Palestine Journal of Mathematics

Vol. 6(2)(2017) , 580–584

A NEW PUBLIC KEY SCHEME BASED ON INTEGER FACTORIZATION AND DISCRETE LOGARITHM

Pinkimani Goswami, Madan Mohan Singh and Bubu Bhuyan

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94A60.

Keywords and phrases: Public key cryptography, integer factorization, discrete logarithm.

Abstract. In this paper, we present a new public key scheme which is a combination of RSA variant namely the Dependent-RSA (DRSA) and the general formulation of DGDLP. The security of this scheme depend equally on the integer factorization of n and the discrete logarithm on $\mathbb{Z}_n^*$, where n is a product of two large primes and $\mathbb{Z}_n^*$ is the multiplicative group modulo n. The scheme is a randomized algorithm and it is at least as secure as the DRSA and ElGamal schemes.

1 Introduction

The public key cryptography has a major advantage over the symmetric key cryptography. It has an own public key which is known to everybody and has a corresponding private key which is only known to the intended recipient. Therefore, it does not require a prior communication of a secret key which is the main disadvantage of symmetric key cryptography. Most of the public key cryptosystems are based on one-way trapdoor function, where the encryption rule is easy to compute, but decryption rule is computationally infeasible without any additional information. Thus, the security of a public key cryptosystem is based on the intractability of hard mathematical problems such as integer factorization problem (IFP), discrete logarithm problem (DLP) etc. The two problems which are used in this paper are the Computational Dependent-RSA problem (C-DRSA problem) [7] and the generalization of generalized discrete logarithm problem (generalization of GDLP or generalized GDLP) [6]. For a large composite RSA modulus n and an exponent e relatively prime to $\phi(n)$, the Computational Dependent-RSA problem [7] stated that for given $k^e \ (mod\ n)$ find $(k+1)^e \ (mod\ n)$ where $k \in \mathbb{Z}_n^*$. The C-DRSA problem is intractable for large RSA modulus n [7]. The Generalization of GDLP [6] stated that given a finite group G and elements $\alpha, \gamma \in G$, find an integer x such that $\alpha^x = \gamma$, provided that such an integer exists. In this formulation, it is not required that G be a cyclic group, and even it is, it is not required to consider generator of the group [6]. Since α is not a generator of the group so α^x is not unique, which makes this problem harder to solve than GDLP. In this paper, we consider two generalized GDLP (we call it the generalization of DGDLP or general formulation of DGDLP) on $\mathbb{Z}_n^*$, the non-cyclic group of multiplication modulo n, where n is the product of large primes.

Up to now, most of the public key schemes are based on one cryptographic assumption. Although these schemes are secure but it is possible that in future efficient algorithms will be developed to solve these assumptions false. In 1988, K. S. McCurley [5] proposed the first key distribution scheme based on two hard dissimilar assumptions. The scheme is a modification of the ElGamal cryptosystem. Instead of using an arithmetic modulus a prime p, he used a modulus n that is a product of two primes. To break the scheme requires the prime factorization of n and ability to solve DLP. After that, many public key schemes were developed which are based on two cryptographic assumptions (for example [4, 2, 3, 10, 8] etc)

By this motivation, we propose a new public key scheme whose security is based on the Computational Dependent-RSA problem and the generalization of GDLP. In this proposed scheme, an attacker has to solve simultaneously the integer factorization problem (IFP) and the generalization of DGDLP. One advantage of this scheme is that it include non-cyclic groups. Moreover, the encryption scheme is more efficient than the Quadratic exponentiation randomized (QER) cryptosystem [2]. We also show that the proposed scheme is at least as secure as each of the DRSA scheme [8] and the ElGamal scheme [9].

The paper is organized as follows. In section 2, we present our cryptosystem. Section 3 is devoted to the security of the proposed cryptosystem and in section 4 we deal with its performance. Finally, we conclude the paper in section 5. Throughout the paper, all notations are usual. For example, the multiplicative group of $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^*$, the Euler's phi function of n is denoted by $\phi(n)$ etc.

2 The Proposed Public Key Scheme

In this section we present our public key scheme.

Public and private key generation:

A user $\mathcal{A}$, who wants to create a public and private key, have to do the following steps:

1. Choose two large primes p and q of almost same size.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
3. Choose two integers $e, d \in \{1, \ldots, n-1\}$ such that $ed \equiv 1 \ (mod\ \phi(n))$.
4. Select two random integers a, b such that $0 \leq a, b \leq \phi(n) - 1$.
5. Choose $\alpha, \beta \in \mathbb{Z}_n^*$ and compute $\alpha^a \ (mod\ n)$ and $\beta^b \ (mod\ n)$.

The public key of $\mathcal{A}$ is $(n, e, \alpha, \beta, \alpha^a, \beta^b)$ and the corresponding private key is (p, q, d, a, b).

Encryption:

Suppose that another user $\mathcal{B}$ want to send a message to $\mathcal{A}$ by using $\mathcal{A}$'s public key. Then $\mathcal{B}$ have to do the following steps:

1. Represent the message m as an integer in the interval $[0, n-1]$.
2. Choose $k \in \mathbb{Z}_n^*$ and compute $C_1 \equiv k^e \ (mod\ n)$.
3. Choose two random non-negative integers g and h and compute $C_2 \equiv \alpha^g \ (mod\ n)$ and $C_3 \equiv \beta^h \ (mod\ n)$.
4. Compute $C_4 \equiv (\alpha^a)^g (\beta^b)^h (k+1)^e m \ (mod\ n)$.

$\mathcal{B}$ send to $\mathcal{A}$ the encrypted message (C_1, C_2, C_3, C_4).

Decryption:

For the decryption of the message (C_1, C_2, C_3, C_4), $\mathcal{A}$ should do the following steps:

1. Compute $k \equiv C_1^d \ (mod\ n)$.
2. Compute $M \equiv C_4 (k+1)^{-e} \ (mod\ n)$.
3. Compute $C_2^{\phi(n)-a} \ (mod\ n) \equiv \alpha^{-ag} \ (mod\ n)$ and $C_3^{\phi(n)-b} \ (mod\ n) \equiv \beta^{-bh} \ (mod\ n)$.
4. Compute $N \equiv \alpha^{-ag} \beta^{-bh} M \ (mod\ n)$.

Proof of validity:

From the relation $N \equiv \alpha^{-ag} \beta^{-bh} M \ (mod\ n)$, we have
$N \equiv \alpha^{-ag} \beta^{-bh} C_4 (k+1)^{-e} \equiv \alpha^{-ag} \beta^{-bh} \alpha^{ag} \beta^{bh} m \equiv m \ (mod\ n)$.
Since $0 \leq m, N \leq n-1$, so $N = m$.

3 Security

The security of this proposed cryptosystem is based on factoring and discrete logarithm. A third party who intercepts the encrypt message (C_1, C_2, C_3, C_4) can recover m, by finding the prime factors p and q of n and so d and next by finding a and b from $\alpha^a \ (mod\ n)$ and $\beta^b \ (mod\ n)$ that is an attacker has to solve integer factorization problem and general formulation of DGDLP. So, the primes p and q are consider in such a way that they do not permit the application of the known algorithms of factorization and for computation of discrete logarithm. Furthermore, d must be greater than $n^{0.292}$ to avoid low private exponent attack [1]. Also, the order of α and β are large to prevent exhaustive search attack. To encrypt diffrent messages the parameters k, g and h must be different. Because if a sender used same parameters for encryption of two messages say m_1 and m_2 then he obtains $C_4 \equiv (\alpha^a)^g(\beta^b)^h(k+1)^e m_1 \ (mod\ n)$ and $C_4' \equiv (\alpha^a)^g(\beta^b)^h(k+1)^e m_2 \ (mod\ n)$. So, from the relation $m_2 \equiv C_4^{-1}C_4' m_1 \ (mod\ n)$, an attacker who knows the message m_1 can recover m_2.

Since the parameters k, g and h are randomly chosen by the sender, so the proposed scheme is a randomized algorithm, which increases the security of the scheme. Also, an attacker is not able to find the ciphertext of $m_1 m_2$ even if he knows the corresponding ciphertext of messages m_1 and m_2.

Note that if an attacker finds easily a method to compute d or factoring n, then he has still to solve general formulation of DGDLP. Alternatively, if the attacker can easily solve the general formulation of DGDLP, then he also has to compute d by factoring n. Thus, in any case, an attacker has to solve two hard problems. Since the security of this scheme is based on IFP and general formulation of DGDLP, so it is more secure than the scheme proposed in [8] which is based on IFP and two DLP as generalized GDLP is harder to solve than DLP. The scheme is more secure than the quadratic exponentiation randomized (QER) cryptosystem [2] as it requires IFP and one general formulation of GDLP.

Now, by the following theorem, we will show that the proposed scheme is at least as secure as each of the DRSA and ElGamal schemes. For this, we assume that there exists an oracle $\mathcal{O}$ that can break the proposed scheme that is $\mathcal{O}$ can gives the message from the corresponding ciphertext.

Theorem 3.1. *If there is an oracle that can break the proposed scheme then it can also break the DRSA and ElGamal schemes.*

Proof. If $a = 0 = b$, then $\alpha^a = 1 = \beta^b$ and so the DRSA cryptosystem is a particular case of the proposed scheme. Hence, if there exist an oracle that can break the proposed scheme then it can also break the DRSA scheme.

Let $\mathcal{O}$ be an oracle that can break the proposed scheme. We will show that $\mathcal{O}$ can also break ElGamal Scheme. Let (p, g, y) be the public key and a be the private key of the ElGamal scheme, where $y \equiv g^a \ (mod\ p)$.

Suppose that an attacker has captured a ciphertext (C, D), which is encrypted by the ElGamal scheme and he wants to recover the corresponding message m. So, there is a $z \in \{0, \ldots, p-2\}$ such that $C \equiv g^z \ (mod\ p)$ and $D \equiv y^z m \ (mod\ p)$. First, he chooses a prime q such that $q \nmid D$ and compute $n = pq$. Secondly, he chooses integers $\alpha, y_1, C_1, D_1 \in \{1, ..., n-1\}$ such that

$$\begin{array}{ll} \alpha \equiv g \ (mod\ p), & \alpha \equiv 1 \ (mod\ q), \\ y_1 \equiv y \ (mod\ p), & y_1 \equiv 1 \ (mod\ q), \\ C_1 \equiv C \ (mod\ p), & C_1 \equiv 1 \ (mod\ q), \\ D_1 \equiv D \ (mod\ p), & D_1 \equiv 1 \ (mod\ q). \end{array}$$

Since $\alpha^a \equiv y \ (mod\ p)$ and $\alpha^a \equiv 1 \ (mod\ q)$, so $\alpha^a \equiv y_1 \ (mod\ n)$. Similarly, $\alpha^z \equiv C_1 \ (mod\ n)$. Consider $M \in \{1, \ldots, n-1\}$ such that $M \equiv m \ (mod\ p)$ and $M \equiv 1 \ (mod\ q)$. Then $D_1 \equiv y_1^z M \ (mod\ n)$.

Again, choose $\beta \in \mathbb{Z}_n^*$, $b \in \{0, \ldots, \phi(n) - 1\}$ and compute $y_2 \equiv \beta^b \ (mod\ n)$. So, $(n, e = 1, \alpha, \beta, y_1 = \alpha^a, y_2 = \beta^b)$ mod n is the public key and $(p, q, d = 1, a, b)$ is the private key of the proposed scheme. Since the oracle $\mathcal{O}$ can break the proposed scheme, so from the ciphertext $(1, C_1 = \alpha^z, C_2 = \beta^0, C_3 = 2y_1^z y_2^0 M = 2D_1)$ mod n, one can recover M and hence m.

□

4 Performance analysis

The encryption algorithm of the proposed scheme requires six modular exponentiations namely $k^e, \alpha^g, \beta^h, (\alpha^a)^g, (\beta^b)^h, (k+1)^e \bmod n$ and three modular multiplications for computation of C_1, C_2, C_3 and C_4. The six modular exponentiations and two modular multiplications can be done in advance. Thus, the encryption requires only one modular multiplication. The decryption algorithm required four modular exponentiations namely C_1^d, $(k+1)^e$, $C_2^a, C_3^b \bmod n$, three modular multiplications to compute $M, N \bmod n$ and three applications of extended Euclidean algorithm for computation of $((k+1)^e)^{-1}, (C_2^a)^{-1}, (C_3^b)^{-1} \bmod n$. Hence, the encryption of this scheme is as efficient as the encryption scheme proposed in [8] whereas the decryption is less efficient since the decryption scheme of the previous scheme requires three modular exponentiations, two modular multiplications and two applications of extended Euclidean algorithm. The encryption scheme of the QER cryptosystem [2] requires one modular exponentiation and one modular multiplication whereas decryption requires two modular exponentiations, one modular multiplication and one application of the extended Euclidean algorithm. Thus, the proposed encryption scheme is more efficient than the QER encryption scheme and decryption scheme is less efficient. Similarly, encryption scheme is more efficient than the encryption scheme described in section III of [3], [4] and section 3 of [5]. The scheme is more efficient than the trivial use of the DRSA and QER schemes in series. It is also more efficient than the trivial use of the DRSA and ElGamal schemes in series. A disadvantage of the proposed scheme is that the ciphertext is longer than the plaintext.

5 Conclusion

In this paper, we introduced a new public key scheme which is a combination of DRSA and general formulation DGDLP. The use of the general formulation of DGDLP increases the security of the proposed scheme. We also showed that the scheme is at least as secure as the DRSA and ElGamal cryptosystems, which are semantically secure. The encryption scheme is at least as efficient as the most of the existing scheme.

References

[1] D. Boneh and G. Durfee, New results on cryptanalysis of low private exponent RSA, Preprint (1998).

[2] H. Elkamchouchi, K. Elshenawy and Heba. A. Shaban, Two new public key techniques in the domain of Gaussian integers, *Proceedings of the Twentieth national radio science conference, NRSC 2003* **C17**, 1–8 (2003).

[3] H. M. Elkamchouchi, M. E. Nasr and R. Esmail, New public key techniques based on double discrete logarithm problem, *Proceedings of the Twenty-First National radio science conference, NRSC 2004* **C23**, 1–9 (2004).

[4] L. Harn, Public-key cryptosystem design based on factoring and discrete logarithms, *IEE Proceedings - Computers and Digital Techniques* **141:3**, 193–195 (1994).

[5] K. S. McCurley, A key distribution system equivalent to factoring, *J. Cryptology* **1 : 2**, 95–106 (1988).

[6] A. J. Menezes , P. van Oorschot and S. Vanstone, *Handbook of Apllied Cryptography*, CRC Press, (1997).

[7] D. Pointcheval, New public key cryptosystems based on the dependent-RSA problems, *Proceedings of Advances in cryptology - EUROCRYPT'99, J. Stern (editor), Springer, Berlin, Lect. Notes Comput. Sci.* **1592**, 239–254 (1999).

[8] D. Poulakis, A public key encryption scheme based on factoring and discrete logarithm, *Journal of Discrete Mathematical Sciences and Cryptography* **12 : 6**, 745–752 (2009).

[9] Y. Tsiounis and M. Yung, On the security of ElGamal based encryption, *Proceedings of 1st International Workshop on Practice and Theory in Public Key Cryptography (PKC'98), H. Imai et al. (editor), Springer, Berlin, Lect. Notes Comput. Sci.* **1431**, 117–134 (1998).

[10] W. Wei, T. van Trung, S. Magliveras, F. Hoffman, Cryptographic primitives based on groups of hidden order, *Tatra Mt. Math. Publ.* **29**, 147–155 (2004).

Author information

Pinkimani Goswami, Department of Mathematics, North-Eastern Hill University, Shillong-793022, India.
E-mail: pinkimanigoswami@yahoo.com

Madan Mohan Singh, Department of Basic Sciences and Social Sciences, North-Eastern Hill University, Shillong-793022, India.
E-mail: mmsingh2004@gmail.com

Bubu Bhuyan, Department of Information Technology, North-Eastern Hill University, Shillong-793022, India.
E-mail: bbhuyan@gmail.com

Received: July 30, 2015.
Accepted: May 9, 2016.