Computer Science Journal of Moldova, vol.**23**, no.1(67), 2015

Provably sender-deniable encryption scheme*

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

Abstract

The use of the well known provably secure public-key cryptoscheme by Rabin is extended for the case of the deniable encryption. In the proposed new sender-deniable encryption scheme the cryptogram is computed as coefficients of quadratic congruence, the roots of which are two simultaneously encrypted texts. One of the texts is a fake message and the other one is a ciphertext produced by public-key encryption of secret message. The proposed deniable encryption method produces a ciphertext that is computationally indistinguishable from the ciphertext produced by some probabilistic public-key encryption algorithm applied to the fake message.

Keywords: cryptography, ciphering, deniable encryption, public key, public encryption, probabilistic encryption

1 Introduction

Article [1] introduces the notion of public-key deniable encryption as cryptographic primitive that resists the attacks performed by the coercive adversary that intercepts ciphertext and has power to force sender, receiver, or both parties to open the ciphertext and disclose the encryption key and random values used while encrypting the plaintext. In scientific literature the sender-deniable [2], receiver-deniable [3], and sender- and- receive-deniable (bi-deniable) [4] schemes in which coercive adversary attacks the sending message party, the receiving message party, and both parties, respectively, are considered.

©2015 N.A. Moldovyan, A.A. Moldovyan, V.A. Shcherbacov

* This work was supported by Russian Foundation for Basic Research, project Ref. Nr. 14-07-00061-a

The encryption is deniable if the sender or/and receiver has the possibility not to open the secret message, i.e. to lie, and the coercer is not able to disclose their lie.

In particular, the public-key encryption protocol (algorithm) is called sender-deniable if the sender is able to disclose the fake plaintext and the fake random value that defines transformation of the fake plaintext into the cipher text intercepted by the adversary using the receiver's public key. One of the important problems relating to the deniable encryption schemes is justifying their deniability [5], i.e. computational infeasibility for the coercive adversary to prove the ciphertext can be decrypted into a message different from the fake message.

The present paper proposes a new sender-deniable encryption scheme that has provable deniability. The scheme is based on using the computational indistinguishability between the deniable encryption procedure and the probabilistic ciphering of the fake message.

2 A new method for public-key encryption

2.1 Encryption on the base of quadratic equations

In the proposed public-key encryption method it is used computational difficulty of finding square roots modulo composite number $n = pq$, where p and q are two strong primes composing the private key, like in the Rabin public-key cryptoscheme [6]. The value n represents the public key. If the values x_1 and x_2 are roots of the quadratic congruence $x^2 - Ax + B \equiv 0$ modulo n, then this polynomial can be written as $(x - x_1)(x - x_2)$, i.e. $x^2 - Ax + B \equiv (x - x_1)(x - x_2) \equiv x^2 - (x_1 + x_2)x + x_1x_2 \mod n$, $A \equiv (x_1 + x_2) \mod n$ and $B \equiv x_1x_2 \mod n$.

Thus, if two messages R and Z are required to be the roots of some quadratic congruence, the coefficients should be given as follows: $A = (R + Z) \mod n$ and $B = RZ \mod n$.

The last two formulae define an encryption procedure of simultaneous encryption of the messages R and Z, which outputs the cryptogram in the form of the pair of numbers (A, B). Decryption of the cryptogram $C = (A, B)$ can be performed as solving the following

quadratic congruence:

$$x^2 - Ax + B \equiv 0 \mod n. \tag{1}$$

Congruence (1) can be solved using the secret key (p, q) in the following way. The following two congruences are solved: $x^2 - Ax + B \equiv 0 \mod p$ and $x^2 - Ax + B \equiv 0 \mod q$, each of which has two roots. The roots of the first congruence are the following two values:

$$x_{p1} = \frac{A}{2} + \sqrt{\frac{A^2}{4} - B} \mod p \quad \text{and} \quad x_{p2} = \frac{A}{2} - \sqrt{\frac{A^2}{4} - B} \mod p.$$

The roots of the second congruence have the following two values

$$x_{q1} = \frac{A}{2} + \sqrt{\frac{A^2}{4} - B} \mod q \quad \text{and} \quad x_{q2} = \frac{A}{2} - \sqrt{\frac{A^2}{4} - B} \mod q.$$

Four roots X_1, X_2, X_3, and X_4 of the congruence (1) are computed as solutions of the following four systems of linear congruences:

$$\begin{cases} X_1 \equiv x_{p1} \mod p \\ X_1 \equiv x_{q1} \mod q, \end{cases} \quad \begin{cases} X_2 \equiv x_{p1} \mod p \\ X_2 \equiv x_{q2} \mod q, \end{cases}$$

$$\begin{cases} X_3 \equiv x_{p2} \mod p \\ X_3 \equiv x_{q1} \mod q, \end{cases} \quad \begin{cases} X_4 \equiv x_{p2} \mod p \\ X_4 \equiv x_{q2} \mod q. \end{cases}$$

In accordance with the Chinese remainder theorem these systems have the following four solutions, respectively:

$$\begin{aligned} X_1 &= (x_{p1} q (q^{-1} \mod p) + x_{q1} p (p^{-1} \mod q)) \mod n, \\ X_2 &= (x_{p1} q (q^{-1} \mod p) + x_{q2} p (p^{-1} \mod q)) \mod n, \\ X_3 &= (x_{p2} q (q^{-1} \mod p) + x_{q1} p (p^{-1} \mod q)) \mod n, \\ X_4 &= (x_{p2} q (q^{-1} \mod p) + x_{q2} p (p^{-1} \mod q)) \mod n. \end{aligned}$$

Evidently, two of the four roots X_1, X_2, X_3, and X_4 are equal to the values Z and R. Two other roots represent random values that are to be discarded.

2.2 Encryption on the base of cubic equations

One can also implement encryption process as generating coefficients of some cubic equation, three roots of which represent three independent messages M, T and U. If the last values are to be roots, then one can write

$$(x-M)(x-T)(x-U) = x^3 - (M+T+U)x^2 + \\ (MT+MU+TU)x - MTU = 0 \mod n$$

and the encryption process consists in computing coefficients

$$A = M+T+U \mod n,\ B = MT+MU+TU \mod n, \\ A = MTU \mod n.$$

Decryption of the cryptogram (M, T, U) is to be performed as solving the following cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \mod n. \tag{2}$$

The owner of public key n using his private key (p, q) is able to find roots of the last equation. For this purpose he solves cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \mod p \tag{3}$$

and cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \mod q. \tag{4}$$

To find the roots of the cubic equation (3) over the prime field $GF(p)$, we propose to solve the equation $(1,0)x^3 - (A,0)x^2 + (B,0)x - (D,0) = (0,0)$ over the extension field $GF(p^2)$ that is given evidently in the vector form [7]. This method gives three roots computed using the following standard (up to designations) formula [8]:

$$(x,0) = \frac{(A,0)}{3} + \sqrt[3]{-\frac{\mathbf{Q}}{2} + \sqrt{\frac{\mathbf{Q}^2}{4} + \frac{\mathbf{P}^3}{27}}} + \sqrt[3]{-\frac{\mathbf{Q}}{2} - \sqrt{\frac{\mathbf{Q}^2}{4} + \frac{\mathbf{P}^3}{27}}}, \tag{5}$$

where $\mathbf{P}$ and $\mathbf{Q}$ are elements of the field $GF(p^2)$; $\mathbf{P} = (P, 0) = (B, 0) - \frac{(A,0)^2}{3}$ and $\mathbf{Q} = (Q, 0) = \frac{(A,0)(B,0)}{3} - \frac{2(A,0)^3}{27} - (D, 0)$. In general case the value $\frac{Q^2}{4} + \frac{P^3}{27}$ can be equal to a quadratic non-residual in the field $GF(p)$, therefore computation in (5) is to be performed in the field $GF(p^2)$.

In the case under consideration $p > 3$, therefore number 3 divides the value $p^2-1 = (p-1)(p+1)$ and there exist three different cubic roots in $GF(p^2)$ for each of the values $-\frac{\mathbf{Q}}{2} + \sqrt{\frac{\mathbf{Q}^2}{4} + \frac{\mathbf{P}^3}{27}}$ and $-\frac{\mathbf{Q}}{2} - \sqrt{\frac{\mathbf{Q}^2}{4} + \frac{\mathbf{P}^3}{27}}$. The last gives three vectors $(x_1, 0)$; $(x_2, 0)$; and $(x_3, 0)$ computed from equation (5) which define three solutions x_1; x_2; and x_3 of equation (3).

Let x_{1p}, x_{2p}, and x_{3p} be the roots of equation (3) and x_{1q}, x_{2q}, and x_{3q} be the roots of equation (4). Then nine roots of the equation (2) can be computed solving nine systems of the congruences of the following form:

$$\begin{cases} X_{ij} \equiv x_{ip} \mod p \\ X_{ij} \equiv x_{jq} \mod q, \end{cases}$$

where $i, j \in \{1, 2, 3\}$. Three of the computed roots are equal to the values M, T and U that represent messages sent to the owner of public key n.

3 Deniable encryption and associated probabilistic ciphering

The encryption scheme described in the previous section can be used as deniable encryption method. For this purpose the sender of the secret message T is previously to generate a fake message (the message planned for presenting to the coercive attacker) and then, using the public key n of the receiver, to compute the pseudorandom value $R = T^2 \mod n$ and to encrypt simultaneously the values M and R. In such encryption method it is supposed that only the receiver has the possibility to compute the value T from the value R using his private key (p, q). It is so if the secret message T is sufficiently large, for ex-

ample, $n \mod 2^{128} < T < n$. In the case of short secret messages, for example, $n^{1/2} < T < 2^{20}n^{1/2}$, finding T from R without knowing the secret key (p, q) takes about 2^{40} multiplication operations. To provide the possibility to encrypt short secret messages, one can propose the following modified formula for computing the value R from the value T: $R = (2^{-1} - T)^2 \mod n$. In its turn, to provide more secure encryption of the message M, the second root of the considered quadratic congruence is defined in the form $Z = (R - M) \mod n$.

Thus, we have come to the following deniable encryption protocol using receiver's public key n which includes the following steps:

1. The pseudorandom value $R = (2^{-1} - T)^2 \mod n$ is computed.
2. The fake message M is formed.
3. The value $A = (2R - M) \mod n$ is computed.
4. The value $B = R(R - M) \mod n$ is computed.
5. The ciphertext $C = (A, B)$ is send to the receiver via a public communication channel.

The receiver performs the decryption procedure as follows:

1. The receiver using his private key (p, q) computes four roots X_1, X_2, X_3, and X_4 of the congruence $x^2 - Ax + B \equiv 0 \mod n$.
2. He computes the values M_1, M_2, M_3, and M_4 using the formula $M_i = (2X_i - A) \mod n (i = 1, 2, 3, 4)$.
3. He rejects three random messages from the set $\{M_1, M_2, M_3, M_4\}$. Let the fourth (sensible) message represent the message M.
4. Then the receiver using his private key (p, q) computes the value $R = (M + A)/2 \mod n$ and four quadratic roots S_1, S_2, S_3, and S_4 from R modulo n.
5. He discloses the secret message computing the values $T_i = (2^{-1} - S_i) \mod n$, where $i = 1, 2, 3, 4$; and selecting the sensible message T from the set $\{T_1, T_2, T_3, T_4\}$.

Distinguishing the pseudorandom value R from a random choice is computationally infeasible without knowing the private key of the receiver of the message. Therefore the sender, while being coerced, can reasonably invoke to the use of the following probabilistic public-key encryption algorithm for enciphering the fake message M:

1. Generate random value $R_\phi < n$.

2. Compute the value $A = (2R_\phi - M) \mod n$.
3. Compute the value $B = R_\phi(R_\phi - M) \mod n$.

The last algorithm (that can be called the associated probabilistic public-key encryption algorithm) outputs the same ciphertext $C = (A, B)$ as the described above deniable encryption algorithm, if $R_\phi = R$.

4 Discussion and conclusion

Since the value R is computed as squaring the value $2^{-1} - T$ modulo n it looks like a random choice. Therefore the sender of the cryptogram $C = (A, B)$ can claim that the cryptogram is the result of the probabilistic public-key encryption of the message M while using the public key n and the random value R. When being coerced the sender provides to the attacker the message M and value R. The coercer encrypts the message M using receiver's public key and value R as random choice. The encryption procedure produces the cryptogram C that has been intercepted previously by the coercer. To argue that the value R is not a random choice, the coercive attacker has to compute at least one quadratic root (modulo n) from the value R. The last problem is computationally infeasible since finding quadratic roots modulo n is as difficult as factoring the value n [6]. Thus, the attacker has no possibility to detect that the value R is not random, and to disclose the lie of the sender is as difficult as factoring problem. The proposed sender-deniable encryption protocol is provably deniable.

One can consider the proposed protocol and the associated public-key encryption algorithm as some extensions of the Rabin public-key encryption system [6] in which the public key represents the pair of integers n and $b < n$. The private key is the pair of primes p and q such that $n = pq$. Using the public key (n, b) the message $M < n$ can be encrypted by some sender as computing the cryptogram $C = M(M+b) \mod n$. Using the private key (p, q) decryption of the cryptogram C is performed by the receiver (owner of the public key) as solving the quadratic congruence $x^2 + bx - C \equiv 0 \mod n$. From four solutions the receiver selects the sensible one as message M. In paper [6] it is

proved that the Rabin encryption algorithm is as secure as factoring the composite value n. In the Rabin public-key encryption system the cryptogram represents one of the coefficients of quadratic congruence (the second coefficient is equal to number b that is a part of the public key) whereas in the public encryption described in Section 2 the cryptogram represents two coefficients and the public key is the number n.

In paper [9] a class of provably secure public-key cryptosystems is described. In one of these systems the public-key encryption of the message M is performed as computing the cryptogam $C = M^3 \mod n$, where $n = pq$ and private primes p and q are such that number 3 divides $p-1$ and does not divide $q-1$. Decryption of the cryptogram C in that cryptoscheme consists in finding three cubic roots modulo n from C and selecting one of them as message M. Taking into account the results of paper [9] one can assume the possibility of designing a provably secure method for simultaneous encryption of three independent messages interpreting them as roots of cubic congruence modulo n. In this case the cryptogram will represent three coefficients of some cubic congruence selected from the following eight variants: $x^3 \pm Ax^2 \pm Bx \pm D \equiv 0 \mod n$. Existence of the algebraic formulas for computing roots of the cubic equations provides potential possibility of implementing the procedure for decryption of the cryptogram $C = (A, B, D)$.

The detailed consideration of constructing the deniable encryption scheme based on computing cubic roots represents an individual research topic, as well as extension to the case of simultaineous encryption of four messages interpreted as roots of the fourth-degree congruence.

The public-key encryption method described in Section 2 can be also implemented using any of the following four variants of the quadratic congruences: $x^2 \pm Ax \pm B \equiv 0 \mod n$.

The estimation of the hardware implementation of the proposed algorithms, like in the case of other cryptographic systems [10,11], is very useful for evaluating all aspects of their practical usability, however this problem represents a topic of individual research.

As a topic directly connected with the proposed deniable encryption method one can indicate development of the receiver-deniable and bi-

deniable encryption protocols based on the algorithm of simultaneous public-key encryption of two messages.

References

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

[2] J. Howlader, S. Basu. *Sender-Side Public Key Deniable Encryption Scheme.* Advances in Recent Technologies in Communication and Computing. Proceedings of the ARTCom '09 International Conference. 2009. pp. 9-13. (DOI: 10.1109/ARTCom.2009.107)

[3] Bo Meng, Jiang Qing Wang. *A Receiver Deniable Encryption Scheme.* Proceedings of the 2009 International Symposium on Information Processing (ISIP09). Huangshan, P. R. China, August 21-23, 2009. pp. 254–257.

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

[5] C. Wang, J. Wang. *A Shared-key and Receiver-deniable Encryption Scheme over Lattice.* Journal of Computational Information Systems, 2012, vol. 8, no. 2, pp. 747–753 ($http://www.Jofcis.com$).

[6] M. O. Rabin. *Digitalized signatures and public key functions as intractable as factorization.* Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[7] V. B. Alexeev. *Theorem of Abel in problems and solutions,* Moskva, MTSNMO, 2001 (in Russian).

[8] N. A. Moldovyan, P. A. Moldovyanu, *Vector form of the finite fieldsGF*(p^m), Bul. Acad. de Ştiinţe Repub. Mold. Mat., 2009, no.3, pp. 57–63.

[9] N. A. Moldovyan, A. A. Moldovyan. *Class of Provably Secure Information Authentication Systems.* Springer Verlag CCIS, 2007, vol. 1, pp.147–152, 4th Int. Workshop MMM-ANCS'07 Proc. September 13-15, 2007.

[10] N. Sklavos, P. Kitsos, O. Koufopavlou, *VLSI Design and Implementation of Homophonic Security System.* Proceedings of IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'12), Amherst, USA, August 19-21, 2012.

[11] N. Sklavos, C. Efstathiou, *Area-Optimized Architectures & Implementation of PELICAN MAC Function.* Proceedings of the 2nd IEEE International Conference On Information & Communication Technologies: From Theory To Applications (IEEE ICTTA'06), Damascus, Syria, April 24-28, 2006.

N. A. Moldovyan[1], A. A. Moldovyan[2],
V. A. Shcherbacov[3]

Received December 29, 2014

[1] Dr., St. Petersburg Institute for Informatics
and Automation of Russian Academy of Sciences
14 Liniya, 39, St. Petersburg 199178
Russia
Email: nmold@mail.ru

[2] Professor, ITMO University,
Kronverksky pr., 10, St.Petersburg, 197101
Russia
Email: maa1305@yandex.ru

[3] Dr., Institute of Mathematics and Computer Science
Academy of Sciences of Moldova Academiei str. 5, MD−2028 Chişinău
Moldova
Email: scerb@math.md