Malaysian Journal of Computing and Applied Mathematics 2020, Vol 3(1): 47-51

(Online)

MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS

A Different Encryption System Based on the Integer Factorization Problem

***Karima Djebaili*[a]*, Lamine Melkemi*[b]**

[a]Department of Computer Science and Information Technologies, University of Ouargla, Ouargla, Algeria
[b]Department of Mathematics, University of Batna, Batna, Algeria

**Corresponding author: djebaili.karima@univ-ouargla.dz*

Received: 12/12/2019, Accepted: 29/04/2020
http://dx.doi.org/10.37231/myjcam.2020.3.1.43

Abstract

We present a new computational problem in this paper, namely the order of a group element problem which is based on the factorization problem, and we analyze its applications in cryptography. We present a new one-way function and from this function we propose a homomorphic probabilistic scheme for encryption. Our scheme, provably secure under the new computational problem in the standard model.

Keywords: Public key encryption, factorization problem, order of a group element problem.

INTRODUCTION

The idea of public-key encryption was introduced by Diffie and Hellman (1976) Several cryptographic schemes take place in the multiplicative group $\mathbb{Z}_n^*$, under the assumption that it is difficult to invert the one-way function of an encryption process without the knowledge of the factorization of the composite number $n = pq$ where p and q are two large prime numbers. Real examples of such schemes [Rivest et al. (1978), Rabin (1979), Cohen and Fischer (1985), Kurosawa et al. (1991), Paillier (1999)] and digital signatures [Cramer and Shoup (2000),Camenisch and Lysyanskaya (2003). In this paper we propose two schemes; public key encryption scheme and a signature scheme and we will demonstrate their security under the order of a group element problem which is based on the factorization problem.

NOTATIONS

Consider an RSA-modulus $n = pq$, where p and q are large primes. Assume that $x \in \mathbb{Z}_n^*$, the order of x is defined to be the least positive integer z such that $x^z = 1 \bmod n$, (see Menezes et al. (1996)). In our case such an integer z ($x^z = 1 \bmod n$) always exists. We denote by $|x|$ the order of x. Moreover, the subgroup generated by x denoted by $< x >$. It is well known that the order $|x|$ of x divides the Euler totient function $\varphi(n) = (p - 1)(q - 1)$.

A. Key Generation and Cryptographic Scheme

Depending on the security parameter, a one-way function defines the public and secret keys of a public key encryption (PKE) scheme for each user: a G key generation algorithm takes as argument the security parameter k, then randomly sets public key pk and secret key sk: $(pk,sk) \leftarrow G(1^k)$. We denote m and c for the message and ciphertext respectively.

B. The Order of a Group Element Problem

Let x be an element in $\mathbb{Z}_n^*$. Given $x^z = 1 \bmod n$, the Assumption 1 define the order of a group element problem as the computational problem of computing z. We assume this problem is difficult without the knowledge of factorization of the modulus n.

Assumption 1 *(*The order of a group element problem*). For every probabilistic polynomial time (PPT) adversary* A*, there exists a negligible function negl*(.) *and a security parameter* k_0 *such that the following holds for all* $k > k_0$*:*

$$Pr[z \leftarrow \mathcal{A}(x, \mathbb{Z}_n^*) | x^z = 1 \; mod\, n] = negl(k). \tag{1}$$

C. Semantic security

Semantic security (see Goldwasser and Micali (1984)) also known as indistinguishability of ciphertexts or polynomial security, it is like *perfect security* but we only allow an adversary with polynomially bounded computing power.

Definition 1 *(*Semantic security*). A PKE scheme is said to be semantically secure (or IND-CPA secure) if for any adversary* A *uses a pair of PPT algorithms* (A_1,A_2) *the following advantage Adv holds for* $n,k \in \mathbb{N}$ *and some state information:*

$$Adv_A^{IND-CPA} = Pr[b \leftarrow A_2(c,state) | (pk,sk) \leftarrow G(1^k), (m_0,m_1,state) \leftarrow A_1,$$

$$c \leftarrow Encrypt(m_b,pk)] < \frac{1}{2} + \frac{1}{n^k} \tag{2}$$

ENCRYPTING PROTOCOL

This section describes the encryption scheme proposed in this paper which consists of three algorithms:

1. **Key generation**: Select an RSA-modulus $n = pq$ where p and q are co-prime and select $\alpha, \beta \in \mathbb{Z}_n^*$ where $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$, that is $\delta\alpha + \gamma\beta = 1$ for two integers δ and γ. Now select a and b such that $|a| = \alpha$ and $|b| = \beta$. The public key $pk = (n,a,b)$ and the secret key $sk = (p,q,\delta,\gamma)$. Each public key is associated with a message space $MsgSp(pk)$ and a ciphertext space $CipSp(pk)$.
2. **Encryption**: We wish to encrypt a message $m \in MsgSp(pk)$. The ciphertext is $c_1 = a^x m \bmod n$ and $c_2 = b^y m \bmod n$, for two random values x and $y \in Z_n$.
3. **Decryption**: Given a ciphertext $(c_1,c_2) \in CipSp(pk)$ we output $m = c_1^{\delta\alpha} c_2^{\gamma\beta} \bmod n$.

Proof of Decryption Validity
At the time of decryption, the receiver computes:

$$\begin{aligned}
c_1^{\delta\alpha} c_2^{\gamma\beta} \bmod n &= (a^x)^{\delta\alpha} m^{\delta\alpha} (b^y)^{\gamma\beta} m^{\gamma\beta} \bmod n \\
&= (a^\alpha)^{\delta x} m^{\delta\alpha} (b^\beta)^{\gamma y} m^{\gamma\beta} \bmod n \\
&= m^{\delta\alpha} m^{\gamma\beta} \bmod n \\
&= m^{\delta\alpha+\gamma\beta} \bmod n \\
&= m \bmod n \\
&= m.
\end{aligned} \tag{3}$$

A. Security Analysis
This section discusses the security results of the cryptosystem proposed in this paper.

i) One-Wayness

Theorem 1 *The proposed encryption function provides one-wayness if there is no adversary who can recover p and q.*

Proof. It is easy to see that if the problem of factorization is not intractable in $\mathbb{Z}_n^*$, it is easy to recover the secret key (i.e, α and β), from which the determination of *m* is obvious.

ii) IND-CPA Security

Definition 2 *(*Decisional generator problem*). Select an RSA-modulus n = pq.*
Define the formulation:
$a, b, f, g \in \mathbb{Z}_n^*$ *determine if f ∈< a > and g ∈< b > .*
We call this the decisional generator problem (DGP) which is based on the integer factorization problem.

<u>The Proposed Cryptosystem is at Least as Hard as The DGP</u>

Theorem 2 *If the proposed cryptosystem is not secure in the sense of INDCPA attacks, then there is an adversary that solves the DGP with non-negligible advantage.*

Proof. Assume that A is an adversary that can break the proposed cryptosystem in the sense of IND-CPA with a non-negligible advantage ϙ, we will use this to create a new adversary B which breaks the DGP. The following discussion describes the construction of B:

Algorithm B:
The algorithm is given $\mathbb{Z}_n^*$, *a,b,f,g* as input.
- Set *pk* = (*n,a,b*) and run A(*pk*) to obtain two messages m_0,m_1.
- Choose a random bit $b \in \{0,1\}$, and set:
  (a) $c_1 = fm_b \bmod n$.
  (b) $c_2 = gm_b \bmod n$.
- Give the ciphertext (c_1,c_2) to A and obtain an output bit b'.
  If $b' = b$ output 1; otherwise output 0.

We analyze the behavior of B. There are two cases.
Case 1. If $f \in \langle a \rangle$ and $g \in \langle b \rangle$ then (c_1,c_2) is a valid encryption, so A will guess correctly *b* with non-negligible probability, therefore:

$$Pr[\text{B output=1}] = \frac{1}{2} + \epsilon.$$

Case 2. If *f* and *g* are random numbers then in this case, *b* is independent of the adversary's view, therefore:

$$Pr[\text{B output=0}] = \frac{1}{2}.$$

<u>The DGP is at Least as Hard as the Proposed Cryptosystem</u>

Theorem 3 *If there exists an oracle O which solves the DGP with nonnegligible probability, then the proposed cryptosystem is not secure in the sense of IND-CPA.*

Proof. We assume that we have an oracle *O* which solves the DGP such that solving this problem permits the adversary A to distinguish the ciphertext for messages m_0 and m_1. If *f* (or *g*) (*f*f and *g* are the input of this oracle), ∈< *a* > (or ∈< *b* >), *O* outputs 1; otherwise it output 0. A should run in two stages:
- Find stage: At this stage A asked the encryption oracle on two messages m_0, m_1, such that $gcd(m_0,\varphi) = 1$, the outputs of this oracle is:
  $$[fm_i,gm_i],[fm_{1-i},gm_{1-i}] \text{ where } i \in \{0,1\}.$$
- Guess stage: At this stage A asked the oracle *O* on:
  $$[fm_i m_0^{-1}, gm_i m_0^{-1}]$$

If the output of the oracle O is 1 (i.e., $f \in < a >$ or $g \in < b >$) with probability non-negligibly, then $m_i = m_0$. Otherwise $m_i = m_1$.
Because the hardness assumption of the integer factorization problem it is difficult to find α and β, so the probability of determine whether or not $f \in < a >$ and $g \in < b >$ is negligible, which means that the proposed cryptosystem is IND-CPA secure and this concludes the proof.

SIGNING PROTOCOL

Let m be a message which the sender wishes to sign. He performs the following singing protocol which consists of three algorithms.

- Key generation: Select an RSA-modulus $n = pq$ where p and q are co-prime and select $\alpha, \beta \in \mathbb{Z}_n^*$ where $\alpha = \frac{p-1}{2}$ and $\beta = \frac{q-1}{2}$, that is $\delta\alpha + \gamma\beta = 1$ for two integers δ and γ. Now select a and b such that $|a| = \alpha$ and $|b| = \beta$. Public verification key $vk = (n,a,b)$. Private signature key $sk = (p,q,\delta,\gamma)$. Each public verification key is associated with a message space $MsgSp(vk)$ and a signing-message space $SigSp(vk)$.

- Signature: To sign a message $m \in MsgSp(vk)$, Choose at random $\phi \in < a >$ and $\psi \in < b >$. Compute $c_1 = (\phi h(m))^{\beta} \bmod n$, $c_2 = (\psi h(m))^{\alpha} \bmod n$ and $\omega = (\phi\psi)^{-1} \bmod n$, where $h(.)$ is a cryptographic hash function. The signature on m is $(c_1, c_2, \omega) \in SigSp(vk)$.

- Verification: Given a signature (c_1, c_2, ω) on $m \in MsgSp(vk)$. Accept if:

$$h(m) = c_1^{\gamma} c_2^{\delta} \omega \bmod n.$$

A. Proof of Verification Validity

At the time of verification the receiver computes:

$$\begin{aligned} c_1^{\gamma} c_2^{\delta} \bmod n &= \varphi^{\gamma\beta} h(m)^{\gamma\beta} \psi^{\delta\alpha} h(m)^{\delta\alpha} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} h(m)^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} h(m) \bmod n. \end{aligned} \quad (4)$$

and because:

$$\begin{aligned} \varphi\psi \bmod n &= (\varphi\psi)^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\delta\alpha+\gamma\beta} \psi^{\delta\alpha+\gamma\beta} \bmod n \\ &= \varphi^{\gamma\beta} \psi^{\delta\alpha} \bmod n. \end{aligned} \quad (5)$$

From 4 and 5, he finds $h(m) = c_1^{\gamma} c_2^{\delta} \omega$ mod n, so the verification condition holds.

B. Security Analysis

An adversary might attempt to forge user's signature on m by selecting a random integers $\phi \in < a >$ and $\psi \in < b >$. The adversary must then determine $c_1 = (\phi h(m))^{\beta} \bmod n$ and $c_2 = (\psi h(m))^{\alpha} \bmod n$. If the order of a group element problem is computationally infeasible in $\mathbb{Z}_n^*$, the adversary can do no better than to choose a c_1 and c_2 at random, this forgery only occurs with negligible probability.

CONCLUSIONS AND FURTHER RESEARCH

We constructed two systems that are provably secure under the order of a group element problem which is based on the factorization problem. The first construction is a public key cryptosystem and the second construction is a signature scheme. As future work we look to improve our main schemes to ensure security in the sense of NM-CCA2 (see Djebaili and Melkemi (2018)). However, these schemes are quite practical and more efficient compared with other schemes.

References

Camenisch J. and Lysyanskaya A. (2003). A signature scheme with efficient protocols. In *Security in communication networks*, pp. 268–289. Springer.

Cohen J D and Fischer M J. (1985). *A robust and verifiable cryptographically secure election scheme*. Yale University. Department of Computer Science.

Cramer, R. and V. Shoup (2000). Signature schemes based on the strong RSA assumption. *ACM Transactions on Information and System Security, 3*(3), 161–185.

Diffie W and Hellman M E. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on 22*(6), 644–654.

Djebaili K and Melkemi L. (2018). Security and robustness of a modified El-gamal encryption scheme. *International Journal of Information and Communication Technology 13*(3), 375–387.

Goldwasser S and Micali S. (1984). Probabilistic encryption. *Journal of computer and system sciences 28*(2), 270–299.

Kurosawa K, Katayama Y, Ogata W and Tsujii S. (1991). General public key residue cryptosystems and mental poker protocols. In *Advances in CryptologyEUROCRYPT'90*, pp. 374–388. Springer.

Menezes A J, Van Oorschot P C, and Vanstone S A. (1996). *Handbook of applied cryptography*. CRC press.

Paillier P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology-EUROCRYPT'99*, pp. 223–238. Springer.

Rabin M O. (1979). Digitalized signatures and public-key functions as intractable as factorization.

Rivest R L, Shamir A, and Adleman A. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 21*(2), 120–126.