Research Article

Vitalii A. Roman'kov*

New probabilistic public-key encryption based on the RSA cryptosystem

Abstract: We propose a novel probabilistic public-key encryption, based on the RSA cryptosystem. We prove that in contrast to the (standard model) RSA cryptosystem each user can choose his own encryption exponent from a more extensive set of positive integers than it can be done by the creator of the concrete RSA cryptosystem who chooses and distributes encryption keys among all users. Moreover, we show that the proposed encryption remains secure even in the case when the adversary knows the factors of the modulus $n = pq$, where p and q are distinct primes. So, the security assumptions are stronger for the proposed encryption than for the RSA cryptosystem. More exactly, the adversary can break the proposed scheme if he can solve the general prime factorization problem for positive integers, in particular for the modulus $n = pq$ and the Euler function $\varphi(n) = (p-1)(q-1)$. In fact, the proposed encryption does not use any extra tools or functions compared to the RSA cryptosystem.

Keywords: Cryptography, public-key, RSA, semantic security

MSC 2010: 94A60, 11T71, 68P25

DOI: 10.1515/gcc-2015-0016
Received July 25, 2015

Introduction

The semantic security is one of the important requirements for a secure public-key cryptosystem. This notion, introduced by S. Goldwasser and S. Micaly in [2], gives the first formal definition of security for public-key encryption. The standard model of the RSA cryptosystem including the modulus $n = pq$, where p and q are different (secret) primes, and the encryption key e, as the public data, the (secret) decryption key d defined by the equation $ed = 1 \pmod{\varphi(n)}$, where $\varphi(n)$ is the Euler function, and the encryption and decryption functions $m \to c = m^e \pmod n$ and $c \to c^d = m \pmod n$, respectively, for a message $m \in \mathbb{Z}_n$, is not semantically secure.

Recall that a cryptosystem is called *semantically secure* if any probabilistic polynomial time algorithm that is given the ciphertext c of a certain message m taken from any distribution set of messages, and the message length, cannot determine any partial information on the message with probability non-negligibly higher than all other such algorithms that only have access to the message length and not the ciphertext (see [2]). Loosely speaking, the semantic security means that given any ciphertext c that is obtained by encryption of one of two possible messages m_1 and m_2, an adversary cannot determine which of the two has been encrypted.

Our contribution. In this paper, we propose a novel probabilistic public-key encryption based on the standard model of RSA cryptosystem. Also we discuss properties and preferences of the proposed encryption. We show that in contrast to the RSA cryptosystem the proposed encryption is not entirely based on hardness of the factoring problem for the set $\mathbb{Z}^{(2)} = \{n = pq : p \neq q \text{ are big primes}\}$. Even in the case where an adversary can recover the factors p and q of the modulus $n \in \mathbb{Z}^{(2)}$, he cannot recover a message m from the public data and the corresponding ciphertext. To do it, he has to solve an additional problem. He has to

***Corresponding author: Vitalii A. Roman'kov:** Mathematical Department, Omsk State University n.a. F.M. Dostoevskiy, Prospekt Mira 55-A, Omsk 644077, Russia, e-mail: romankov48@mail.ru

determine the order of a given element of the multiplicative group $\mathbb{Z}_n^*$. Note that if an adversary can determine the order $t = |m|$ of each element m of $\mathbb{Z}_n^*$ in the standard model of the RSA cryptosystem, he can effectively recover each message m from the ciphertext $c = m^e \pmod n$ with the help of the individual decryption key d_m computed from the equation $ed_m = 1 \pmod t$: $c^{d_m} = m \pmod n$. Also note that an adversary cannot determine the order of the given element g of a prime field $\mathbb{F}_p$ without knowing the prime factorization of $p - 1$. He can find the order of g if he knows the factorization of $p - 1$ (see [4]). If one can solve the general prime factorization problem for positive integers, in particular for n and $\varphi(n)$, then he can break the proposed scheme.

1 New probabilistic public-key encryption based on the RSA cryptosystem

The objective of this section is to propose a novel probabilistic public-key encryption. We will analyze its security in Section 3.

Let $n = pq \in \mathbb{Z}^{(2)}$, where p and q are different odd primes. We take the residue ring $\mathbb{Z}_n$ as the platform for the proposed encryption.

Alice chooses subgroups M and H of the multiplicative group $G_n = \mathbb{Z}_n^*$ of $\mathbb{Z}_n$ under the assumption that their orders r and t, respectively, are coprime: $\gcd(r, t) = 1$. She presents these subgroups by their generating elements as: $M = \mathrm{gp}(u_1, \dots, u_i)$ and $H = \mathrm{gp}(v_1, \dots, v_j)$, or in a different effective way.

We suppose that M is the message space, i.e., each message m is presented as an element of M, and vice versa. Now we fix public and secret data that are established off-line as follows.

Public data: n (and therefore $\mathbb{Z}_n$ and $G_n = \mathbb{Z}_n^*$), $u_1, \dots, u_i$ (and therefore M), $v_1, \dots, v_j$ (and therefore H).

Secret data: p, q, $\varphi(n) = (p - 1)(q - 1)$, r, t.

Alice chooses public key $e \in \mathbb{Z}$ such that $\gcd(e, r) = 1$. Then she computes the secret key $d = td_1$ from the equation $(te)d_1 = 1 \pmod r$. This is possible because $\gcd(t, r) = \gcd(e, r) = 1$ by our assumption. Then $ted_1 = 1 + rk$ for some integer k. Thus, Alice has the following keys:

Public key: e.

Secret key: d.

To send a message $m \in M$ to Alice, the other correspondent Bob chooses a random element $h \in H$ (secret session key) and acts as follows:

Encryption: $m \to c = (hm)^e \pmod n$.

Alice recovers m as follows:

Decryption: $c \to m = c^d \pmod n$.

Correctness: $c^d = (h^t)^{ed_1} m (m^r)^k = m \pmod n$.

Choice of M and H: Alice chooses a cyclic subgroup L of G_n of a prescribed order l when she generates p and q.

Suppose she constructs p with primality testing using the factorization of $p - 1$. She seeks for p written in the form $p = 2lx + 1$ taking x randomly. Then she checks the primality of p with some of the known primality tests.

Recall the following primality test from [4].

Let $p \geq 3$ be an integer. Then p is prime if and only if there exists an integer a satisfying:

(i) $a^{p-1} = 1 \pmod p$ and

(ii) $a^{p-1/s} \neq 1 \pmod p$ for each prime divisor s of $p - 1$.

This result follows from the fact that G_n has an element a of order $p - 1$ if and only if p is a prime. If p is a prime, the number of elements a satisfying conditions (i) and (ii) has order $p - 1$.

When Alice gets a prime $p = 2lx + 1$, she finds an element g of order l. She takes randomly elements $f \in \mathbb{F}_p^*$ and checks whether or not $f^{2x} = 1$. With probability at least $1 - 1/l$ she finds f of order l.

By the Chinese Remainder Theorem, Alice gets a solution y of the set of equations

$$y = f \pmod{p}, \quad y = 1 \pmod{q}.$$

Thus she succeeds in determining L by setting $L = \mathrm{gp}(y)$. This way Alice can present the (cyclic) subgroups $M = \mathrm{gp}(u)$ and $H = \mathrm{gp}(v)$ of the prescribed coprime orders r and t. The generators u and v can be chosen simultaneously with the construction of p and q. The corresponding orders t and r can both divide $p-1$ or $q-1$, or we can take one of them as divisor of $p-1$, and the other as divisor of $q-1$. For security reasons these numbers t and r should be sufficiently big.

Alice can take H as a subgroup generated by a tuple of cyclic groups $\mathrm{gp}(u_1), \ldots, \mathrm{gp}(u_k)$ of orders $t_1, \ldots, t_k$, respectively, that are coprime to a given set of primes $r_1, \ldots, r_l$, and then construct the subgroup M as the product of cyclic groups $\mathrm{gp}(v_1), \ldots, \mathrm{gp}(v_l)$ of orders $r_1, \ldots, r_l$, respectively. These primes $t_1, \ldots, t_k, r_1, \ldots, r_l$ have to be divisors of $p-1$ or $q-1$. Thus, the primes p and q are to be obtained with regard to these conditions.

Choice of e: The only assumption on e is its relative primality with r. When r is a big prime, Bob can choose randomly e by himself. The probability that e is divided by r is negligible in many senses. Anyway it can be done practically.

Another option is to choose e not so big as r. Alice announces that $r \geq z$ where z is public. Then Bob can take any e such that $2 \leq e \leq a-1$. Obviously, in this case $\gcd(e, a) = 1$.

2 Some decision problems for $G_n = \mathbb{Z}_n^*$

Let n be a product of two different primes p and q, i.e., $n \in \mathbb{Z}^{(2)}$. Let Q_n be the subgroup of $G_n = \mathbb{Z}_n^*$ consisting of all quadratic residues. The following problem is one of the most known decision problems in number theory and cryptography.

The Quadratic Residuosity Problem (QRP) with parameter n. Given an element $f \in G_n$, determine if $f \in Q_n$.

This problem is considered by many authors as intractable. A number of cryptographic schemes are based on this intractability, and the famous Goldwasser–Micaly cryptosystem is one of them. It is important to note that the semantic security property of the Goldwasser–Micaly cryptosystem is based on the intractability of the QRP.

The QRP is a particular case of the following decision problem.

The Membership Problem (MP_L) with parameters n and L. Let L be a subgroup of G_n. Given an element $f \in G_n$, determine if $f \in L$.

We can change L and get the following decision problem.

The Membership Problem (MP) with parameter n. Given a subgroup L of G_n and an element $f \in G_n$, determine if $f \in L$.

The following problem is not so famous but is very important for the proposed RSA-type cryptographic scheme.

The Order (of element) Problem (OP). Given an element $f \in G_n$, determine the order $|f|$ of f.

In general, finding the order of an element of a group G_n is at least as hard as factoring (see [3]). However, the problem becomes significantly easier, provided that the primality factorization of $|G_n| = \varphi(n)$ is known. Under these circumstances, efficient algorithms are known [1]. Note that in the case of a prime finite field $\mathbb{F}_p$ one can effectively find the order $|f|$ of a given element $f \in \mathbb{F}^*$ if the primality factorization of $|\mathbb{F}^*| = p-1$ is known (see [4]). Otherwise, this problem is open.

3 Cryptanalysis of the proposed encryption

As we explained above, Alice can recover each message $m \in M$ because she knows the decryption key d. This key can be found if one knows all open data and the secret parameters $\varphi(n)$, t and r. The adversary can break the proposed scheme if he can solve the general prime factorization problem for positive integers, in particular for the modulus n and the Euler function $\varphi(n)$.

We consider the proposed encryption as a good candidate to be semantically secure if the membership problem MP_H is intractable. Indeed, suppose we have an encrypted message $c = (hm)^e \pmod n$, and we want to check if $m = m'$ for some possible message $m' \in M$. This happens if and only if $c(m')^{-1} \in H$.

When we take $H = Q_n$, this problem reduces to QRP. Hence, if one can solve the membership problem MP, he can solve QRP, too.

Solvability of the OP for G_n implies solvability of the RSA problem in the standard RSA cryptosystem because if one knows the order t of any ciphertext $c = m^e$, which is equal to the order $|m|$ of m as $\gcd(e, \varphi(n)) = 1$, he can recover m using the individual decryption key d_m, computed from the equation $ed_m = 1 \pmod t$.

Suppose the adversary knows the factors p and q of the modulus n, and so he knows $\varphi(n)$. Then he can get the key d_1 and compute $hm \pmod n$. If it happens that e is coprime with $\varphi(n)$, then he finds a solution for $ed_1 = 1 \pmod{\varphi(n)}$; it exists and $ed_1 = 1 \pmod{\varphi(n)}$. If e is not coprime with $\varphi(n)$ and $\gcd(\varphi, e) = l$, then prime factors of l do not divide r. In that case, the adversary simply removes l from $\varphi(n)$ lowering the modulus. Finally, he solves $ed_1 = 1 \pmod{\varphi(n)/l}$.

Now the adversary gets $hm \pmod n$. To recover m he needs to know the secret parameter t. He can find it effectively if he knows the prime factorization of $p - 1$ and $q - 1$.

4 Advantages of the proposed encryption

The proposed encryption is based not only on hardness of the factoring problem for numbers from $\mathbb{Z}^{(2)}$, but also on hardness of the OP in the multiplicative group $G_n = \mathbb{Z}_n^*$. Recall, that the RSA problem is solvable if the OP is solvable.

The encryption exponent e can be chosen from a wider key space than in RSA cryptosystem. It can be done by each user, not only by a creator of a concrete cryptosystem.

The proposed encryption is possible semantic secure. In the particular case when $H = Q_n$ it is semantically secure under the assumptions of the semantic security of the Goldwasser–Micaly cryptosystem [2].

We believe that the proposed encryption gives new possibility to establish digital signature and authentication schemes. Also the possible semantic security of the proposed encryption is a subject of future study.

Funding: This research was supported by RFBR grant 15.41.04312.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, New York, 1993.
[2] S. Goldwasser and S. Micaly, Probabilistic encryption & how to play mental poker keeping secret all partial information, in: *Annual ACM Symposium on Theory of Computing* (STOC '82), ACM, New York (1982), 365–377.
[3] A. R. Meijer, Groups, factoring and cryptography, *Math. Mag.* **69** (1996), 103–109.
[4] A. Menezes, P. G. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.