BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(76), 2014, Pages 23–29
ISSN 1024–7696

Bi-Deniable Public-Key Encryption Protocol which is Secure against Active Coercive Adversary

A. A. Moldovyan, N. A. Moldovyan, V. A. Shcherbacov

Abstract. We consider a practical public-key deniable encryption protocol based on the RSA cryptosystem. The protocol begins with the authentication of the both parties participating in the protocol (the sender and the receiver of secret message). The authentication is performed by exchanging random values and the RSA signatures to them. Due to this stage of the protocol the security against coercive attacks of the active adversary is provided. After the mutual authentication the protocol specifies performing the deniable encryption of the secret message, like the probabilistic ciphering of some fake message by using the RSA encryption algorithm. The novelty of the proposed protocol consists in using random values as single-use public keys that are used to generate single-use shared key with which the sender encrypts the secret message and the receiver discloses it. The coercive adversary provided with private keys of the both parties can only disclose the fake message. Proving that the sent cryptogram contains a message different from the fake one is computationally infeasible for the adversary.

Mathematics subject classification: 11T71, 94A60.
Keywords and phrases: Cryptographic protocols, public-key encryption, deniable encryption, probabilistic ciphering, factoring problem, entity authentication.

1 Introduction

When considering security of the encryption algorithms used in the communication protocols against potential attacks performed by the adversary that has power to force sender, receiver, or the both parties to open the shared secret key (if symmetric encryption algorithm is used), the private key (if asymmetric encryption algorithm is used), or both the shared key and the private one (if some combined encryption algorithm is used) one can state that conversional encryption algorithms do not provide security against the mentioned coercive attacks. Paper [1] introduces the notion of deniable encryption as the cryptographic primitive of cryptographic protocols that resist the coercive attacks. The deniable encryption is a procedure of ciphering a secret message such that the produced ciphertext can be decrypted with opened keys into a fake message. To provide such property (deniability) random values or additional secret key (which is not opened to the coercive attacker) in the process of the deniable encryption are used. Besides the information protection in the telecommunication systems, the potential practical application of deniable encryption schemes relates to providing secure multiparty computations [2] and preventing vote buying in the internet-voting systems [3].

Majority of the papers related to the deniable encryption are devoted to the public-key deniable encryption [2, 4–6]. A possible deniable encryption scheme of such type is as follows. The secret message T is encrypted with public-encryption algorithm E and public key P using a random value R : $C = E_P(T, R)$, where C is the produced cryptogram. While being coerced the sender (receiver) opens to adversary the fake message M and another random value r such that $E_P(M, r) = C$, where $r \neq R$ (the receiver additionally opens his private key connected with the public key P). Thus, it is supposed that the coercer is not able to disclose the value R, i.e. the last value plays role of the single-use secret key that is shared by the sender and the receiver. In this paper we propose a deniable encryption protocol which provides bi-deniability in the case of opening *all used random values send via communication channel*.

In the known papers different types of the coercive attacks are considered in which the adversary is passive, i. e. he approaches the parties of the secret communication protocol after the ciphertext has been sent. The sender-deniable, receiver-deniable, and sender- and receive-deniable (bi-deniable) protocols are possible in which coercive adversary attacks only the sender, only the receiver, and the both parties, respectively. It is supposed that a party or the both parties simultaneously should open to adversary all the private information related to the cryptogram (ciphertext) after it has been sent. The encryption is deniable if both the sender and receiver have possibility not to open the secret message, i. e. to lie, and the coercer is not able to disclose their lies.

However the coercive adversary can undertake an active attack in which he will play the role of the sender or of the receiver and after sending the secret message he will demand to open him the message contained in the cryptogram and the private key. For example, acting as sender in the protocol the attacker can generate and send two messages, the secret one and the fake one. Then he can demand the receiver's opening the cryptogram and private key. If the receiver opens only one message, then the attack is considered successful, since the attacker is able to argue that the receiver lies, presenting alternative message contained in the cryptogram. The deniable encryption protocol proposed in the present paper provides security against the active attacks (here we not use the term *deniability* since authentic party stops the protocol before performing encryption of messages if an adversary tries to perform an active attack). The security is provided with the RSA signatures to random values send via the channel.

The present paper is organized as follows. Section 2 describes the model of the coercive attack and the design criteria for constructing the deniable encryption protocol. Section 3 describes the constructed deniable encryption protocol deniability of which is based on the computational indistinguishability between the deniable encryption procedure and the probabilistic ciphering of the fake message. The described protocol is based on the RSA cryptosystem (that is briefly described) to perform several passes of the protocol. Section 4 discusses the security and bi-deniability provided by the protocol. Section 5 concludes the paper.

2 Model of the coercive adversary and design criteria

The assumed model of the coercive attack is described by the following four items.

1. The adversary can impersonate some sender and initiate the deniable encryption protocol by using public key of the receiver and after a ciphertext has been sent he can force the receiver to open the received message and receiver's private key.

2. The adversary can impersonate some receiver and after the protocol terminates can force the sender to open the sent message and sender's private key (in the constructed protocol public keys of both the sender and the receiver of the message are used).

3. All data (cryptogram, random values et. al.) sent via communication channels become known to the adversary.

4. The adversary is not able to force a party to open private key before the deniable encryption protocol terminates.

To resist the attacks of the assumed adversary the deniable encryption protocol has been constructed with the following design criteria:

i) the protocol should include the stage of verifying the authenticity of both the sender and the receiver with using random values and the RSA digital signature scheme;

ii) the random values used at the authentication stage should be used as single-use public keys of the sender and of the receiver at the stage of deniable encryption; disclosing such use of the random values should be computationally infeasible for the coercive attacker;

iii) the single-use public keys should serve to compute single-use shared key;

iv) the single-use shared keys should be used for pseudo-randomizing the encryption process;

v) a probabilistic public-key encryption algorithm should be associated with the deniable encryption algorithm; the encryption should be performed using the RSA public key of the receiver;

vi) the ciphertext produced by the deniable encryption algorithm should be computationally indistinguishable from the ciphertext produced by the probabilistic encryption algorithm.

3 Proposed protocol

3.1 Cryptosystem RSA

The RSA public key cryptosystem [7] can be used for public encryption and for signing electronic messages. This cryptosystem is described as follows. The public key is represented by a pair of numbers $(n,\ e)$, where $n\ =\ pq$ is the product of two randomly chosen primes and e is a random number that is relatively prime with Euler phi function $\phi(n)\ =\ (p\ -\ 1)(q\ -\ 1)$. The triple $(p,\ q,\ d)$ is secret, where $d\ =\ e^{-1}\ \bmod \phi(n)$ is a private key. The encryption of some message $M\ <\ n$ is

performed using the public key as the computation of the value $C = M^e \mod n$ that is the output ciphertext of the public-key encryption procedure. The decryption of the cryptogram C is performed using the private key and the formula $M = C^d \mod n$. The RSA signature S to the message M is computed using the private key and the formula $S = M^d \mod n$. The verification of the signature is performed using public key and formula $M = S^e \mod n$. If the last equation holds, then the signature is accepted as a valid one.

Usually the documents to be signed have arbitrary size and are comparatively long. In such cases some specified hash-function F_H is used and the signature S to document M is generated as signature to the hash-value $H = F_H(M)$: $S = H^d \mod n$. The security of the RSA cryptosystem is based on the difficulty of factoring modulus n. Factoring n is a computationally difficult problem if the primes p and q are strong ones [8] and have large size. For example, using 512-bit (1232-bit) strong primes p and q one gets the security equal to 2^{80} (2^{128}) modulo n multiplication operations.

3.2 Public-key deniable encryption protocol

Let Alice be a sender of the secret message T and Bob be a receiver. Suppose also they are users of the RSA cryptosystem; the pair of numbers (n_1, e_1) is Alice's public key; d_1 is her private key; (n_2, e_2) is Bob's public key; d_2 is his private key. Besides, Bob public key is such that the number $P = 2n_2 + 1$ is prime and order of the number 3 is equal to $2n_2$ or n_2. Earlier primes with such structure were used in papers [9, 10]. The protocol designed using the design criteria declared in Section 2 includes the following steps:

1. Alice generates a random value k_1 and computes $R_1 = 3^{k_1} \mod P$ and sends the value R_1 to Bob as her random choice.

2. Bob generates a random value k_2, computes the value $R_2 = 3^{k_2} \mod P$ and his signature S_2 to the sum $(R_1 + R_2 \bmod n_2) : S_2 = (R_1 + R_2)^{d_2} \mod n_2$. Then he sends the values R_2 and S_2 to Alice.

3. Alice verifies Bob's signature to the value $(R_1 + R_2 \bmod n_2)$. If the signature S_2 is false she terminates the protocol. If the signature S_2 is valid, she computes her signature S_1 to the value $(R_1 + R_2 \mod n_2) : S_1 = (R_1 + R_2)^{d_1} \mod n_1$. Then Alice generates a fake message M, computes the values $Z_1 = R_2^{k_1} \mod P$, $V = TZ_1 \mod n_2$, $C_1 = (M + V)^{e_2} \mod n_2$, and $C_2 = V^{e_2} \mod n_2$, and sends the ciphertext (C_1, C_2) and signature S_1 to Bob.

4. Bob verifies Alice's signature to the value $(R_1 + R_2 \bmod n_2)$. If the signature S_1 is false he terminates the protocol. If the signature S_1 is valid, he computes the values $Z_2 = R_1^{k_2} \mod P$ and $V = C_2^{d_2} \mod n_2$. Then he computes the value $T' = VZ_2^{-1} \mod n_2$ that is equal to T, i.e. he discloses the secret message T sent by Alice. (Indeed we have the following: $Z_2 \equiv R_1^{k_2} \equiv 3^{k_1 k_2} \bmod P; Z_1 \equiv R_2^{k_1} \equiv 3^{k_2 k_1} \bmod P \Rightarrow Z_2 = Z_1 \Rightarrow T' \equiv VZ_2^{-1} \equiv VZ_1^{-1} \equiv TZ_1Z_1^{-1} \equiv T \mod n_2 \Rightarrow T' \equiv T$.)

4 Discussion

The presented protocol satisfies the design criteria formulated in Section 2:

i) Alice (Bob) proves her (his) authenticity by signing the value $(R_1+R_2 \bmod n_2)$ that depends on Bob's (Alice's) random choice; the signatures are computed using the RSA cryptoscheme;

ii) the random values R_1 and R_2 are connected with the single-use private keys k_1 and k_2 and actually represent the single-use public keys generated by Alice and Bob, correspondingly;

iii) the single-use public keys R_1 and R_2 are used at the stage of deniable encryption for computing the single-use shared key $Z = Z_1 = Z_2$;

iv) the single-use shared key Z is used for computing pseudo-random value $V = TZ \mod n_2$ that contains the secret message T and is used for randomizing the encryption of the fake message M;

v) a probabilistic public-key encryption algorithm associated with the deniable encryption algorithm is as follows:
– generate random value W,
– encrypt the message M with formula $C_1 = (M + W)^{e_2} \mod n_2$,
– encrypt the value W using formula $C_2 = W^{e_2} \mod n_2$;

vi) if $W = V$, then the associated probabilistic encryption algorithm generates the same ciphertext as that produced by the public-key deniable encryption algorithm; to distinguish between the probabilistic encryption and the deniable encryption one should open the value V and disclose the secret message T, however this is computationally infeasible. The 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 a random value. Respectively, Bob decrypts the ciphertext only after Alice's proving her authenticity with her signature to a value depending on Bob's random choice R_2. Thus, the active coercive attacker is detected before performing procedures connected directly with the deniable encryption. In the case of passive coercive attack the public-key encryption stage of the protocol is performed and the sender opens to coercer the fake message M. The receiver opens to coercer both the message M and private key d_2. However the coercer can open only the randomization parameter V that connects 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 $V = T'Z' \mod n_2$. To disclose the secret message coercer need to know at least one of the values k_1 and k_2, i.e. he should compute the discrete logarithm $\log_3 R_1 \mod P$ or $\log_3 R_2 \mod P$.

Since the prime P has a large size (more than 1025 bits (2465 bits) in the case of 80-bit (128-bit) security), the number $P-1$ contains large prime factors (numbers p and q), and number 3 has a large order ω ($\omega \geq pq$), the discrete logarithm problem is computationally difficult and it is supposed the coercer is not able to find discrete logarithms modulo P. Thus, the proposed protocol provides bi-deniability.

The considered protocol has the following merits:

– it is bi-deniable;

– it is sufficiently fast (its performance if only about two times lower than the rate of the RSA public-key encryption);

– its overhead in terms of the ciphertext size is comparatively low (only 100% larger than the ciphertext produced by the RSA encryption algorithm);

– it can be easily implemented in practice using the RSA public-key infrastructure.

5 Conclusion

A practical and computationally efficient bi-deniable public-key encryption protocol has been proposed. The bi-deniability of the method is based on associating a probabilistic public-key encryption algorithm with the deniable encryption algorithm in such a way that both algorithms produce the same ciphertext. One can suppose that the computational indistinguishability between the probabilistic and deniable encryption can serve as a novel design concept for constructing deniable encryption schemes of different types. Due to performing the authentication of the both parties of the protocol provides the security against active coercive attacks. Including in the protocol the user's authentication mechanism provides also a natural argumentation for using random values in the protocol. A novel item applied in the proposed protocol consists in using the mentioned random values as single-use public keys R_1 and R_2 and performing hidden key agreement subprotocol with which the sender and the receiver of the message obtain the single-use shared key Z. To distinguish the random values R_1 and R_2 from the random values that are generated directly the coercer should compute the discrete logarithm modulo P. The last means the deniability of the proposed protocol is based on the computational difficulty of finding discrete logarithms.

The first author was supported by Government of Russian Federation, Grant 074-U01 and the second author supported by the Board of Education of Russia.

References

[1] Canetti R., Dwork C., Naor M., Ostrovsky R. *Deniable Encryption.* Proceedings Advances in Cryptology – CRYPTO 1997. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 1997, vol. 1294, 90–104.

[2] Ishai Yu., Kushilevits E., Ostrovsky R. *Efficient Non-interactive Secure Computation.* Advances in Cryptology – EUROCRYPT 2011. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 2011, vol. 6632, 406–425.

[3] Bo 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. 2009, **4**, No. 5, 370–377.

[4] O'Neil A., Peikert C., Waters B. *Bi-Deniable Public-Key Encryption.* Advances in Cryptology – CRYPTO 2011. Lectute Notes in Computer Science. Springer–Verlag. Berlin, Heidelberg, New York, 2011, vol. 6841, 525–542.

[5] Klonowski M., Kubiak P., Kutylowsk M. *Practical Deniable Encryption* SOFSEM 2008: Theory and Practice of Computer Science, 34th Conference on Current Trends in Theory and Practice of Computer Science, Novy Smokovec, Slovakia, January 19–25, 2008, 599–609.

[6] Bo Meng, Jiang Qing Wang. *A Receiver Deniable Encryption Scheme*. Proceedings of the 2009 International Symposium on Information Processing (ISOP'09), Huangshan, China, August 21–23, 2009, 254–257.

[7] Rivest R.L., Shamir A., and Adleman L.M. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Communications of the ACM, 1978, **21**, No. 2, 120–126.

[8] Gordon J. *Strong primes are easy to find*. Advances in cryptology – EUROCRYPT'84, Springer-Verlag LNCS, 1985, vol. 209, 216–223.

[9] Moldovyan N. A. *An approach to shorten digital signature length*. Computer Science Journal of Moldova, 2006, **14**, No. 3(42), 390–396.

[10] Moldovyan A. A., Moldovyan N. A., Shcherbacov V. A. *Short signatures from difficulty of the factoring problem*. Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2013, No. 2(72)–3(73), 27–36.

Received April 2, 2014

A. A. Moldovyan
Saint-Petersburg National Research University
of Information Technologies, Mechanics and Optics
Kronverksky pr., 10, St.Petersburg, 197101
Russia
E-mail: *maa1305@yandex.ru*;

N. A. Moldovyan
Saint-Petersburg Electrotechnical University "LETI"
Prof. Popova str., 5, St.Petersburg, 197342
Russia
E-mail: *nmold@mail.ru*;

V. A. Shcherbacov
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD−2028 Chişinău
Moldova
E-mail: *scerb@math.md*; Web: *www.scerb.com*