Crypto Algorithm for Binary Numbers using Knapsack via Bezier curve

Baleegh M. Alshaeer
Department of Mathematics, Faculty of Computer science and Mathematics
University of Kufa
Najaf, Iraq
baleeghm.alshaeer@student.uokufa.edu.iq
Orcid.org/0009-0002-9441-9066

Adil AL-Rammahi
Department of Mathematics, Faculty of Computer science and Mathematics
University of Kufa
Najaf, Iraq
adilm.hasan@uokufa.edu.iq
Orcid.org/0000-0003-3856-0663

DOI: http://dx.doi.org/10.31642/JoKMC/2018/120103
Received Jun. 14, 2025. Accepted for publication Feb.14, 2025

***Abstract*—** *These days we are constantly sharing and storing sensitive information online. From credit card numbers to personal identity details, our data is vulnerable to cyber-attacks and breaches. With the increase in cybercrime and hacking techniques, it is becoming increasingly important to protect our data through encryption.*

This work aims to create a secure binary number of the system of encryption and to make cipher analysis impossible. We will combine Knapsack's cipher with the equations of Bezier curves using the three-pass protocol.

The robustness of the proposed methods has been proved and the high security level by the experimental results, where the proposed methods have been more efficient and complex. The computational complexity of this method has been implemented in detail.

***Keywords*— Binary numbe; Knapsack cipher; Bezier curves**

I. INTRODUCTION

To encryption and re-encryption, or what is called the encryption system, which deals with texts, images, and sounds to be circulated through a special language between the sender and the receiver, despite being noticed by everyone. The encryption is carried out using a secret key that the two communicating parties had previously agreed upon. The encryption and decryption keys are kept secret, so only those who know them for encryption or decryption of the message .An adversary cannot understand or decipher the message because of the secret keys. Thus, Alice and Bob can communicate freely.

These four points must be applied to prevent someone outside the system from opening the code: :

1. Read the secret message.
2. Locate the secret key, so that they can read all messages encrypted with it.
3. Modify Alice's message to avoid detection by others.
4. Pretend to be Alice and send Bob a message, making Bob believe he is speaking with Alice when he is actually speaking with the adversary. [1-2]

Cryptosystems employ several security features, including as secrecy, data integrity, authentication, and nonrepudiation, to keep adversaries from achieving their objectives.

1. The term "confidentiality" refers to the keeping of a sent message or information private, with only authorized parties able to decode it.
2. Data integrity verifies that no modifications are being made to the messages. This prevents the enemy from achieving their third objective.
3. The authentication may be enable Bob to recognize Alice has the sender and prevents the work of attacker.
4. Alice cannot refute that she sent the communication because of nonrepudiation.[3-5]

Knapsack encryption deals with any n-vectors of binary digits with respect to its super increasing basis. It has enough flexibility in use. For instance when we wanted to encrypt 10-binary vectors, we can use the increasing basis (1,2,3,6,12,18,30,48,78,136) mod 217. This paper studied for improved Knapsack encryption with Bezier approximation method. The powerful of Bezier deduced form its control points which here choosing randomly. This work seeks to develop a secure binary number of encryption systems which makes cipher analysis impossible. We will use the combining of Knapsack problem and Bezier curve equation without requiring the exchange of keys. One can put the procedure of this work as following.

1) Given n-vector binary digit B.
2) Compute K(B) the integer kpnapsack value.

3) *The sender computes any Bezier(Z_1) of K.*
   Z_1*K
4) *The receiver computes any Bezier(Z2) of (Z_1).*
   Z_2* Z_1*K
5) *The sender computes (Z_1) $^{-1}$* Z_2* Z_1*K.*
6) *The receiver computes (Z2) $^{-1}$* Z_2* K and so he has K.*

For a survey of related works, Merkli and Helman introduced the knapsack for hiding information and signature of binary numbers[6]. Krishna algorithm is iterated by the values which are randomly picked from the basin of knapsack values [7]. Khalifa et al [8] used the combination of RSA (Rivest-Shamir-Adelman) hybrid system and knapsack method. Lu and Li [9] used knapsack in the text cryptography. Yamanda et al [10] introduce combination method of knapsack problem and the minimum spanning tree. In Peasah et al algorithm [11] Knapsack is employed in selecting adverts to play on air from a pile of adverts. Roland et al [12] measured the adjustment of encrypted knapsack by the Chebyshev distance. Dean [13] studied the stochastic knapsack problem and its benefit. Bonus, and Boating [14] used knapsack technique in improved shield of drift reduction centre nozzle. Vinothini enhanced asymtric key via knapsack[15]. Habib etal [16] used approximated Legendre method to encryption of integer numbers. Alrammahi[17] used least squares approximations for cryptography for any degree. Sujit and Dhara using Bezier curve for image encryption Via scan pattern [18]. Ismail and Yushalify used cubic Bezier for eleptic curve and Hill cipher[19]. Hala and Tanya using quadratic curve via Chebyshev polynomial [20]. Srividya and Akhila enhanced Bezier curve over Galio field [21].

II. MATHEMATICAL CONCEPT OF CRYPTOGRAPHY AND INTERPOLATION

A. Cryptography

The security of a knapsack cryptosystem relies on the resilience of the cipher. Simple versions of these algorithms do not provide adequate secrecy, making them less popular [3]. Furthermore, the knapsack cryptography method is represented by Merkle-Hellman Public Key in 1978[4].
Knapsack cryptosystems use smart transformations to hide their basis and defeat attacks techniques. Each knapsack cryptosystem has unique methods for defeating common cryptanalytic techniques.

Merkel and Hellman which is one of the public key algorithms and based on modular super increasing basis.

1. One can select n-vector represents the positive integer super-increasing sequence [5].
2. Choosing random integer q , $q > \sum_{i=1}^{n} S_i$
3. One can select r where GCD (r , q) = 1.
4. Calculating sequence $B = (b_1, b_2, \dots, b_n)$ where $b_i = rS_i mod\ q$ for (s ,q ,r)- private key while B-Public-key.

For the plain binary vector m = (m_1 ,m_2 ,…,m_n) we have encryption,

$C = \sum_{i=0}^{n} m_i\, b_i$ (C is the ciphertext)
The Crypto-Kp offers a great way to generate public and private keys.
Encryption protects data on computers, storage devices, and in transit over networks. For example and in mod 11, one can take $a = \{1, 2, 4\}$, $n = 3$, $n^{-1} = 4$, $m = (1,0,1)$,
$b = n.a = \{3, 6, 1\}$, then $c = m.b = 4$.
For decryption, the receiver has $n = 3$, $n^{-1} = 4$, $b = \{3, 6, 1\}$, and modular 11 to decrypt 4, he calculates
$a = inv(3).b = \{1, 2, 4\}$, and $c_1 = c.n^{-1} = 4(4) \bmod 11 = 5$,
finally comparison c_1 with a as follow:
$5 \geq 4\ yes\ \ ,then\ \ a_3 = 1$
$5 - 4 = 1 \geq 2\ no\ \ ,then\ \ a_2 = 0$
$1 \geq 1\ yes\ \ ,then\ \ a_1 = 1$
So the original message is $(1,0,1)$.

B. Interpolatin

Pierre Bézier introduced the Bézier curve in 1962 [24], and he used it to plan the car's body. Then it had several technological uses, the most prominent of which was the computer graphics applications (CGA).. Bézier curves are polynomial curves that are widely used due to a variety of mathematical properties that make them easy to manipulate and analyze.

The nth degree Bezier curve requires n+1 control points, which distinguishes it from previous approximation methods [22-24]. A degree n Bézier curve has n + 1 control points with blending functions denoted as B_i^n (t).

Where $B_i^n(t) = \binom{n}{i}(1-t)^{n-t}t^i\ \ , i = 0,1,2, \dots, n$

Such that $\binom{n}{i} = \frac{n!}{i!(n-i)!}$

In the degree three case, $n = 3$ and $B_0^3 = (1-t)^3, B_1^3 = 3.t.(1-t)^2$,
$B_2^3 = 3.t^2.(1-t)$ and $B_3^3 = t^3.B_i^n(t)$
: $r(t) = \sum_{i=0}^{n}\binom{n}{i}(1-t)^{n-i}.t^i P_i$
Then : $r(t) = \sum_{i=0}^{n} B_i^n(t) P_i\ \ , 0 \leq t \leq 1.$

1. one degree, $n = 1$

$$r(t) = B_0^1(t)P_0 + B_1^1(t)P_1$$
$$= \binom{1}{0}(1-t)^{1-0}t^0 P_0 + \binom{1}{1}(1-t)^{1-1}t^1 P_1$$
$$= \binom{1}{0}(1-t)P_0 + \binom{1}{1}t^1 P_1$$

$= \frac{1!}{0!(1-0)!}(1-t)P_0 + \frac{1!}{1!(1-1)!}t^1 P_1 = (1-t)P_0 + tP_1$
Then, the equation of linear Bezier curve is :
$\boldsymbol{r(t)} = (1-t)P_0 + tP_1\ \ , for\ t \in [0,1] \dots\dots\dots (1)$

Let $(x(t), y(t))$ is a parametric form of linear Bezier curve $B(t)$ with the point $P_0 = (1,3)$ and $P_1 = (3,5)$ where [10]

$$x(t) = (1-t)(1) + t(3) = 1 + 2.t$$
$$y(t) = (1-t)(3) + t(5) = 3 + 2.t$$

So, when $t = 0.5$
Then

$$x(0.5) = 1 + 2.(0.5) = 2$$
$$y(0.5) = 3 + 2.(0.5) = 4$$
$$r(t) = (x(t), y(t))$$

Then $r(0.5) = (2,4)$

In the same manner one can work for any degree.

III. CRYPTOGRAPHY OF BINARY NUMBERS USING KNAPSACK AND BEZIER CURVE

In this section, a method that combines algebra and numerical analysis was explained. The algebraic method will be represented by the Knapsack cipher algorithm, and Bézier curves will represent the numerical method. We will apply the method to binary numbers.

A. Proposed algorithm

1. Agreement between the sender and receiver on the Knapsack cipher algorithm.
2. Share the public key, M modulo.
3. Apply the algorithm steps below.

Step 1: key generation (the sender)

1. Alice chooses the private key " P " must be a basis super-increasing vector.
2. Alice chooses M modulo.
3. Alice chooses N such that $1 \leq N < M$.
4. Alice computes the public key $PK_i = N * P_i \ mod \ M$.

Step 2: Encryption (the sender)

1. Alice chooses a plaintext W that is a binary number if it is a decimal number, convert it to a binary number, or if it is a word, convert it to decimal numbers by ASCII and then to binary numbers.
2. Alice will split the plaintext into groups of the number of value the private key have.
3. Alice computes $C_j = \sum_1^n W_{j_i} * PK_i$.
4. Alice chooses three control points P_0, P_1, P_2 .
5. Alice substitutes the control points in the quadratic Bézier curve.
6. Alice chooses $t_1, t_2$to get two points lies on the Bézier curve.
7. Alice computes the distance between the new points d_A.
8. Alice computes $C_j * d_A \ mod \ M = CA_i$.
9. Alice sends CA_i .

Step 3:Decryption (the receiver)

1. Bob receives CA_i.
2. Bob chooses four control points P_0, P_1, P_2, P_3 .
3. Bob substitutes the control points in the cubic Bézier curve.
4. Bob chooses $t_1, t_2$to get two points lie on the Bézier curve.
5. Bob computes the distance between the new points d_B.
6. Bob computes $CA_i * d_B \ mod \ M = CAB_i$
7. Bob sends CAB_i to Alice.

Step 4: decryption (the sender)

1. Alice receives CAB_i.
2. Alice computes $CAB_i * d_A^{-1} mod \ M = CB_i$.
3. Alice sends CB_i to Bob.

Step 5: decryption (the receiver)

1. Bob receives CB_i.
2. Bob computes $CB_i * d_b^{-1} mod \ M = C_i$.
3. Bob computes $N^{-1} mod \ M$.
4. Bob computes P= $N^{-1} * PK_i \ mod \ M$.
5. Bob computes $C_i * N^{-1} mod \ M = W_i$
6. Bob will have to make the sum of W_i from the values of the private key.
7. Bob gets the plaintext.

B. Implementation

Alice chooses a super increasing private key { 2, 5, 13, 23 } = P, and two numbers one of them the module M=47 such that $M > \sum P_i$, the other one is N =25 such that $1 \leq N < M$ and gcd(M,N)=1.

Alice computes the public key by using this

$$PK = \{N * P_i \ mod \ M\}$$
$$PK = \{3, 31, 43, 11\}$$

Alice wants to send a plaintext " 1010 1110 0110 " of three 4-vectors. To encrypt the plaintext Alice divided it into three sets of four numbers depending on the number of values in the private key

$$m_1 = 1010 \ , m_2 = 1110 \ , m_3 = 0110$$

Alice computes $C_j = \sum_1^n M_{j_i} * PK_i$

$$C_1 = 46 \ , C_2 = 77 \ , C_3 = 74$$

Now Alice uses a quadratic Bézier curve of control points (which chosen randomly) $P_0(1,4), P_1(3,6), P_2(5,10)$.

$$r(t) = (1-t)^2.P_0 + 2.(1-t).t.P_1 + t^2.P_2 \qquad t \in [0,1]$$

When $t = 0.25$

$$x(t) = x(0.25) = (1-0.25)^2.1 + 2\ .(1-0.25).(0.25).(3)$$
$$+(0.25)^2.(5) = 2$$
$$y(t) = y(0.25) = (1-0.25)^2(4) + 2.(1-0.25)(0.25)(6)$$
$$+(0.25)^2(10) = 5.125$$

The first point is P (2, 5.125)

If $t = 0.4$

$$x(t) = x(0.4) = (1-0.4)^2.1 + 2\ .(1-0.4).(0.4).(3)$$
$$+(0.4)^2.(5) = 2.6$$
$$y(t) = y(0.4) = (1-0.4)^2(4) + 2.(1-0.4)(0.4)(6)$$
$$+(0.4)^2(10) = 5.92$$

The second point is Q (2.6, 5.92) .

Now Alice computes the distance between points

$$d_A = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

$$d_A = \sqrt{(2 - 2.6)^2 + (5.125 - 5.92)^2} = 996 * 1000^{-1}$$

Now do

$$C_j * d_A \ mod \ M$$

$$46 * 996 * 1000^{-1} \ mod \ 47$$

$$46 * 996 * 29 \ mod \ 47 = 21 = CD_1$$

$$77 * 996 * 29 \ mod \ 47 = 28 = CD_2$$

$$74 * 996 * 29 \ mod \ 47 = 44 = CD_3$$

Alice sends CD_1, CD_2, CD_3 to Bob .

Bob receives CD_1, CD_2, CD_3

Bob uses cubic Bezier of control points

$P_0(0,5), P_1(3,9), P_2(5,12), P_3(8,20)$.

$$r(t) = (1-t)^3 P_0 + 3(1-t)^2 t P_1 + 3(1-t)t^2 P_2 + t^3 P_3$$

If t = 0.1

$$x(t) = x(0.1) = (1-0.1)^3.(0) + 3.(1-0.1)^2.(0.1).(3) + 3.(1-0.1).(0.1)^2.(5) + (0.1)^3(8) = 0.872$$

$$y(t) = y(0.1) = (1-0.1)^3.(5) + 3.(1-0.1)^2.(0.1).(9) + 3.(1-0.1).(0.1)^2.(12) + (0.1)^3(20) = 6.176$$

The first point P(0.872,6.176)

If t =0.7

$$x(t) = x(0.7) = (1-0.7)^3.(0) + 3.(1-0.7)^2.(0.7).(3) + 3.(1-0.7).(0.7)^2.(5) + (0.7)^3(8) = 5.51599$$

$$y(t) = y(0.7) = (1-0.7)^3.(5) + 3.(1-0.7)^2.(0.7).(9) + 3.(1-0.7).(0.7)^2.(12) + (0.7)^3(20) = 13.988$$

The second point is Q (5.51599,6.176)

Now Bob computes the distance between points

$$d_B = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

$$d_B = 9088 * 1000^{-1}$$

Now compute

$$CD_i * d_B \ mod \ 47$$

$$21 * 9088 * 1000^{-1} mod \ 47$$

$$21 * 9088 * 29 \ mod \ 47 = 13$$

$$28 * 9088 * 29 \ mod \ 47 = 33$$

$$28 * 9088 * 29 \ mod \ 47 = 25$$

Bob sends 13,33,25 to Alice

Alice receives 13,33,25 and multiply it by the inverse of the distance

$$13 * 996^{-1} * 29^{-1} mod \ 47$$

$$13 * 21 * 13 \ mod \ 47 = 24$$

$$33 * 21 * 13 \ mod \ 47 = 32$$

$$25 * 21 * 13 \ mod \ 47 = 10$$

Alice sends 24,32,10 to Bob.

Bob receives 24,32,10 and multiplies it by the inverse of the distance

$$24 * 9088^{-1} * 29^{-1} mod \ 47$$

$$24 * 36 * 13 \ mod \ 47 = 46$$

$$32 * 36 * 13 \ mod \ 47 = 30$$

$$10 * 36 * 13 \ mod \ 47 = 27$$

Now Bob computes the inverse of $25^{-1} mod \ 47 = 32$

Then finds private key {2,5 ,13,23}

Multiply $46 * 32 \ mod \ 47 = 15$

Multiply $30 * 32 \ mod \ 47 = 20$

Multiply $27 * 32 \ mod \ 47 = 18$

Now Bob takes 15,20,18 and see

$$15 < 23 \rightarrow 0 \ , \ 15 > 13 \rightarrow 1 \ , 2 < 5 \rightarrow 0 \ , 2 \leq 2 \rightarrow 1, m_1 = 1010 \ .$$

$$20 < 23 \rightarrow 0 \ , \ 20 > 13 \rightarrow 1 \ , 7 > 5 \rightarrow 1 \ , 2 \geq 2 \rightarrow 1, m_2 = 1110$$

$$18 < 23 \rightarrow 0 \ , \ 18 > 13 \rightarrow 1 \ , 5 \geq 5 \rightarrow 1 \ , 0 \leq 2 \rightarrow 0, m_3 = 0110$$

$$M = \text{"1010 1110 0110"}$$

which represents the plain text.

iv. DISCUSSION AND CONCLUSION

For the purpose of presenting a new method for encrypting binary numbers, the knapsack method has been enhanced by the Bezier approximation method. Bezier may be used for any degree for both parties of the cipher without the condition that they agree on the same degree. Bezier's possession of control points makes him more flexible than others. In addition, it has the possibility of maneuvering and talking to change these points. The parameter variable t in Bezier produces two paths, one for x(t) and the other for y(t). These two paths were used to present the distance by choosing any two values for the parameter variable. This added a lot of

complexity to the combined method of knapsack and Bezier. The distance here is independent for both the sender and the receiver. The elegance of our proposed method deduced from the preserved the nature of the integer numbers. In a single encryption process, we noticed that the number, after being affected under a Bezier, is sent from sender to the receiver, who in turn performs another Bezier operation and then sends it to the sender. Thus, the both encryption and decryption processes are completed in a manner similar to a path on the letter Z. The Proposed method has compound. Here the traditional method of single transmission has been bypassed. These conclusions have been observed, applied and seen through the detailed implementation. Finally, we can say that two branches of mathematics, namely algebra represented by knapsack, as well as the approximation represented by Bezier, have been combined and agreed between them to produce a new method of encryption of binary numbers.

References

[1] Wade Trappe and Lawrence Washington, "Introduction to Cryptography with Coding Theory", Pearson Education, Inc., 2006.

[2] Christof Paar and Jann Pelzl, "Understanding Cryptography, Springer, Berlin, Heidelberg", 2010.

[3] A. Menezes, and P. Orschot, "Handbook of Applied Cryptography" ,CRC Press,1996, pp.283-319.

[4] Dwi Liestyowati, "Public Key Cryptography" Journal of Physics Conference Series 1477:052062, March 2020.

[5] Richard A. Mollin, "An Introduction to Cryptography" Journal Discrete Mathematical& Applications, 2000.

[6] R. Merkle, M. Hellman, "Hiding Information and Signatures In Trapdoor Knapsacks", IEEE Trans. on Inform. IT-24, 5,Sept., 1978, pp. 525-530.

[7] A. Krishna, "An Improvised ECC Mechanism with Probabilistic Approach", Information Security Journal: A Global Perspective ,vol 21, no.1, 2012, pp. 28-35.

[8] S. Kallpha, J. Abdul Sada , H. Hussain, "New Public-Key cryptosystem", International Journal of Systems Science,Vol.1, No.1,(2012, Pp. 205-215.

[9] Y. Lu , J. Li, "New forward-secure public-key encryption without random oracles, International Journal of Computer Mathematics", Vol. 90, Issue 12, , 2013, pp. 2603-2613.

[10] T. Yamada, K. Watanabe And S. Kataoka, "Algorithms to Solve the Knapsack Constrained Maximum Spanning Tree Problem", International Journal Of Computer Mathematics, Taylor & Francis Group Publisher, Vol. 82, No. 1, January, 2013, pp.23–34.

[11] O.K. Peasah, S. K. Amponsah and D. Asamoah, "Knapsack problem: A case study of garden city radio (GCR), Kumasi", Ghana,African Journal of Mathematics and Computer Science Research , Academic Journals Vol. 4(4), April, 2011, pp. 170 -176.

[12] J. Roland, Y. Smet, and J. Fegueira, "The Inverse Multi-Objective {0,1}-Knapsack Problem Under the Chebyshev Distance", Technical Report Number, 2011, pp,1-9.

[13] B. C. Dean, M. X. Goemans, J. Vondrak, "Approximating the Stochastic Knapsack Problem: The Benefit of Adaptivity", Mathematics of Operations Research, Inform Publisher Vol. 33, No. 4, November,. 2008, pp. 945–964.

[14] P. O. Bonsu, and M. A. Boateng, "Improved shield for knapsack sprayers", Agricultural Science Research Journals, International Research Journals publisher, Vol. 3(3), , March, 2013, pp. 93-96.

[15] N. Vinothini, "Asymmetric Key Cryptography using Merkle-Hellman Knapsack Method and Genetic Algorithm", Journal of Computer Engineering and Applications, Vol. XII, Issue I, Jan. 18, 2018, pp.1-9.

[16] Hamza B. Habib, Wadhah A. Hussein, Diana S. Mahdi "Improving the security of the Knapsack Cryptosystem by using Legendre Symbol", Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12(11), , 2021, pp. 2249-2255.

[17] Adil Alrammahi, "Image Cryptography with Least Squares Approximations", JCS, science publications, 15,11, 2019, pp. 1659-1668.

[18] Sujit Das, Bibhas Dhara, "A new image encryption method using Bezier curve", Multimedia Tools and Applications, 82,30, 2023, pp. 1-42.

[19] Nur Ismail, Yushalify Misro, "An Improved Image Encryption Algorithm Based on Bézier Coefficients Matrix", Journal of King Saud University - Computer and Information Sciences 34(1), 2022, pp. 1-8

[20] Hala Abdul Wahab, Tanya Jaber, "Using Chebyshev Polynomial and Quadratic Bezier Curve for Secure Information Exchange", Eng. Tech, 34, 5, 2016, pp. 666-674.

[21] B. Srividya, S. Akhila, "Selective Encryption of Video Frames Using Bezier Curve Over Galois Field GF (P^m)", ICTCS 16, 2016, pp. 33-44.

[22] Armstrong, Jim., " Quadratic Bézier curve", TecNote TN-05-003, 2005.

[23] Burkardt John. "Forcing Bezier Interpolation." Archived from the original on, 2013, pp. 12-25.

[24] M. Fadhel, "Analysis of Bézier Method Numerically with Applications", M.Sc thesis, Department of mathematics, College of Science, University of Kufa, 2009.