SeMA (2016) 73:77–83
DOI 10.1007/s40324-015-0056-7

A new cryptosystem using generalized Mersenne primes

Jayanta Kalita[1] · **Azizul Hoque**[2] · **Himashree Kalita**[2]

Received: 16 June 2015 / Accepted: 9 November 2015 / Published online: 25 November 2015
© Sociedad Española de Matemática Aplicada 2015

Abstract In this paper we introduce a secure and efficient public key cryptosystem using generalized Mersenne primes based on two hard problems: the cubic root extraction modulo a composite integer and the discrete logarithm problem (DLP). These two problems are combined during the key generation, encryption and decryption phases. To break the scheme, an attacker has to solve the cubic root computation and the DLP separately which is computationally infeasible.

Keywords Public key cryptosystem · Generalized Mersenne primes · Discrete logarithm problem · Cubic root

Mathematics Subject Classification 94A60

1 Introduction

Diffie and Hellman [4] introduced the concept of public key cryptography, a new direction in cryptosystem through one of their seminal papers. This cryptography is widely used in e-commerce for authentication and secure communication. Diffie and Hellman [2] described a two-key cryptosystem in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. After that many public key cryptography were introduced based on tricky mathematical problems. Among these, RSA is one of the famous cryptosystems based on the factorization of a large integer was developed by Rivest et al. [15] in 1978. After a year, Rabin [14] proposed an RSA look alike cryptosystem based on the difficulty of extracting the square root modulo a large composite integer. On the other hand, El Gamal [5] proposed a proficient and simple cryptosystem based on discrete logarithmic problem (DLP). Elliptic curve cryptosystem (ECC) is another widely

✉ Azizul Hoque
ahoque.ms@gmail.com

[1] Department of Information Technology, GUIST, Guwahati 781017, India

[2] Department of Mathematics, Gauhati University, Guwahati 781014, Assam, India

used cryptosystem based on the problem of Discrete Logarithm. This Discrete Logarithmic Problem is computationally very hard to solve over a prime field or when considering the group of rational points of an elliptic curve defined over a finite field. Integer factorization and discrete logarithm problem are only believed to be hard but no proof is known for their NP-completeness or NP-hardness. Improvements in factorisation algorithms and computation power demand larger bit size in RSA key which makes RSA less efficient for practical applications. Although RSA and ECC have some drawbacks, they are still not broken. In 1999, Shor [16] discovered the polynomial time algorithm for integer factorization and computation of discrete logarithm on quantum computers. Thus once we have quantum computers in the range of 1000 bits, the cryptosystems based on these problems can no longer be considered secure. So, there is a strong motivation to develop public key cryptosystems based on problems which are secure on both conventional and quantum computers.

The composite discrete logarithm problem (CDLP) is a generalization of DLP which is used to design public key cryptosystems and certain protocols. It deals with the computation of $g^x \, mod \, n$ for some well chosen integers n and g. Hastad et al. [7] established, under the assumption of intractability of factoring a Blum integer n, that each bit of $g^x \, mod \, n$ is computationally very hard. They [7] also showed that the function $f_{g,n} \equiv g^x \, mod \, n$ can be used for efficient pseudorandom bits generators and multi-bit commitment schemes. Bach [1] established that solving the CDLP for composite moduli n is as hard as factoring n and solving it modulo primes. McCurley [12] proposed an alternative Diffie–Hellman key distribution protocol. He [12] also proposed an El Gamal signature scheme based on the CDLP. Pointcheval [13] developed an efficient authentication scheme based on the CDLP which is more secure than factorization. On the other hand, Ismail and Hijazi [10] believed that an efficient cryptographic scheme for a long term security can be designed by combining many cryptographic assumptions. With this conviction, they [10] proposed an efficient cryptographic scheme based on both the square root extraction and the CDLP. Since this scheme is based on two problems, they [10] claimed that it is more secure against the three common algebraic attacks using heuristic security technique.

Designing secure and efficient public key cryptosystems continues to be a challenging area of research in recent years. In this paper, we propose, by using generalized Meresenne primes, an efficient and strongly secure public key cryptographic scheme based on the cubic root extraction and the CDLP. This scheme is quite simple and has some advantages over similar scheme based on square root problem.

2 Generalized Mersenne primes

The concept of generalized Mersenne prime (GMP) was introduced by Hoque and Saikia [8]. They defined GMP as a prime number of the form:

$$M_{p,q} = p^q - p + 1$$

where p and q are some positive integers.

Hoque and Saikia [8,9] used these primes in study of class number problem of quadratic fields and cyclotomic fields. In this paper, we present another application of generalized Mersenne primes in construction of cryptosystems.

Throughout this article we consider the GMPs, $M_{p,q}$ with the following restrictions:

(i) p is a prime.
(ii) q is an odd positive integer.

Under these restrictions, we obtain that $M_{p,q} \equiv 1 (mod \, 3)$.

We now have the following immediate result.

Proposition 2.1 *Let $M_{p,q}$ be a generalized Mersenne prime. Then the function $\mathbb{Z}_{M_{p,q}} \to \mathbb{Z}_{M_{p,q}}$ given by $x \to x^3 (mod\ M_{p,q})$ is a one–one correspondence with the inverse function $x \to x^{\frac{1}{3}} (mod\ M_{p,q}) \equiv x^{\frac{p-1}{3}} (mod\ M_{p,q})$.*

3 The proposed public key cryptosystem

In this section, we present the proposed public key cryptosystem which will work in any arbitrary finite field of the form $\mathbb{Z}_{M_{p,q}}$.

3.1 Key generation

In this subsection, we describe the key generation of the proposed cryptosystem. Both public and private keys are used in this cryptographic scheme. These keys are generated as follows:

(i) Choose two generalized Mersenne primes M_{p_1,q_1} and M_{p_2,q_2}.
(ii) Compute $N = M_{p_1,q_1} M_{p_2,q_2}$.
(iii) Take an element $t \in \mathbb{Z}_N^* = \{z : \gcd(z, N) = 1\}$ such that $O(t)$, the order of t, is high.
(iv) Choose a number (randomly) $k < O(t)$.
(v) Compute $T \equiv t^k (mod\ N)$.

The finite field elements (N, t, T) and (N, t, k) are respectively the public keys and private keys.

3.2 Encryption

If Bob wants to send a message M to Alice, then he does the following steps to convert the plain text (message) P into the cipher text C.

(i) He transforms the plain text (message) into its numerical equivalent $m \in \mathbb{Z}_N$.
(ii) He chooses an integer (randomly) $l < N$ such that $|l| \leq \frac{|N|}{8}$.
(iii) He computes $c_1 \equiv (mT^l)^3 (mod\ N)$ and $c_2 \equiv t^l (mod\ N)$.

Finally he sends c_1 and c_2 to Alice.

3.3 Decryption

Alice uses both c_1 and c_2 to recover the original message M from the cipher text C. The following Lemma plays a vital to retrieve the original message M from the couple c_1 and c_2.

Lemma 3.3.1 $m' = c_1^{\frac{1}{3}} \times c_2^{-k} (mod\ N) \equiv m (mod\ N)$.

Proof. We have

$$m' = c_1^{\frac{1}{3}} \times c_2^{-k} (mod\ N) = m t^{lk} \times t^{-lk} (mod\ N) \equiv m (mod\ N)$$

By Proposition 2.1, the congruence

$$x^3 \equiv c_1 (mod\ N) \tag{3.1}$$

has a unique solution modulo M_{p_1,q_1} and has a unique solution modulo M_{p_2,q_2}. Thus using the Chinese Remainder theorem, we retrieve the unique solution modulo N to the congruence (3.1). The fact of unique solution to the cubic congruence is a great advantage over the Rabin [14] scheme where one can get four solutions to the quadratic congruence.

Example 3.3.2 Here is a toy example for our cryptosystem. Suppose we want to send a message M whose numerical value is $m = 5$ using our proposed cryptosystem.

Let us consider $M_{p_1,q_1} = 7$ and $M_{p_2,q_2} = 73$. Then $N = M_{p_1,q_1} M_{p_2,q_2} = 511$.

Let us choose $t = 11$ and $k = 5$. Then the public key is given by t, $T = t^k (mod\ N) \equiv 86(mod\ 511)$ and N. Also the private key is given by t, k and N.

We now encrypt the message $m = 5$ by considering $l = 5$. We compute $c_1 \equiv (mT^l)^3 (mod\ N) \equiv 97(mod\ 511)$ and $c_2 \equiv t^l (mod\ N) \equiv 309(mod\ 511)$.

For the decryption, we solve

$$x^3 \equiv 97(mod\ 511) \tag{3.2}$$

The congruence (3.2) can be re-written as the following system of congruence's:

$$x^3 \equiv 6(mod\ 7) \tag{3.3}$$

$$x^3 \equiv 24(mod\ 73) \tag{3.4}$$

Using Proposition 2.1, the solution of the congruence (3.3) is given by $x \equiv 5(mod\ 7)$. Similarly the solution of the congruence (3.4) is given by $x \equiv 35(mod\ 73)$. By the Chinese Remainder Theorem, the solution of the congruence (3.2) is $x \equiv 327(mod\ 511)$ and hence $c_1^{\frac{1}{3}} \equiv 327(mod\ 511)$.

Also we compute $c_2^{-k} = c_2^{-5} \equiv 386(mod\ 511)$.

Finally we obtain $m' = 327 \times 386(mod\ 511) \equiv 5(mod\ 511) = m$.

4 The security of the proposed cryptosystem

In this section we discuss the security of the proposed cryptosystem. In general, it is very difficult to prove the security of a public key as well as private key cryptosystem [11,17]. For example, if the public modulus of RSA is decomposed into its prime factors then the RSA is broken. However, it is not proved that breaking RSA is equivalent to factoring its modulus [6]. In this section, we give some security arguments and evidence that the proposed cryptosystem is highly secure against certain attacks. The security of the proposed cryptosystem partially depends of the factorization of N, where N is a product of two generalized Mersenne primes (GMP) M_{p_1,q_1} and M_{p_2,q_2}. However, this factorization problem is equivalent to determine the values of the primes p_1, p_2 and the odd integers q_1, q_2 such that they form two distinct generalized Mersenne primes M_{p_1,q_1} and M_{p_2,q_2} having property that congruence to 1 modulo 3. Thus it is not easy to solve this problem. It is noted that a pair of RSA primes may be generalized Mersenne primes having the above property. Therefore in this context we are not comparing generalized Mersenne primes with RSA primes. Brown [2] established that if the encryption function is $E(x) \equiv x^3 (mod\ N)$ and if N is a RSA number (or product of two RSA primes) with RSA public key $e = 3$, then the breaking of the corresponding cryptosystem is equivalent to the factorization of N. Thus a cryptosystem with the encryption function $E(x) \equiv x^3 (mod\ N)$ is not secure if $N$is a RSA number. In our cryptosystem, we use the cubic root extraction which is somehow analogous to $E(x) \equiv x^3 (mod\ N)$. This method is used to determine c_1 and its cubic root. This computation depends on the randomly chosen

integers l and T (or more precisely on l, t and k). Thus the problem of the computation of c_1 and its cubic root is not the same as if we use $e = 3$ in RSA cryptosystem. Even if c_1 and its cubic root are computable, then c_2 and its inverse have to be computed which is computationally very hard. Thus we claim that our cryptosystem is more secure than that of RSA alike cryptosystems. We now discuss some attacks developed for the proposed cryptosystem. We also obtain that this proposed scheme is heuristically secure against these common attacks. The attacks discuss in this section are Direct attack, Factoring attack and Discrete Logarithmic attack.

4.1 Direct attack

Suppose an adversary *Adv* wants to recover all secret keys using all informations available from the system. Then *Adv* needs to solve the factorization problem to find the generalized Mersenne primes M_{p_1,q_1} and M_{P_2,q_2}. Moreover, *Adv* needs to solve the discrete logarithm problem to find the secret k. Thus the security of the private key k depends on the factorization of N. Most of the cryptanalysts use trial division, Quadratic Sieve (QS), Multiple Polynomial Quadratic Sieves (MPQS), Double Large Prime Variation of the MPQS and Number Field Sieve (NFS) for the factorization. Among these methods, NFS is the faster algorithm for numbers larger than 110 digits. It was used to factoring the ninetieth Fermat number. All these methods depend on the size of $|N|$. In other words, the complexity increases with the size of $|N|$. When the $|N| = 1024$, these techniques are computationally infeasible. Thus we use large generalized Mersenne primes M_{p_1,q_1} and M_{p_2,q_2} such that $|M_{p_1,q_1}| = |M_{p_2,q_2}| = 1024$ to maintain very strong security level.

4.2 Factoring attack

Suppose the attacker successfully factorized N and finds the values of p_1, p_2, q_1 and q_2. Now the attacker knows the values of M_{p_1,q_1} and M_{p_2,q_2}. By using Cube root method and Chinese Remainder Theorem, the attacker computes $m'' \equiv c_1^{\frac{1}{3}} (mod\ N) \equiv mA^l (mod\ N)$. However, to recover the message m from mA^l, the attacker needs the value of l which is the Computational Diffie–Hellman assumption. He has to solve the DLP modulo primes to find l. Since M_{p_1,q_1} and M_{p_2,q_2} are two Generalized Mersenne primes of size 1024, the DLP modulo primes infeasible and the attacker would fail.

4.3 Discrete logarithm attack

Suppose the attacker be able to solve the DLP and recover the private key. Then he can compute t^{lk} which is a part of the decryption. But it is still insufficient to recover m because he has to compute $c_1^{\frac{1}{3}} (mod\ N)$. Since the factorization of N is not known, it is computationally infeasible to compute the cubic root of c_1 modulo N. One can say that cubic root of c_1 modulo N can be computed by putting $e = 3$ just as in RSA cryptosystem. However, it is not possible as the factorization of N depends on four positive integers that form two generalized Mersenne primes and thus the attacker fails once again.

5 Efficiency

The encryption and decryption algorithm of the proposed cryptosystem have been designed in a beneficial approach but of course not sacrificing the security issues. It can be successfully

implemented on the various types of data. We have also tried to benchmark the performance of the encryption and decryption algorithms against some selected algorithms. The encryption algorithm is faster and it offers more enhanced security features than the others. Hence these algorithms are proved to be as a very efficient technique for transferring messages from sender to the receiver, achieving confidentiality as well as message authentication.

We compute the computation cost of our cryptosystem using the same method as described in [3]. The computational cost of the encryption and decryption of the proposed cryptosystem are respectively $(4\,|l| + 3)M_N$ and $(\frac{2}{3}\,|N| + |l|)M_N$, where M_N is the unity of the complexity, that is, the cost of a multiplication modulo N. On the other hand, the computational cost of the encryption and decryption of Galindo et al. as recorded in [3] are respectively $(36\,|e| + 3)M_N$ and $(\frac{20}{3}\,|N| + 36\,|e| + 24)M_N$. Similarly, the computational cost of the encryption and decryption of El Gamal cryptosystem are respectively $(40\,|p| + 13)M_N$ and $(20|p| + 24)M_N$. Thus we claim that our new cryptosystem is more efficiency than other RSA alike cryptosystems.

6 Conclusion

We have successfully designed an efficient and secure cryptosystem by combining two cryptographic assumptions namely the cubic root extraction and the discrete logarithm problem modulo a composite integer. We have also analysed our proposed cryptosystem against all known attacks and found that it is very secure.

Acknowledgments The corresponding author acknowledges UGC for JRF. The author's thank to Prof. H. K. Saikia, Head, Department of Mathematics for her valuable suggestions.

References

1. Bach, E.: Discrete Logarithms and Factoring, Technical Report UCB 84/186. Computer Science Division, University of California, Berkeley (1984)
2. Brown, D.R.L.: Breaking RSA may be as difficult as factoring. In: Cryptology. ePrint Archive, Report 205/380 (2006)
3. Castagnos, G.: An efficient probabilistic public-key cryptosystem over quadratic fields quotients. Finite Field Their Appl. **13**, 563–576 (2007)
4. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
5. El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**, 469–472 (1985)
6. Goldwasser, S., Bellare, M.: Lecture Notes on Cryptography, 2001 (Online). Available at http://www.cs.ucsd.edu/users/mihir/papers/gb.html
7. Hastad, J., Schrift, A., Shamir, A.: The discrete logarithm modulo a composite hides $O(n)$ bits. J. Comput. Syst. Sci. **47**(3), 376–404 (1993)
8. Hoque, A., Saikia, H.K.: On generalized Mersenne prime. SeMA J. **66**, 1–7 (2014)
9. Hoque, A., Saikia, H.K.: On generalized Mersenne primes and class-numbers of equivalent quadratic fields and cyclotomic fields. SeMA J. **67**, 71–75 (2015)
10. Ismail, E.S., Hijazi, M.S.: New cryptosystem using multiple cryptographic assumptions. J. Comput. Sci. **7**(12), 1765–1769 (2011)
11. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, New York (1997)
12. McCurley, K.S.: A key distribution equivalent to factoring. J. Cryptol. **1**, 95–105 (1988)
13. Pointcheval, D.: The composite discrete logarithm and a signature scheme based on discrete logarithms. In: Proceedings of the 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC'2000), LNCS 1751, Springer, Berlin, Heidelberg, pp. 113–128 (2000)

14. Rabin, M.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization. MIT Laboratory for Computer Science, Technical Report MIT/LCS/TR-212, Cambridge, USA (1979)
15. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
16. Shor, P.: Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Comput. **26**, 14–84 (1997)
17. Stinson, D.R.: Cryptography: Theory and Practice. CRC Press, Boca Raton (1995)