ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha*, Vol. 53(2) (2023), 74-78**
(Dedicated to Professor V. P. Saxena on His 80th Birth Anniversary Celebrations)

SECURITY OF PUBLIC KEY ENCRYPTION USING DICKSON POLYNOMIALS OVER FINITE FIELD WITH 2^k

Kamakhya Paul[1], Pinkimani Goswami[2] and Madan Mohan Singh[3]
[1]Department of Mathematics, North Eastern Hill University, Shillong, Meghalaya, India-793022
[2]Department of Mathematics, University of Science and Technology Meghalaya,
Ri-Bhoi, Meghalaya, India-793101
[3]Department of Basic Sciences & Social Sciences, North Eastern Hill University, Shillong,
Meghalaya, India-793022
Email: kamakhyapaul4@gmail.com, pinkimanigoswami@yahoo.com, mmsingh2004@gmail.com

*(Received : May 16, 2023; In format : May 27, 2023; Revised : August 09, 2023;
Accepted: August 30, 2023)*

DOI: https://doi.org/10.58250/jnanabha.2023.53209

Abstract

The application of Dickson polynomial in public key cryptography is observed due to its permutation behaviors and semi-group property under composition. Here we have mostly concentrated on checking the one-wayness and semantic security of our scheme. The proposed scheme is based on Dickson polynomial over a finite field with 2^k, whose security depends on the Integer Factorization Problem(IFP) and the Discrete Dickson Problem(DDP), which is as difficult as solving discrete logarithmic Problem (DLP). Our proposed cryptosystem is computationally secured with one-wayness and semantic security, it also reduces the complexity of many other proposed schemes.

2020 Mathematical Sciences Classification: 94A60, 11T06
Keywords and Phrases: Dickson Polynomial, Integer Factorization Problem, Discrete Dickson Problem, Discrete logarithm Problem, Encryption Scheme.

1 Introduction

Diffie and Hellman [5] in 1976 firstly proposed a cryptosystem, where transmission of messages takes place in an open network, known as Public Key Cryptography or asymmetric cryptosystem. In symmetric cryptosystem, the transmission of the secret key is done over an insecure channel and hence it is of higher insecurity. However, in asymmetric cryptosystem, separate keys are being used for encryption and decryption and hence it overcomes the insecurity problem. Security is of key importance in cryptography, as it is on which the proposed cryptosystem depends on.

Various parameters including number theory, group theory, field theory, braid group[21] and many others were involved to propose numerous cryptosystem to improve the security & efficiency and hence also came the involvement of Dickson polynomials too for the preparation of a more computationally secured and efficient cryptosystem. The application of Dickson polynomial in public key cryptography[10, 11, 12, 13] was involved due to its permutation behaviors and semi-group property under composition. It gave the researchers a new direction in cryptography. Dickson polynomial was firstly introduced by Dickson [4] in 1896, but it was later named by Schur[23] as Dickson polynomial. Lidl [13], in his paper have also surveyed the algebraic properties of Dickson polynomial over $\mathbb{F}_q$ and over the integers $\mathbb{Z}_n$, which helped to found the better way of its application in public key cryptography.

If prior knowledge of the hard problems is known only then it can be solved both ways, based on which most of the cryptographic schemes are being developed. Discrete logarithm and factoring of a large composite number in terms of primes, taken only one hard problem at a time were initially the hard problems that were being used includes for the propose of schemes. In 1988, two different number theoretic assumption were involved in the development of a single key distribution protocol by McCurley [17]. Numerous cryptosystem were proposed in the later year by [2, 6, 7, 8, 9, 18, 20, 24, 25, 26] which were based on the merging of two hard problems such as Discrete logarithm and factoring of a large composite number, Elliptic Curve discrete Logarithm, knapsack problem, and many more.

Here Discrete Logarithm and Integer Factorization is operated on Discrete Dickson Problem(DDP) over the finite field with cardinality 2^k and proposed a cryptosystem whose security is based on the hardness of solving *IFP* and *DDP*. Our work is mainly based on checking the one-wayness and semantic security of the scheme.

The rest of the paper is started with defining dickson polynomial, then followed by the security of our proposed cryptosystem which involved the One-way security and semantic security and finally the conclusion.

2 Dickson Polynomial

In 1896, Dickson [4] introduced a type of polynomial of the form

$$y^k + k\sum_{i=1}^{(k-1)/2} \frac{(k-i-1)...(k-2i+1)}{2.3...i} a^i y^{k-2i},\ k\ is\ odd,$$

over finite field F_q, which later came to be known as Dickson polynomial by Schur[23].

Definition 2.1. *(Dickson polynomial of first kind)* ([27]). *Let N be a positive integer and $a \in \mathbb{F}_q$,then the Dickson polynomial $D_N(y,a)$ of the first kind over any finite field F_q is defined by*

$$D_N(y,a) = \sum_{i\ =\ 0}^{\lfloor \frac{N}{2} \rfloor} \frac{N}{N-i}\binom{N-i}{i}(-a)^i y^{N-2i},$$

where $\lfloor \frac{N}{2} \rfloor$ is the largest integer less than or equal to $\frac{n}{2}$.

The Dickson polynomial satisfy the resurrence relation : $D_N(y,a) = yD_{N-1}(y,a) - aD_{N-2}(y,a)$, $N \geq 2$. under the initial condition $D_0(y,a) = 2$ and $D_1(y,a) = y$ and few initial polynomial are given below:

$D_2(y,a)= y^2 - 2a,$
$D_3(y,a)=y^3 - 3ay,$
$D_4(y,a)=y^4 - 4ay^2 + 2a^2,$
$D_5(y,a)=y^5 - 5ay^3 + 5a^2y.$

Commutativity under composition is of considerable importance satisfied by Dickson polynomial for $a = 0$ or 1 [19] *and hence it satisfies the semi-group property under composition:*

$$D_{MN}(y,1) = D_M(D_N(y,1),1) = D_M(y,1) \circ D_N(y,1) = D_N(y,1) \circ D_M(y,1) = D_{NM}(y,1)$$

Definition 2.2 (Modified Dickson Polynomial)**.** *Let us define a map, $D_P : \mathbb{Z}_N \to \mathbb{Z}_N$ defined as $z = D_P(y)(modN)$, where y and N are positive integers. Here, we call $z = D_P(y)(modN)$ as the modified Dickson polynomial. Below are few properties satisfied by modified dickson polynomial.*

1. *Modified Dickson polynomial is commutative under composition, that is*
$$D_P(D_Q(y)(modN)) = D_{PQ}(y)(modN) = D_Q(D_P(y)(modN)).$$
2. *Let Q be an odd prime and let $y \in \mathbb{Z}$ such that $0 \leq y < Q$. Then the period of the sequence $D_N(y)(mod\ Q)$ for $N = 0, 1, 2, 3, 4, ...$ is a divisor of $Q^2 - 1$.*

Müller and Nöbauer [19] *in* 1981, *firstly introduced the first key exchange cryptosystem which was based on Dickson polynomial, where the power functuions of the RSA system, introduced by Rivest et al.*[22] *in* 1978, *was replaced by Dickson ploynomials $D_n(x,a)$ with parameter $a = -1, 0, 1$. It was also observed the RSA cryptosystem was equivalent to Dickson system for parameter $a = 0$*[19] . *In* 2011, *Wei* [27] *introduced in his paper that Dickson polynomial $D_n(x,1)$ over a finite field 2^m is a permutation polynomial if and only if n is odd and proved that solving a discrete Dickson problem(DDP) is as difficult as solving discrete logarithmic problem (DLP). Note that, The hardness of DLP was also observed by McCurley* [16] *in his paper. It is also observed that, computable groups where DLP is hard to solve* [1, 3, 13] *are of very importance in cryptography.*

Definition 2.3 (Discrete Dickson Problem)**.** *Let R be a commutative ring with unity, for any $n \in \mathbb{Z}^+$, and given y and x , the problem of calculating the value of n such that $y = D_n(x,1)$ is called the Discrete Dickson Problem(DDP).*

It is observed throughout the paper that we have used for $a = 1$, $D_n(x,1) = D_n(x)$.

3 Security of the proposed public key encryption scheme

For the completeness of our work, here we have included our proposed public key encryption scheme. The scheme consists of three parts, that includes key generation, encryption and decryption.

Key Generation

1. Choose two random large primes P and Q of the same size, such that $2^P - 1$ and $2^Q - 1$ is prime.

2. Using the above P and Q compute $N = 2^k$, where $k = P \times Q$.
3. For the value of N, find $\phi(N)$, where $\phi(N) = (2^{2P} - 2^{P+1}) \times (2^{2Q} - 2^{Q+1})$.
4. Choose f, such that $1 < f < \phi(N)$ and $gcd(f, \phi(N)) = 1$.
5. Find c, such that $cf \equiv 1 \pmod{\phi(N)}$, where c is the modular inverse of f.
6. Choose h, such that $0 \leq h \leq \phi(N)$ - 1.
7. Choose a random $\alpha \in \mathbb{Z}_N^*$ and compute $y = \frac{1}{2}D_h(2\alpha) \pmod{N}$.

- ***PUBLIC KEY***: (N, f, y, α),
- ***PRIVATE KEY***: (P, Q, h, c).

Encryption

Here the process of encrypting the simple plain text into cipher text is permormed, so that an intruder doesn't get to read the message. For the message $M \in \mathbb{Z}_N$,

1. Select a random $s \in \mathbb{Z}_N^*$ and for the selected s, Compute $p_1 = \frac{1}{2}D_f(2s) \pmod{N}$.
2. Simillarly select $t \in \mathbb{Z}_N^*$ and for the selected t, compute $p_2 = \frac{1}{2}D_t(2\alpha) \pmod{N}$.
3. Now finally compute p_3 using selected s and the given y, where $p_3 = \frac{M}{4}D_t(2y)D_f(2s) \pmod{N}$.

For the plain text message 'M', the encrypted ciphertext is (p_1, p_2, p_3), which will be received by the decoder to generate the message.

Decryption

On receiving the encrypted message (p_1, p_2, p_3), the receiver performs the below given steps:

1. Firstly, he/she deals with obtaining the value of s, by computing $\frac{1}{2}D_c(2p_1) \pmod{N}$.
2. Followed by computing U, where $U = p_1^{-1} \pmod{N}$.
3. Compute V, where $V = p_3U \pmod{N}$.
4. Then compute T, where $T = \frac{1}{2}D_{h^{\phi(N)+1}}(2p_2) \pmod{N} = \frac{1}{2}D_t(2y) \pmod{N}$.
5. Finally obtain the plain-text message $M = VT^{-1} \pmod{N}$.

The security of the proposed cryptosystem is found to be completely build upon Integer Factorization Problem(IFP) and Discrete Dickson Problem(DDP). Here we have observed few cases of common attacks, one-wayness and semantic security, where the proposed cryptosystem was found to be computationally secured.

As the encrypted message can be assessed by an intruder, he/she can have assess to (p_1, p_2, p_3). Now, for him/her to generate the message M, he/she have to obtain the value of P and Q of k and so the value of c and followed by finding h from $\frac{1}{2}D_h(2\alpha)(\text{mod } N)$. And this can only be achieved if Integer factorization problem and Discrete Dickson problem can be solved. The value of P and Q is chosen in such a way that the size of k is 1024-bit and above, so no known algorithm can be used to factor k. And also to find h from $\frac{1}{2}D_h(2\alpha)(\text{mod } N)$, the intruder have to solve DDP. Also the value of α and s should be large enough to prevent exhaustive search attack. It should be kept in mind that to encrypt different messages different values of s and t should be used. Because if a sender uses same parameters for the encryption of two different messages M_1 and M_2, then the intruder can obtain $p_3 = \frac{M_1}{4}D_t(2y)D_f(2s)(\text{mod} N)$ and $p_3^{'} = \frac{M_2}{4}D_t(2y)D_f(2s)(\text{mod} N)$. And hence from the relation $M_2 = p_3^{'}p_3^{-1}M_1$, the intruder can have the message M_2 on knowing M_1. So on choosing different values of s and t, the message M_2 cannot be known even on knowing M_1.

Suppose the intruder somehow manages to find the value of P and Q and then computes $s = \frac{1}{2}D_c(2p_1)(\text{mod} N)$ and $V = p_3U(\text{mod} N) = p_3p_1^{-1}(\text{mod} N) = \frac{M}{2}D_t(2y)(\text{mod} N)$. To find the message M from above, one has to know t, which is computationally impossible assumption of Discrete Dickson Problem which is equivalent to solving DLP.

3.1 One-wayness

Here we check the one wayness of our proposed cryptosystem mentioned above.

Theorem 3.1. *Our proposed cryptosystem is one-way secured if both Integer Factorization Problem(IFP) and Discrete Dickson Problem(DDP) holds.*

Proof. Let us suppose that both integer factorization problem and discrete dickson problem is simple i.e., given a composite integer X, finding integers p and q such that $p.q = X$ is effortless and under a commutative ring R with unity, with given y and z, the task of obtaining the value of N, such that $z = D_N(y, 1)$ is also effortless, where $N \in \mathbb{Z}^+$, which means that , there exist a PPT algorithm $\mathcal{A}$ which can solve both integer factorization problem and discrete dickson problem. Our motive is to break the one-wayness of our proposed scheme by using the algorithm $\mathcal{A}$ and hence recover the plain text message m.

Let the challenging ciphertext be (p_1, p_2, p_3), $p_1 = \frac{1}{2}D_f(2s) \pmod N$, $p_2 = \frac{1}{2}D_t(2\alpha) \pmod N$ and $p_3 = \frac{M}{4}D_t(2y)D_f(2s) \pmod N$ and the public key be (N, f, y, α), where $y = \frac{1}{2}D_h(2\alpha) \pmod N$. Now we commence with aquiring the value of M. From the given value of p_1 and f, we obtain the value of s, followed by using the algorithm $\mathcal{A}$ we obtain the value of t from $p_2 = \frac{1}{2}D_t(2\alpha) \pmod N$, followed by obtaining the value of M, as $M = 4p_3(D_t(2y))^{-1}(D_f(2s))^{-1} \pmod N$. □

3.2 Semantic Security

In this section we are involved with checking the semantic security of our proposed cryptosystem. In semantic security the challenger generates the public key and the private key, *pk* and *sk* respectively. Keeps the private key to himself/herself and sends the public key to the adversary. Next the adversary selects two distinct messages m_0 and $m_1 \in M$ of same length and send it to the challenger. Here, the challenger selects any one of m_0 or m_1 and encrypts the corresponding ciphertext to it and send it to the adversary. On receiving the ciphertext from the challenger, the adversary objective is to identify which message was encrypted. If it can be achieved then the encryption scheme is not semantically secured else not, then semantically secured.

Discrete Dickson Assumption

Under the Discrete Dickson assumption, we assume that it is computationally hard to obtain the value of $N \in \mathbb{Z}^+$, given the value of z and y, where $z = D_N(y, 1)$.

Computational Discrete Dickson Assumption

The Computational Discrete Dickson Assumption states that, given the value of y and z, it is computationally hard to obtain the value of N from $z = D_N(y, 1)$.

Theorem 3.2. *If Computational Discrete Dickson Assumption holds, then the scheme presented in section* 3, is semantically secured.

Proof. Let us presume that the scheme proposed in section 3 is not semantically secured for the purpose of contradiction. Which speaks about the existence of a polynomial time algorithm $\mathcal{A}$, which can break the semantic security of our proposed scheme. With this, our objective is that to, given $\mathcal{G} = (y, z, w)$, with the help of algorithm $\mathcal{A}$, it is to decide whether it is conjugacy search problem of a random one (i.e $p = ab$ or not). Where $y = \frac{1}{2}D_a(2\alpha) \pmod N$, $z = \frac{1}{2}D_b(2\alpha) \pmod N$ and $w = \frac{1}{2}D_{ab}(2\alpha) \pmod N$. We first set the public key (N, f, y, α), where $y = \frac{1}{2}D_p(2\alpha) \pmod N$ and $\alpha \in \mathbb{Z}_N^*$; then once the adversary has chosen the messages m_0 and m_1, we overturn a bit q and we encrypt m_q as follows: $\mathrm{E}(m_q) = (p_1, p_2, p_3)$ where $p_1 = \frac{1}{2}D_f(2s) \pmod N$, $p_2 = \frac{1}{2}D_t(2\alpha) \pmod N$ and $p_3 = \frac{m_q}{4}D_t(2y)D_f(2s) \pmod N$.

Seemingly if $\mathcal{G}$ is a discrete dickson assumption, the above is an authentic encryption of m_q and algorithm $\mathcal{A}$ will deliver the accurate output with non negligible gain. On the contrary, if $\mathcal{G}$ is not a discrete dickson assumption, we assert that even a polynomially unbounded adversary gains no information about m_q from $\mathrm{E}(m_q)$ in a strong information-theoretic sense.

Let $p = ab$, and then the information received by the adversary is of the form $p_1 = \frac{1}{2}D_f(2s) \pmod N$, $p_2 = \frac{1}{2}D_t(2\alpha) \pmod N$ and $p_3 = \frac{m_q}{4}D_t(2y)D_f(2s) \pmod N = \frac{m_q}{4}D_t(D_{ab}(2\alpha))D_f(2s) \pmod N = \frac{m_q}{4}D_{ab}(D_t(2\alpha))D_f(2s) \pmod N \implies m_q = 4p_3(D_{ab}(2p_2))^{-1}(D_f(2s))^{-1} \pmod N$, and hence making the value of m_q infeasible which is completely hidden. And thus $\mathcal{A}$ cannot guess q better than at random. □

4 Conclusion

In this paper we have proved the one-way security and semantic security of our proposed public key cryptosystem based on *IFP* and *DDP*. Satisfying the one-wayness and semantic security by our proposed cryptosystem has proven that, it is computationally well secured against any known attack.

Acknowledgment

The authors are very much thankful to the Editor and the anonymous reviewer for their valuable suggestions to bring the paper in its present form.

References

[1] R. Alvarez, L. Tortosa, J. F. Vicent, and A. Zamora, Analysis and design of a secure key exchange scheme, *Information Sciences*, doi:10.1016/j.ins.2009.02.008, 2009, 2014-2021.

[2] W. Baocang and H. Yupu, Public key cryptosystem based on two cryptographic assumptions, *IEE Proceedings and Communications*, **152**(6) (2005), 861-865.

[3] D. Coppersmith, A. Odlyzko and R. Schroeppel, *Discrete Logarithms in GF(p)*, Algorithmica, 1986, 1-15.

[4] L. E. Dickson, The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group, *The Annals of Mathematics*, **11** (1896), 65120, 161-183.

[5] W. Diffie and M. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, **22**(6) (1976), 644654.

[6] P. Goswami, M. M. Singh and B. Bhuyan, A new public key scheme based on DRSA and generalized GDLP, *Discrete Mathematics, Algorithms and Applications*, **8**(4) (2006), 1650057.

[7] P. Goswami, M. M. Singh and B. Bhuyan, A New Public Key Scheme Based on Integer Factorization and Discrete Logarithm, *Palestine Journal of Mathematics*, **6** (2017), 580-584.

[8] R. Guo, Q. Wen, Z. Jin and H. Zhang, Pairing Based Elliptic Curve Encryption Scheme with Hybrid Problems in Smart House, *Fourth International Conference on Intelligent Control and Information Processing(ICICIP)*, Beijing, China, 2013, 64-68.

[9] E. S. Ismail and M. S. N Hijazi, A new Cryptosystem Based on Factoring and Discrete Logarithm Problems, *Journal of Mathematics and Statistics*, **7**(3) (2011), 165-168.

[10] R. Lidl and W. B. Müller, Permutation polynomials in RSA-cryptosystems, *Advances in Cryptography*, (1984), 293-301.

[11] R. Lidl and W. B. Müller, A note on polynomials and functions in algebraic cryptography, *Ars Combinatoria*, **17** (1984), 223-229.

[12] R. Lidl and W. B. Müller, On commutative semigroups of polynomials with respect to composition, *Monastsh. Math.*, **102** (1986),139-153.

[13] R. Lidl, Theory and applications of Dickson polynomials, *Topics in Polynomials of One and Several Variables and Their Applications: Volume Dedicated to the Memory of PL Chebyshev* , 1993, 371-395.

[14] A. Menezes, P.V. Oorschot and S. Vanstone, *Hand book of Applied Cryptographhy*, Bacon Raton, 1997.

[15] G. L. Mullen and D. Panario, *Handbook of finite fields*, CRC Press, 2013.

[16] K. S. McCurley , The discrete logarithm problem, *Cryptology and Computational Number Theory,Proceedings of Symposia in Applied Mathematics*, **42** (1990), 49-74.

[17] K. S. McCurley, A key Distribution System Equivalent to Factoring, *Journal of Cryptology*, **1** (1988), 95-105.

[18] M. S. A. Mohamad and E. S. Ismail, Threshold Cryptosystem Based on Factoring and Discrete Logarithm Problems, *AIP Conference Proceedings, American Institute of Physics*, **1571**(1) (2013), 1020 - 1023.

[19] W. B. Müller and R. Nöbauer, Some remarks on public key cryptography, *Studia Scientiarum Mathematicarum, Hungarica.* **16** (1981), 71-76.

[20] D. Poulakis, A Public Key Encryption Scheme Based on Factoring and Discrete Logarithm, *Journal of Discrete Mathematical Sciences and Cryptography*, **12** (2009), 745-752.

[21] K. Paul, M. M. Singh and P. Goswami, Algebraic braid group public key cryptography, www. vijnanaparishadofindia. org/jnanabha *Jñanabha*, **52**(2) (2022), 219-224, DOI: https://doi.org/10.58250/jnanabha.2022.52225.

[22] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM*, **21** (1978), 120-126.

[23] I. Schur, Arithmetisches über die Tschcbyscheffschen Polynome, Abhandlungen I-III, Spinger-Verlag, 1973, 422-453.

[24] Z. Shao, Signature Schemes Based on Factoring and Discrete Logarithms, *IEE Proceedings-Computers and Digital Techniques*, **145** (1998), 33-36.

[25] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah and O. M. Al-Hazaimeh, A new public key encryption scheme with chaotic maps, *International Journal of electrical and computer engineering*, **10**(2) (2020), 1430-1437.

[26] N. Tahat, A. K. Alomari, O. M. Al-Hazaimeh and M. F. Al-Jamal, An efficient self-certified multiproxy signature scheme basedon elliptic curve discrete logarithm, *Journal of Discrete Mathematical Sciences and Cryptography*, **23**(4) (2020), 935-948, DOI: 10.1080/09720529.2020.1734293.

[27] P. Wei, Key exchange based on Dickson Polynomials over finite field with 2^m, *Journal of computers*, **6**(12) (2011), 2546-2551.