deniable schemes both the sender and the receiver should open the same fake message.

In the literature there are known public-key deniable encryption methods that differ in the following: i) in using interactive mechanism of the message sending (interactive schemes), ii) in using secret key shared by sender and receiver of the secret message (shared-key schemes), and iii) in selecting the fake message before performing the encryption (plan-ahead deniable encryption schemes). For practical application it is interesting to use the schemes that are free from using any shared key and from using many interactive passes of the sending message protocol. Example of such schemes is presented in [6]. However that scheme uses both the private key of the receiver and private key of the sender. Besides, that scheme does not provide bi-deniability.

The present paper proposes a new method for plan-ahead public-key deniable encryption that uses only receiver's public key in the encryption process and provides bi-deniability. The described method uses no shared secret key and can be implemented on the base of currently existing public key infrastructures. The method includes two interactive steps and performs both the authentication of the sender and the deniable encryption.

The paper is organized as follows. Section 2 describes the model of the coercive adversary and the design criteria. Section 3 describes the proposed method based on the computational indistinguishability between the deniable encryption and the probabilistic one. Section 4 discusses the practical applicability and the bi-deniability provided by the method. Section 5 concludes the paper.

2. Model of the coercive attack and design criteria

There is assumed the model of the coercive attack in which, after ciphertext has been sent from the sender to the receiver of the message, the coercive adversary has possibility to force both the sender and the receiver to open the following:

- the plaintext corresponding to the ciphertext;
- the private keys of both the receiver and the sender.
- the decryption algorithm output of which depends on each bit of ciphertext.

In the last item it is assumed that the output of the opened decryption algorithm represents the opened plaintext (a fake message), while using the opened private keys. Besides, the adversary can send a ciphertext containing both the secret and the fake messages and then to force the receiver to disclose the ciphertext. If the receiver will not open the secret message known to adversary, then the last attack is considered as successful one, since the adversary is able to prove

that the receiver is lying.

To resist such attack the following design criteria are proposed for constructing a practical public-key deniable encryption scheme:

1) the scheme should include two interactive steps and perform authentication of the sender as its internal procedure;

2) the deniable encryption should be performed with using only receiver's public key and random values (i.e. the encryption process should be performed without using the public key of sender and without using a shared key);

3) a probabilistic public-key encryption algorithm should be associated with the deniable encryption algorithm and the ciphertext generated by the last algorithm should be computationally indistinguishable from the ciphertext generated by the first one.

3. Proposed method

Let Alice be the sender of the secret message t and Bob be the receiver. The generalized description the proposed method is illustrated by the following two-step protocol:

1. Bob generates a random value r and his signature $SignB(r)$ to r and sends $SignB(r)$ and r to Alice.

2. Alice verifies the signature $SignB(r)$. If the signature is valid, then she generates a fake message m and, using Bob's public key and r, encrypts simultaneously the messages t and m, and gets the ciphertext c that coincide with ciphertext generated by some probabilistic encryption of the fake message m with using Bob's public key and some random value $r' \neq r$. Then Alice computes her signature $SignA(c)$ to ciphertext c and sends the signature $SignA(c)$ and the ciphertext c to Bob.

After receiving the ciphertext Bob verifies the signature $SignA(c)$. If the signature is valid, then he accepts the ciphertext as that containing a message from Alice, otherwise he rejects the ciphertext. For practical implementation of the protocol it is supposed to use some standard public key infrastructure (PKI) to perform signature generation and signature verification procedures, for example, PKI relating to using the ElGamal digital signature algorithm [2] with public keys y computed as follows: $y = a^x \bmod p$, where p is a 2048-bit prime such that number $p-1$ contains a 256-bit prime divisor q, a is a primitive element modulo p, x is the private key. It is also supposed to implement the public encryption using the algorithm, like the ElGamal public encryption algorithm [2], and Bob's public key $y_B = a^{x_B} \bmod p$, where x_B is Bob's private key, i.e. the deniable encryption procedure uses the same PKI that is used for digital signatures.

To satisfy the design criteria in the proposed method at step 1 the value r is generated using the formula $r = a^k \bmod p$, where k is a randomly selected number $(1 < k < p-1)$. This gives possibility for Alice and Bob to compute the same pair of random values Z and K such that no other person can compute

one of these values, using the publicly known parameters and values sent via communication channel. The deniable encryption is performed so that it generates the same ciphertext as that generated by the following associated public encryption algorithm.

Associated public encryption algorithm.

1. Generate random values $r' < p$ and $w < p-1$ and compute the value $W = a^w \bmod p$.
2. Using Bob's public key y_B compute the value $Z = {y_B}^w \bmod p$.
3. Solve the following system of linear congruences with unknowns c_1 and c_2:

$$\begin{cases} Zc_1 + Z^2c_2 = m \bmod p \\ c_1 = r'c_2 \bmod p \end{cases}$$

4. Send to Bob the ciphertext represented by the triple (W, c_1, c_2).

Bob decrypts the ciphertext (W, c_1, c_2) into the fake message using the following algorithm.

Associated decryption algorithm.

1. Using his private key x_B Bob computes the value $Z = W^{x_B} \bmod p$.
2. Then he computes the fake message $m = Zc_1 + Z^2c_2 \bmod p$.

The proposed method for deniable encryption of the secret message $t < p$ is described as follows.

Two-pass public-key deniable encryption protocol.

1. Bob generates a random value $k < p-1$ and computes the value $r = a^k \bmod p$. Then he computes his signature $SignB(r)$ to r and sends the values $SignB(r)$ and r to Alice.

2. Alice verifies the signature $SignB(r)$. If the signature is invalid she terminates the communication session. Otherwise she generates a fake message $m < p$ and a random value $w < p-1$ and computes the value $W = a^w \bmod p$. . Then, using Bob's public key y_B and the value r, Alice computes the values $Z = {y_B}^w \bmod p$ and $K = r^w \bmod p$ and solves the following system of linear congruences with unknowns c_1 and c_2:

$$\begin{cases} Zc_1 + Z^2c_2 = m \bmod p \\ Kc_1 + K^2c_2 = t \bmod p \end{cases} .$$

Then Alice computes her signature $SignA(r)$ to message r and sends the signature $SignA(r)$ and the ciphertext $c = (W, c_1, c_2)$ to Bob. He verifies the signature $SignA(c)$. If the signature is invalid, then he rejects the ciphertext.

To compute the secret message Bob performs the following procedure.

Decryption algorithm.

1. Using the value k Bob computes the value $K = W^k \bmod p$.
2. Then he computes the secret message $t = Kc_1 + K^2c_2 \bmod p$.

In the case of the coercive attack Bob opens his private key and performs the following procedure.

Dishonest decryption algorithm.

1. Using his private key x_B Bob computes the value $Z = W^{x_B} \bmod p$.
2. Then he computes the fake message value $m = Zc_1 + Z^2c_2 \bmod p$.

4. Discussion

The proposed method implements design criteria 1, since Alice responses random request r sending her signature to ciphertext c that depends on r. It implements design criteria 2, since Alice's public key is not used at the stage of deniable encryption. Design criteria 3 is also evidently implemented and one can easily compute the random value $r' = c_1/c_2 \bmod p$ that defines the associated public encryption algorithm generates the cryptogram $c = (W, c_1, c_2)$ sent to Bob. The last criteria is essential for providing resistance of the method to the two-side coercive attack. In the case of such attack Alice opens the fake message m that after performing the associated public probabilistic encryption with using Bob's public key and random value r' defines formation of the ciphertext c. Correspondingly, Bob opens his private key with which the associated decryption algorithm outputs the fake message m, each bit of m being dependent on each bit of the ciphertext c.

Due to performing the sender authentication subprocedure the method resists the coercive attacks in which the adversary tries to initiate the deniable encryption protocol participating as sender and trying to convict Bob is lying. Attacks in which the coercive adversary tries to participate as receiver (suppose the adversary uses the values $SignB(r)$ and r sent by Bob earlier) and trying to convict Alice is lying are also not efficient, since Alice uses random value w that defines randomness of the values K and Z for each session of sending a secret message. In the case of the last attack Bob opens the fake message m and refers to using the associated probabilistic public encryption and random input r'. If the attacker is not able to solve the discrete logarithm problem in the $GF(p)$ finite field (it is assumed this problem is computationally intractable in the case of the used prime p), then he is not able to prove the ciphertext contains some other message different from m.

The proposed method for public-key deniable encryption represents interest for practical application due to the following its merits:

-it provides bi-deniability of the encryption;

-it is sufficiently fast (its performance is only about two times lower than performance of the ElGamal public encryption algorithm [2]);

-it is implemented as two-pass protocol in frame of which procedure of the receiver's authenticating the sender is performed;

-its overhead in terms of the cryptogram size is comparatively low (only 50% larger than the size of the ciphertext produced by the ElGamal public encryption algorithm while encrypting secrete message t);

-it can be easily implemented with using computations on elliptic curves and practically applied on the base of currently existing PKIs.

Implementation of the proposed method on the base of computational difficulty of the discrete logarithm problem on elliptic curve is of special practical interest,

such implementation has some peculiarities, connected with the fact that a random value x only with probability about 0.5 defines an abscissa of some elliptic curve point, though. However the general construction of the public-key deniable encryption protocol based on using computations on elliptic curve can remain the same, like described in section 3.

5. Conclusion

It has been proposed a practical and computationally efficient method for public-key deniable encryption. The method is implemented as two-pass protocol including mechanism for deniable encryption and mechanism for authenticating the sender of the ciphertext. Bi-deniability of the method is based on associating a probabilistic encryption algorithm with the deniable encryption algorithm in such a way that both algorithms produce the same ciphertext. Due to using authentication of the sender the method resists the coercive attacks in which the adversary masquerades as sender. Important merit of the proposed method is its using the standard PKI. The paper presents the implementation of the method with using computational difficulty of the discrete logarithm problem in the finite field $GF(p)$. It can be similarly implemented with using the discrete logarithm problem on elliptic curves, however detailed consideration of such implementation represents interest for independent research.

References

[1] **R. Canetti, C. Dwork, M. Naor, R. Ostrovsky**, *Deniable encryption*, Lecture Notes Comp. Sci. **1294** (1997), 394–104.

[2] **T. ElGamal**, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Information Theory **IT–31** (1985), 469–472.

[3] **Yu. Ishai, E. Kushilevits, R. Ostrovsky**, *Non-interactive secure computation*, Lecture Notes Comp. Sci. **6632** (2011), 406–425.

[4] **M. Klonowski, P. Kubiak, M. Kutyłowski**, *Practical deniable encryption*, Theory and Practice of Computer Science: Proc. 34th Confer. Current Trends in Theory and Practice of Computer Sci., 2008, 599–609.

[5] **Meng Bo**, *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 Networks **4** (2009), 370–377.

[6] **Meng Bo, Qing Wang Jiang**, *A receiver deniable encryption scheme*, Proc. 2009 Intern. Symp. Information, 2009, 254–257.

[7] **A. O'Neil, C. Peikert, B. Waters**, *Bi-deniable public-key encryption*, Lecture Notes Comp. Sci. **6841** (2011), 525–542.

Received Febuary 10, 2014

ITMO University,
Kronverksky pr., 10, St. Petersburg 197101, Russia
Email: nmold@mail.ru