

Addition chain heuristics in application to elliptic curve cryptosystems

Mohamad Afendee Mohamed¹, Yahaya Garba Shawai^{1,2}, Mohd Noor Derahman³, Abd Rasid Mamat¹, Siti Dhalila Mohd Satar¹, Ahmad Faisal Amri Abidin¹, Mohd Fadzil Abdul Kadir¹

¹Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia

²Directorate of Examination and Assessment, National Open University of Nigeria, Lagos, Nigeria

³Department of Communication Technology and Network, Faculty of Computer Science, and Information Technology, Universiti Putra Malaysia, Seri Kembangan, Malaysia

Article Info

Article history:

Received Dec 21, 2023

Revised May 14, 2024

Accepted May 17, 2024

Keywords:

Addition chain

Elliptic curve cryptosystem

Finite arithmetic

Heuristics method

Polynomial time problem

ABSTRACT

The idea of an addition chain can be applied to scalar multiplication involving huge number operations in elliptic curve cryptosystems. In this article, initially, we study the taxonomy of the addition chain problem to build up an understanding of the problem. We then examine the mathematics behind an optimal addition chain that includes the theoretical boundary for the upper limit and lower limit which laid the foundation for experimentation hereafter. In the following, we examine different addition chain solutions that were used to increase efficiency in scalar multiplication. To avoid any possible confusion, we intentionally separated the discussion into two modules called integer recoding method and chain generator based on the heuristics method. These methods were developed by considering various aspects such as the space within which the operation is executed, the curve that is selected, the formulation to express the original equation, and the choices of operation and arithmetic, all together to improve operational efficiency.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohamad Afendee Mohamed

Department of Computer Science, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin
Gong Badak, 21300 Kuala Nerus, Terengganu Darul Iman, Malaysia

Email: mafendee@unisza.edu.my

1. INTRODUCTION

This article takes an evolutionary approach to the studies on the problematic addition chain [1]. The entire research was spearheaded by a question raised more than 100 years ago, for finding an optimal chain for any integer n by only allowing the addition of 2 earlier integers. When we mention optimal chain for n , we mean the shortest possible chain from 1 to n such that there exists no other path shorter than that. Furthermore, an optimal method means a method that can generate an optimal chain given an integer n . For a long time, the addition chain problem has been an interest of not so vast several researchers. But that was only until cryptosystems such as Rivest-Shamir-Adleman (RSA) and later elliptic curve cryptography (ECC) [2], [3] came around to capsize this perspective. Ever since, researchers have been pulling together efforts to integrate the two isolated fields into each other. The idea of an addition chain has been realized in RSA modular exponentiation and ECC scalar multiplication operations. Indeed, these works marked the real-world applicability of the addition chain for the first time ever.

Cryptography relies on one one-way function and a huge number of operations as the basis of a secrecy system. This function is properly selected such that the security is preserved and treated as the utmost importance consideration. Apart from that, efficiency comes next especially whenever the system is to be

used widely and exhaustively. In ECC this operation is largely contributed by scalar multiplication operation over $E(\mathbb{F}_2)$, formulated as $Q = nP$ where n is a scalar, P and Q are points on the curve. An excellent choice of the design and implementation of this operation contributes to an efficient cryptosystem. In reality, direct computation of scalar multiplication is a very resource-exhaustive operation. An alternative computation is sought to reduce the time and resources needed.

The formulation of scalar multiplication point arithmetic involves 4 different layers as shown in Figure 1. The upper layer is responsible for choosing the space and a specific curve that can contribute to the minimality. In this layer, a choice of working in affine space, projective space, Jacobian space, or Jacobian-Chudnosky space needs to be decided. The curve equation varies from one space to another to satisfy the type of group structure that we need to establish. The second upper layer decides how the original expression nP can be reduced to an equivalent but for more efficient execution. The third layer deals with elliptic curve point arithmetic such as addition, doubling, negation, inversion, and division. These operations are different from ordinary point arithmetic on Cartesian coordinates. A specific formula must be known a priori, and it varies from one curve to another. The lowest layer operates on finite field arithmetic where the formula takes on the values of x and y from a point P to produce point Q .

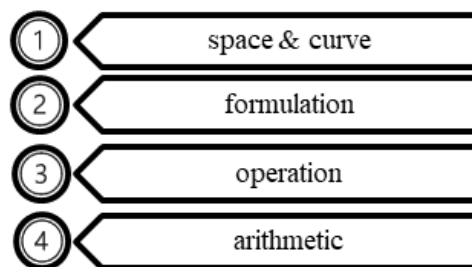


Figure 1. Addition chain-layered approach

In the beginning, the addition chain is seen as a solution to the scalar multiplication formulation layer problem. To some extent, yes indeed. An expression nP can be transformed into a more complicated form but with much simpler execution using iterations, such that $Q = nP = (2 \dots (2(2(P) + b_{r-1}P) + b_{r-2}P) + \dots) + b_0P)$. This formula computes nP into a series of operations each generating an integer altogether in ascending order until n . The goal is to find the least number of terms known as an optimal chain. The method that produces such a series is known as an optimal method. However, along the way, researchers realized that the scalar multiplication problem through the addition chain has only partly been solved, and better yet addition chain in itself is problematic and extra efforts are needed to address this new efficiency issue, that is in finding an optimal method. The optimal addition chain problem is not proved to be a nondeterministic polynomial time (NP) complete problem. Therefore, the complexity of the addition chain problem has remained an open problem until now. In contrast, there is no known algorithm that can generate an optimal chain for all n . In case one discovers an optimal addition chain method, an efficiency issue from the perspective of the addition chain can be closed.

From Figure 2, we can summarize the study of the addition chain problem into two main categories, one that involves theoretical mathematics regarding finding optimal chain, and upper and lower boundary values for a given integer n . The other involves computer experiments (simulation) to evaluate the performance of the methods that have been materialized. Further on, these methods can be subdivided into two namely heuristics and meta-heuristics. Note that, exact methods have been left aside due to the study by [4] which proved that finding an addition chain sequence is an NP problem, and consequently addition chain problem is so assumed.

Heuristics-based methods have been extensively studied and numerous literatures are available on these topics. Artificial intelligence, being an engine for meta-heuristics methods [5]-[8], has been widely accepted for solving NP-complete problems. Genetic algorithm in particular has been used for finding an optimal chain [9], [10]. Recently, the ant colony approach was implemented for finding the shortest addition chain and it was shown that this approach generates a chain that is always shorter than that of the genetic algorithm [11], [12]. Moreover, similar to classical methods, artificial intelligence approaches could also be combined to produce a hybrid method that could reach up to the nearest optimality. In this survey, we examine the list of heuristics methods available to date in great detail. The aim is to provide a comprehensive review of addition chain heuristics methods by having a breadth and depth approach to the subject matter.

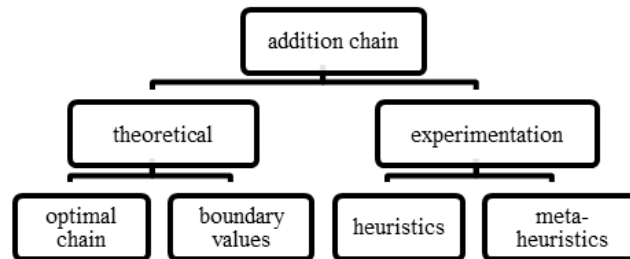


Figure 2. Subareas of study on addition chain

Due to the difficulties in finding the optimal addition chain method, the search for a solution for scalar multiplication through the addition chain approach remains open. However, it was shown that the scalar multiplication problem can be reduced to finding an efficient addition chain method that generates an addition chain, if not with optimal length but with the closest possible to optimal length. Methods that generate near-optimal addition chains are called heuristics methods. One important characteristic of these methods is that no one method is better than the other except for some cases of n . Therefore, a chain generated using a particular method is still possible to have redundant terms, of which other methods may find shorter.

In addition, solutions chain problems designated for ECC are targeting two classes of curves; a curve defined over any field and a curve defined over a specific field. In this paper, we discuss how different methods exploit the formula $Q = nP$ such that the operation of scalar multiplication is at utmost efficiency using an addition chain formula. The number of operations is represented by the number of primitive operations of addition and doubling which is likely proportional to the number of terms. Therefore, the timing parameter from scalar multiplication now depends on the number of terms in the generated addition chain. We denote the number of terms other than the first one as the length of an addition chain. Minimizing this parameter is the main focus of this paper.

As shown in Figure 3, heuristics methods for addition chains have two responsibilities, to recode integer n into some format and to generate the chain based on the recoded format. The right representation allows the generation of a minimal addition chain. Sign and radix are two main contributions to consider when designing a new representation.

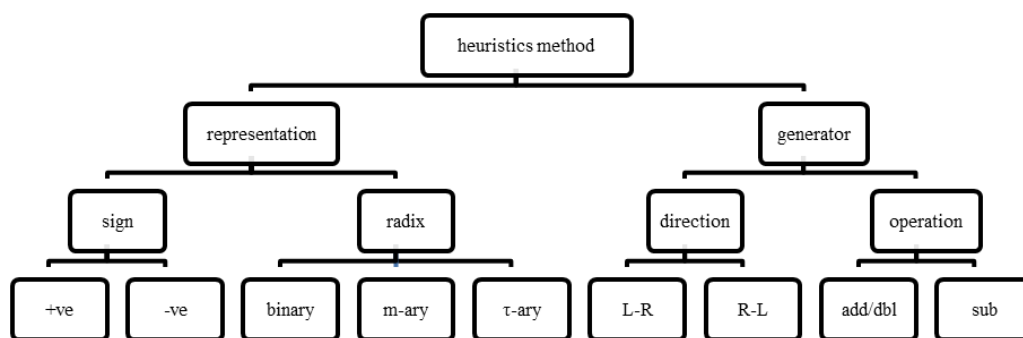


Figure 3. Subdivision of addition chain methods

The fact that the optimal addition chain method is non-existence, the challenges when dealing with the addition chain problem are as follows. Firstly, there is a pressing need to develop applications that effectively utilize addition chain solutions, requiring innovative approaches to tackle the problem. Secondly, the development of heuristic methods becomes essential, particularly those capable of working in conjunction with specific recording techniques to generate minimal chains efficiently. Additionally, there is a considerable endeavor to solve various mathematical open problems related to addition chains, underscoring the complexity and depth of the challenge at hand. In this survey article, we try to expose the following contributions which to the best of our knowledge are not documented anywhere: i) Take an evolutionary approach to understanding the concept of addition chain problem and solution about scalar multiplication that

of ECC and ii) Examine the fundamental issues regarding theoretical and experimental approaches to the addition chain problem.

The discussion is divided into the following. Section 2 examines into optimal addition chain from an analytical perspective. Section 3 examines various near-optimal methods for generating an efficient addition chain. Each method is separable into two different modules to choose a proper representation for n and another module to compute an addition chain for n . Section 4 discusses the challenges and issues of the addition chain.

2. THEORETICAL OPTIMAL OF ADDITION CHAIN

Simple operations such as addition and doubling require fewer resources in computer systems. Instead of operating a point P with a huge scalar n , there is a possible way of breaking this exhaustive computation into a sequence of addition and doubling operations in a journey to reach n .

Definition 2.1. Suppose n is an integer in the form of binary representation such that $n = b_c 2^c + b_{c-1} 2^{c-1} + \dots + b_0$. Then,

$$\lambda(n) = \lfloor \log_2 n \rfloor \quad (1)$$

$$v(n) = \sum_{i=0}^c b_i \quad (2)$$

where $b_i \in \{0,1\}$. Given an integer n , possibly starting from 1 (followed by 2), with allowable operations of addition and doubling of two previous terms to get a new one, the objective is to find the fastest way to reach n . From the computational complexity point of view, Downey *et al.* [4] proved that the problem of finding the smallest number of terms in the sequence is an NP-complete problem which says that there is no known NP algorithm to find an optimal solution. Huge interest was shown in producing a near-optimal solution resulting from various techniques. Researchers [13]-[15] discussed the resulting asymptotic values of addition chains. This idea gives way to the generalized definition of an addition chain which was initially studied by Dellac [16].

Definition 2.2. An addition chain for n is a sequence of positive integers of the form:

$$a_0 = 1, a_1, \dots, a_r = n \quad (3)$$

where $a_\gamma = a_\beta + a_\alpha$ such that $\alpha \leq \beta < \gamma$ for all $\gamma = 1, 2, \dots, r$. The length of the addition chain is equal to the number of elements in the sequence other than the initial term a_0 , in this case, r . For any positive integer n , the shortest possible length of an addition chain for n is denoted by $l(n)$. The $l(n)$ is also famously called an optimal chain. Since there is no one algorithm in NP available to realize $l(n)$ for all n , a few different algorithms were developed to generate a near-optimal chain. One algorithm is better in some conditions than the others and vice versa. There is a special type of addition chain namely *ascending* addition chain, so named because the term $a_i > a_{i-1}$.

Definition 2.3. An ascending addition chain for n is a sequence of positive integers of the form:

$$a_0 = 1 < a_1 < \dots < a_r = n \quad (4)$$

where $a_\gamma = a_\beta + a_\alpha$ such that $\alpha \leq \beta < \gamma$ for all $\gamma = 1, 2, \dots, r$. A variation with $\beta = \gamma - 1$ for all a_i is known as *star* chain, and its chain is denoted by $l^*(n)$ for which $l(n) \leq l^*(n)$ [17]. This chain resembles the sequence generated by *add and double* method to be discussed in section 3. Many studies were conducted to analyze the behavior of $l(n)$ for this specific type of chain. The studies centered around conjectures that were stated in the early 20th century. Researchers tend to prove or disprove those conjectures as well as improve some boundaries for upper bound and lower bound. The most notable one was due to [18], [19]. But before that, let's look at the following lemma that will be of some use later, which simply says that for n of m th power of 2, an optimal chain is given by m .

Lemma 2.4. [20]. Let n be an integer such that $n = 2^m$. Then $l(n) = m$. Lemma 2.4 could also be proved through mathematical induction on m . Much earlier than this, Scholz published his first question on the boundary of $l(n)$ in the following theorem.

Theorem 2.5. [18]. Let an integer n such that $2^m + 1 \leq n \leq 2^{m+1}$, then $m + 1 \leq l(n) \leq 2m$ for $m \geq 1$. The proof is provided by Brauer and is split into two parts, the lower bound and the upper bound. A simple approach was used which is to look at n in its binary form.

Theorem 2.6. [18]. Let n be an integer such that $n = ab$. Then $l(ab) \leq l(a) + l(b)$. This second problem from Scholz was also proved by Brauer. The chain for an integer ab is at most of the same length as the sum of the chains for each factor.

Studies on boundaries have received considerable attention [14], [15], [18], [21]-[24]. Erdos [24] stated that for almost all n , the following boundary is the best possible:

$$\log n + \log v(n) - 2.13 \leq l(n) \leq \log n + (\log n / \log \log n) + O(\log n / \log \log n) \quad (5)$$

For which the lower bound was due to Schonhage [21], while the upper bound was credited to Brauer [18].

Theorem 2.7. [19]. Let n be an integer such that $n = 2^{m+1} - 1$. $l(2^{m+1} - 1) \leq m + l(m + 1)$. This conjecture is known as Scholz's conjecture. From the integer range defined in Theorem 2.5, n was chosen to hold a value having the greatest number of 1's in its equivalent binary representation. It aims at studying the worst case for $l(n)$. Even after almost a decade, this conjecture has remained an open question until today. Although partial proof was suggested for star type addition chain. Brauer proved this conjecture holds for star chains such that $l^*(2^{m+1} - 1) \leq m + l^*(m + 1)$. Only recently, Agama [25] showed that using the pothole method, a slightly weaker inequality holds for this number family. Earlier studies were based on the hamming weight. Utz [20] studied this problem for the case $v(n) = 1$ and $v(n) = 2$ and he proved that $l(n) = \lambda(n)$ and $l(n) = \lambda(n) + 1$ respectively, and the trueness of Scholz's conjecture holds accordingly. Much later Gioia *et al.* [26] came out with a proof for $v(n) = 3$, which was shown to satisfy $l(n) = \lambda(n) + 2$. The proof was simplified by Vegh [27]. Studies on $v(n) = 4$ was quite involved and initially, it was partially solved by Gioia *et al.* [21]. However, Knuth [15] completed the proof for which he showed that for some special n , $l(n) = \lambda(n) + 2$, otherwise $l(n) = \lambda(n) + 3$. Moreover, Gioia *et al.* [26] also showed that for all n such that $v(n) \geq 4$, $l(n) \geq \lambda + 3$. The following studies for $v(n) = 5$ are credited to Tsai and Chin [28], [29] which was proved to satisfy $l(n) \leq \lambda(n) + 4$. Additionally, Knuth [15] showed that $l(n) \geq \lambda(n) + 3$ for $v(n) \geq 5$. Further studies on $v(n) = 6, 7, 8$ were due to Bahig and Nakamura [30] for which they showed that $l(n) = \lambda(n) + 3$ and concluded that Scholz's conjecture is true for this class of integers.

There was an earlier study by Thurber [31] where he showed that $l(n) \geq \lambda(n) + 4$ for $v(n) \geq 8$. In the same paper, he extended the proof for $v(n) \geq 9$ for which $l(n) \geq \lambda(n) + 4$, which was subsequently also obtained in a slightly different way by Tsai and Chin [29]. Moreover, Thurber [31] extended the proof for 1's density of the form $v(n) \geq 2^{4m-1} + 1$ for which he proved that $l(n) \geq \lambda(n) + m + 3$. There were also other conjectures, one after Goulard [32] for which he stated that $l(2n) = l(n) + 1$ for all n . This conjecture was disproved with a counterexample by Knuth [15] for which he found that $l(191) = l(382)$. Theoretically, [22], [33], [34] proved that there exist infinite sequences of n with $l(2n) = l(n)$. Another one was $l(2n) \geq l(n)$ due to Knuth [15], which can be generalized to $l(mn) \geq l(n)$. This conjecture was earlier disproved by Knuth [15] for which he found that $l(3n) < l(n)$ for $n = 2731$. Thurber and Clift [35] found that $l(2n) < l(n)$ for $n = 30958077$ using his very own algorithm having the capacity to calculate an optimal chain for a range of numbers, especially of large set. This algorithm is faster than any existing algorithm in this working condition. Moreover, many recent works on addition chains were to find minimal chains for specific sequences [36], [37] and others by employing parallel computation for faster results [38].

Point negation on the elliptic curve imposes no extra cost. Due to this, a subtraction operation can be introduced to the sequence freely. This gives an additional means to shorten the generated chain. The following definition introduces a subtraction operation into the chain.

Definition 2.8. An addition subtraction chain for n is a sequence of positive integers of the form:

$$a_0 = \pm 1, a_1, \dots, a_r = n \quad (6)$$

where $a_\gamma = a_\beta \pm a_\alpha$ for which $\alpha \leq \beta < \gamma$ for all $\gamma = 1, 2, \dots, r$. Consider n to be a positive integer. The smallest r such that there exists a sequence of an addition subtraction chain for n is denoted as $l'(n)$. Schonhage [21] and Erdős [24] stated clearly that $l'(n) \leq l(n)$ and the boundary for $l(n)$ holds for $l'(n)$ too. A study dedicated to addition subtraction chain is rarely found except from Volger [39] for which he found, with some exceptions, the following inequalities for the boundary of $l'(n)$:

$$\log n + \log v'(n) - 2.13 \leq l'(n) \leq \left\lceil \log \frac{4}{3} n \right\rceil + v'(n) - 2 \quad (7)$$

where $v'(n) \leq 3$ is the non-zero density of the signed representation for n . We observed that the study on theoretical addition chain concentrates on the length, i.e., the number of terms. This is very much related to the length of its representation (e.g., binary and m -ary) and its hamming weight. These two factors can be varied based on the radix and non-zero density. Recently, we come across many new representations for integers such as that found in [40]-[49] which could be further scrutinized for a shorter addition chain.

3. ADDITION CHAIN METHOD

By definition, the heuristic method was designed to solve a complex problem much quicker by allowing marginal error in the result when exact methods are too slow to find the optimal solution. The idea is to tolerate optimality, completeness, accuracy, or precision with speed. In ECC, the addition chain method reads a recoded representation for n to compute the multiplication by a scalar, $Q = nP$. Many methods exist, but each method bears slight differences from others because each one has to be tailored to work with different representations of n . The efficiency of an addition chain method is measured by the number of addition and doubling operations executed during scalar multiplication, which here are denoted by ADD and DBL respectively. Noteworthy, for representation with radix other than 2, precomputation of coefficients is also needed and is denoted here by PRECOMP.

Consider a binary representation for an integer n of length r . The original binary method is designed to operate on an unsigned binary representation. Using this representation, we can have the method scan the input bit both from right to left [15] and left to right to left [50]. The expected running time for both is identical and can be approximated to $\frac{r}{2}ADD + rDBL$. The latter allows on-the-fly computation but with a wasted extra doubling at the end. While the former is suitable for any readily stored unsigned representation. In terms of memory consumption, left-to-right execution requires lesser memory storage than right-to-left. For a limited storage device, a left-to-right algorithm is preferable and the ability to execute scalar multiplication on the fly would be beneficial. These two methods are only suitable for unsigned binary representation. In case when a subtraction operation can be introduced into the chain, the binary method in general needs a little modification which results in a so-called addition subtraction method [51], [52]. This method can take an input having signed bits such as signed representation, non-adjacent form (NAF), and mutual opposite form (MOF), other than the original unsigned. By considering NAF input, the expected running time is near to $\frac{r}{3}ADD + rDBL$.

Nevertheless, things are a bit different with width- w window recording where all elements of the coefficient set other than 1 need to be precomputed [53]. Due to the need for precomputation, the total running time is divided into time to precompute the coefficients and the time taken to execute scalar multiplication. The maximum time required for precomputation is equal to $(2^{w-2})PRECOMP$. Meanwhile, the time needed for computing the chain is given by $\frac{r}{1+w}ADD + rDBL$. It can take inputs from w -NAF [53], w -LtoR [54] as well and an efficient on-the-fly version of scalar multiplication for w -MOF is available from Okeya *et al.* [55]. Further improving the window method, [56] introduced the cross-window method and its variants. The cross-window method with the addition sequence algorithm obtained a 9.5% reduction in the addition chain length, as compared to the window method.

The binary method allows only addition (subtraction) by P and multiplication by 2 to the current term. A shorter chain could be achieved by allowing addition and multiplication by a bigger integer. By allowing a wider range of coefficients c_i and the radix $m = 2^k$ for $k > 1$, the chain could be shortened significantly. The length of this new representation is given by $t = r/k$. Therefore, a smaller number of arithmetic operations are required. Namely, the m -ary method is meant to process m -ary representation. Among a few studies on this method are due to Bahig and Kotb [57], Gordon [58], Koç [59], and Knuth [15]. From the perspective of running time for the left-to-right m -ary method [60], the maximum number of executions required by this method is $(m-2)PRECOMP, \frac{m+1}{m}tADD$ and $t(\log_2 m)DBL$. Again, by introducing a subtraction operation into the chain, an addition subtraction m -ary method executing from left to right [61] is produced. This method takes the input of unsigned m -ary as well as signed m -ary [59] including general non-adjacent form (GNAF) [62]-[64] and generalized star form (GSF) [65]. Let the input be GNAF, the total running time required is devoted to $(m-2)PRECOMP, \frac{m-1}{m+1}tADD$ and $t(\log_2 m)DBL$. The more advanced concept of the ψ -ary addition subtraction method [50] is an efficient procedure that takes in reduced ψ NAF representation to compute scalar multiplication on the main subgroup of $E_u(\mathbb{F}_{2^m})$. By this method, the expected total running time is near to $\frac{m}{3}ADD$ with doubling operation is considerably countless as it is at a negligible amount of time.

4. DISCUSSION

We observed that many ideas, theorems, and experimentations have been brought forward for studying and solving the addition chain problem. The biggest difference between theoretical and experimental is the way they look into the problem by defining different objectives. The theoretical study looks into ways to reduce the number of terms in the addition chain sequence. By assuming that each term is equally weighted, we can freely choose any terms to eliminate by setting up different paths to n , at the same time still satisfying the basic condition of adding previous terms for generating the current term. In real life

this may not be the valid case, one term may have a bigger weightage than the other and thus choosing a particular term is more beneficial than the other. In experimentation, the defining parameter is not only the number of terms but also the time taken to execute the codes. In fact, time connects to the real world much better than the number of terms. We observed that methods such as NAF and MOF focus on minimizing the number of terms by introducing subtraction operation, while complementary recoding and others [66] dismissed the connection to the number of terms and is directly associated with time for execution. These methods mainly manipulate the representation of integers from the perspective of basis, operations allowed as well as its orientation. Different representations result in different addition chains as well as their lengths and thus result in different execution speeds. Future research may look into improving the theoretical boundary for specific families of numbers while on the practical side, some new algorithms can probably be designed to improve the speed of execution.

5. CONCLUSION

That addition chain problem is an NP problem and many heuristics methods have emerged throughout the years. Some methods are considerably better than others but in general, no one method makes the best output at all times for any n . After examining the topic, it is evident that existing methods are creative in their conceptual. We observed how researchers have exploited various corners of knowledge and theories to come out with their novel methods. This survey shows that their collective works have been shown to enjoy very fruitful ends. It should be able to assist researchers diving into this topic with speed and confidence helping them to grasp the fundamentals smoothly.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme FRGS/1/2018/ICT03/UNISZA/02/2 and the Center for Research Excellence and Incubation Management, Universiti Sultan Zainal Abidin.

REFERENCES




- [1] H. Altman, "Internal structure of addition chains: well-ordering," *Theoretical Computer Science*, vol. 721, pp. 54–69, Apr. 2018, doi: 10.1016/j.tcs.2017.12.002.
- [2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.
- [3] M. A. Mohamed, "A survey on elliptic curve cryptography," *Applied Mathematical Sciences*, vol. 8, pp. 7665–7691, 2014, doi: 10.12988/ams.2014.49752.
- [4] P. Downey, B. Leong, and R. Sethi, "Computing sequences with addition chains," *SIAM Journal on Computing*, vol. 10, no. 3, pp. 638–646, Aug. 1981, doi: 10.1137/0210047.
- [5] S. A. G. Sanchez, L. C. L. C. Osorno, and E. R. D. Camarillo, "Simulated annealing meta-heuristic for addition chain optimization," *European Journal of Electrical Engineering and Computer Science*, vol. 3, no. 6, Dec. 2019, doi: 10.24018/ejece.2019.3.6.159.
- [6] A. M. Noma, M. A. Mohamed, A. Muhammed, and Z. A. Zulkarnain, "An initial solution for addition chain optimization problem," *Journal of Engineering and Applied Sciences*, vol. 11, no. 3, pp. 640–643, 2016.
- [7] A. M. Noma, A. Muhammed, M. A. Mohamed, and Z. A. Zulkarnain, "A review on heuristics for addition chain problem: towards efficient public key cryptosystems," *Journal of Computer Science*, vol. 13, no. 8, pp. 275–289, Aug. 2017, doi: 10.3844/jcssp.2017.275.289.
- [8] A. M. Noma, A. Muhammed, Z. A. Zulkarnain, and M. A. Mohamed, "Iterative sliding window method for shorter number of operations in modular exponentiation and scalar multiplication," *Cogent Engineering*, vol. 4, no. 1, p. 1304499, Jan. 2017, doi: 10.1080/23311916.2017.1304499.
- [9] N. Cruz-Cortés, F. Rodríguez-Henríquez, R. Juárez-Morales, and C. A. Coello Coello, "Finding optimal addition chains using a genetic algorithm approach," in *Computational Intelligence and Security*, 2005, pp. 208–215, doi: 10.1007/11596448_30.
- [10] N. Nedjah and L. de Macedo Mourelle, "Minimal Addition chain for efficient modular exponentiation using genetic algorithms," in *Developments in Applied Artificial Intelligence*, 2002, pp. 88–98, doi: 10.1007/3-540-48035-8_10.
- [11] N. Nedjah and L. de Macedo Mourelle, "Towards minimal addition chains using ant colony optimisation," *Journal of Mathematical Modelling and Algorithms*, vol. 5, no. 4, pp. 525–543, Dec. 2006, doi: 10.1007/s10852-005-9024-z.
- [12] N. Nedjah and L. de Macedo Mourelle, "Finding minimal addition chains using ant colony," in *Intelligent Data Engineering and Automated Learning – IDEAL 2004*, 2004, pp. 642–647, doi: 10.1007/978-3-540-28651-6_94.
- [13] H. Zantema, "Minimizing sums of addition chains," *Journal of Algorithms*, vol. 12, no. 2, pp. 281–307, Jun. 1991, doi: 10.1016/0196-6774(91)90005-J.
- [14] A. C.-C. Yao, "On the evaluation of powers," *SIAM Journal on Computing*, vol. 5, no. 1, pp. 100–103, Mar. 1976, doi: 10.1137/0205008.
- [15] D. E. Knuth, *The art of computer programming. Vol 2. Seminumerical Algorithms*, 2nd ed. Pearson Education, Inc., 1981.
- [16] H. Dellac, "Question 49," *L'Intermédiaire Math*, vol. 1, p. 20, 1894.
- [17] W. Hansen, "Zum scholz-brauerschen problem," *Journal für die reine und angewandte Mathematik*, vol. 1959, no. 202, pp. 129–136, 1959, doi: 10.1515/crll.1959.202.129.
- [18] A. Brauer, "On addition chains," *Bulletin of the American Mathematical Society*, vol. 45, no. 10, pp. 736–739, 1939, doi:

- 10.1090/S0002-9904-1939-07068-7.
- [19] A. Scholz, "Aufgabe 252," *Jahresbericht. Deutschen Mathematiker-Vereinigung*, vol. 47, p. 41, 1937.
- [20] W. R. Utz, "A note on the scholz-brauer problem in addition chains," *Proceedings of the American Mathematical Society*, vol. 4, no. 3, pp. 462–463, 1953, doi: 10.1090/S0002-9939-1953-0054618-X.
- [21] A. Schönhage, "A lower bound for the length of addition chains," *Theoretical Computer Science*, vol. 1, no. 1, pp. 1–12, Jun. 1975, doi: 10.1016/0304-3975(75)90008-0.
- [22] E. G. Thurber, "On addition chains $l(mn) \leq l(n) - b$ and lower bounds for $c(r)$," *Duke Mathematical Journal*, vol. 40, no. 4, Dec. 1973, doi: 10.1215/S0012-7094-73-04085-4.
- [23] K. B. Stolarsky, "A lower bound for the scholz-brauer problem," *Canadian Journal of Mathematics*, vol. 21, pp. 675–683, Nov. 1969, doi: 10.4153/CJM-1969-077-x.
- [24] P. Erdos, "Remarks on number theory III. On addition chains," *Acta Arithmetica*, vol. 6, no. 1, pp. 77–81, 1960, doi: 10.4064/aa-6-1-77-81.
- [25] T. Agama, "On the scholz conjecture," *Cryptology ePrint Archive, Paper 2023/051*, Jun. 2023.
- [26] A. A. Gioia, M. V. Subbarao, and M. Sugunamma, "The Scholz-Brauer problem in addition chains," *Duke Mathematical Journal*, vol. 29, no. 3, Sep. 1962, doi: 10.1215/S0012-7094-62-02948-4.
- [27] E. Vegh, "A note on addition chains," *Journal of Combinatorial Theory, Series A*, vol. 19, no. 1, pp. 117–118, Jul. 1975, doi: 10.1016/0097-3165(75)90098-9.
- [28] Y. H. Tsai and Y. H. Chin, "On addition chains 1," *International Journal of Computer Mathematics*, vol. 45, no. 3–4, pp. 145–160, Jan. 1992, doi: 10.1080/00207169208804125.
- [29] Y. H. Tsai and Y. H. Chin, "A study of some addition chain problems," *International Journal of Computer Mathematics*, vol. 22, no. 2, pp. 117–134, Jan. 1987, doi: 10.1080/00207168708803586.
- [30] H. M. Bahig and K. Nakamura, "Some properties of nonstar steps in addition chains and new cases where the scholz conjecture is true," *Journal of Algorithms*, vol. 42, no. 2, pp. 304–316, Feb. 2002, doi: 10.1006/jagm.2002.1212.
- [31] E. Thurber, "The scholz-brauer problem on addition chains," *Pacific Journal of Mathematics*, vol. 49, no. 1, pp. 229–242, Nov. 1973, doi: 10.2140/pjm.1973.49.229.
- [32] A. Goulard, "Question 393," *L'Intermediaire Math*, vol. 1, p. 234, 1894.
- [33] A. TALL, "The scholz conjecture on addition chain is true for infinitely many integers with $l(2n) = l(n)$," *Cryptology ePrint Archive, Paper 2023/020*, 2023.
- [34] E. G. Thurber, "Addition chains and solutions of $l(2n) = l(n)$ and $l(2n - 1) = n + l(n) - 1$," *Discrete Mathematics*, vol. 16, no. 3, pp. 279–289, Nov. 1976, doi: 10.1016/0012-365X(76)90105-9.
- [35] E. G. Thurber and N. M. Clift, "Addition chains, vector chains, and efficient computation," *Discrete Mathematics*, vol. 344, no. 2, p. 112200, Feb. 2021, doi: 10.1016/j.disc.2020.112200.
- [36] P. A. Kameswari and B. Ravitheja, "Addition chain for Lucas sequences with fast computation method," *International Journal of Applied Engineering Research*, vol. 13, no. 11, pp. 9413–9419, 2018.
- [37] A. Flammenkamp, "Integers with a small number of minimal addition chains," *Discrete Mathematics*, vol. 205, no. 1–3, pp. 221–227, Jul. 1999, doi: 10.1016/S0012-365X(99)00103-X.
- [38] H. M. Bahig, "A fast optimal parallel algorithm for a short addition chain," *The Journal of Supercomputing*, vol. 74, no. 1, pp. 324–333, Jan. 2018, doi: 10.1007/s11227-017-2129-0.
- [39] H. Volger, "Some results on addition/subtraction chains," *Information Processing Letters*, vol. 20, no. 3, pp. 155–160, Apr. 1985, doi: 10.1016/0020-0190(85)90085-7.
- [40] S. Prugsapitak and N. Thongngam, "Representation of Integers of the form $x^2 + my^2 - z^2$," *Journal of Integer Sequences*, 2021.
- [41] J. Freixas and S. Kurz, "On minimum integer representations of weighted games," *Mathematical Social Sciences*, vol. 67, pp. 9–22, Jan. 2014, doi: 10.1016/j.mathsocsci.2013.10.005.
- [42] H. Park, B. Cho, D. Cho, Y. D. Cho, and J. Park, "Representation of Integers as sums of fibonacci and lucas numbers," *Symmetry*, vol. 12, no. 10, p. 1625, Oct. 2020, doi: 10.3390/sym12101625.
- [43] U. Isnaini, R. Melham, and P. C. Toh, "The number of representations of a positive integer by triangular, square and decagonal numbers," *Bulletin of the Korean Mathematical Society*, vol. 56, no. 5, pp. 1143–1157, 2019, doi: 10.4134/BKMS.b180914.
- [44] H. Arslan, A. Altoum, and M. Zaarour, "Integer representations of classical weyl groups," Nov. 2022, [Online]. Available: <http://arxiv.org/abs/2211.00427>
- [45] M. Wang and Z.-H. Sun, "On the number of representations of n as a linear combination of four triangular numbers," *International Journal of Number Theory*, vol. 12, no. 06, pp. 1641–1662, Sep. 2016, doi: 10.1142/S1793042116501001.
- [46] O. Trifonov and J. Dalton, "Representing positive integers as a sum of a squarefree number and a small prime," Jan. 2023, [Online]. Available: <http://arxiv.org/abs/2301.12585>
- [47] J. Bernal and C. Witzgall, "Integer representation of decimal numbers for exact computations," *Journal of Research of the National Institute of Standards and Technology*, vol. 111, no. 2, p. 79, Mar. 2006, doi: 10.6028/jres.111.006.
- [48] M. J. C. Lima and V. C. Rocha Júnior, "Adaptive universal codes for integer representation," *Journal of Communication and Information Systems*, vol. 28, no. 1, pp. 8–13, Apr. 2013, doi: 10.14209/jcis.2013.2.
- [49] M. Beck, E. Pine, W. Tarrant, and K. Y. Jensen, "New integer representations as the sum of three cubes," *Mathematics of Computation*, vol. 76, no. 259, pp. 1683–1691, Mar. 2007, doi: 10.1090/S0025-5718-07-01947-3.
- [50] H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates," in *Advances in Cryptology — ASIACRYPT 1998. ASIACRYPT 1998*, 1998, pp. 51–65, doi: 10.1007/3-540-49649-1_6.
- [51] M. Joye and Sung-Ming Yen, "Optimal left-to-right binary signed-digit recoding," *IEEE Transactions on Computers*, vol. 49, no. 7, pp. 740–748, Jul. 2000, doi: 10.1109/12.863044.
- [52] D. Moody and A. Tall, "On addition-subtraction chains of numbers with low Hamming weight," *Notes on Number Theory and Discrete Mathematics*, vol. 25, no. 2, pp. 155–168, Jul. 2019, doi: 10.7546/nntdm.2019.25.2.155-168.
- [53] J. A. Solinas, "Efficient arithmetic on koblitz curves," *Designs, Codes, and Cryptography*, vol. 19, no. 2–3, pp. 195–249, 2000, doi: 10.1023/A:1008306223194.
- [54] R. M. Avanzi, "A note on the signed sliding window integer recoding and a left-to-right analogue," in *Selected Areas in Cryptography. SAC 2004*, 2004, pp. 130–143, doi: 10.1007/978-3-540-30564-4_9.
- [55] K. Okeya, K. Schmidt-Samoa, C. Spahn, and T. Takagi, "Signed binary representations revisited," in *Advances in Cryptology — CRYPTO 2004*, 2004, pp. 123–139, doi: 10.1007/978-3-540-28628-8_8.
- [56] Y. Ding, H. Guo, Y. Guan, H. Song, X. Zhang, and J. Liu, "Some new methods to generate short addition chains," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 270–285, Mar. 2023, doi: 10.46586/tches.v2023.i2.270-285.
- [57] H. Bahig and Y. Kotb, "An efficient multicore algorithm for minimal length addition chains," *Computers*, vol. 8, no. 1, p. 23,




- Mar. 2019, doi: 10.3390/computers8010023.
- [58] D. M. Gordon, "A survey of fast exponentiation methods," *Journal of Algorithms*, vol. 27, no. 1, pp. 129–146, Apr. 1998, doi: 10.1006/jagm.1997.0913.
- [59] Ç. K. Koç, "High-radix and bit recoding techniques for modular exponentiation," *International Journal of Computer Mathematics*, vol. 40, no. 3–4, pp. 139–156, Jan. 1991, doi: 10.1080/00207169108804009.
- [60] C. K. Koç, "Analysis of sliding window techniques for exponentiation," *Computers & Mathematics with Applications*, vol. 30, no. 10, pp. 17–24, Nov. 1995, doi: 10.1016/0898-1221(95)00153-P.
- [61] Ö. Eğecioglu and Ç. K. Koç, "Exponentiation using canonical recoding," *Theoretical Computer Science*, vol. 129, no. 2, pp. 407–417, Jul. 1994, doi: 10.1016/0304-3975(94)90037-X.
- [62] W. Clark and J. Liang, "On arithmetic weight for a general radix representation of integers (Corresp.)," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 823–826, Nov. 1973, doi: 10.1109/TIT.1973.1055100.
- [63] Huapeng Wu and M. A. Hasan, "Closed-form expression for the average weight of signed-digit representations," *IEEE Transactions on Computers*, vol. 48, no. 8, pp. 848–851, 1999, doi: 10.1109/12.795126.
- [64] Fanyu Kong, Jia Yu, Zhun Cai, and Daxing Li, "Left-to-right Generalized non-adjacent form recoding for elliptic curve cryptosystems," in *2006 International Conference on Hybrid Information Technology*, IEEE, Nov. 2006, pp. 299–303, doi: 10.1109/ICHIT.2006.253503.
- [65] M. Joye and S.-M. Yen, "New minimal modified radix-r representation with applications to smart cards," in *Public Key Cryptography. PKC 2002*, 2002, pp. 375–383, doi: 10.1007/3-540-45664-3_27.
- [66] P. Balasubramaniam and E. Karthikeyan, "Elliptic curve scalar multiplication algorithm using complementary recoding," *Applied Mathematics and Computation*, vol. 190, no. 1, pp. 51–56, Jul. 2007, doi: 10.1016/j.amc.2007.01.015.

BIOGRAPHIES OF AUTHORS






Mohamad Afendee Mohamed    received his Ph.D. in Mathematical Cryptography from Universiti Putra Malaysia in 2011. Upon completion, he served the university for three years as a senior lecturer. In 2014, he moved to Universiti Sultan Zainal Abidin and later assumed an associate professor position. His current research interests include both theoretical and application issues in the domain of data security and mobile and wireless networking. He has authored more than 100 articles that have appeared in various journals, book chapters, and conference proceedings. He can be contacted at email: mafendee@unisza.edu.my.






Yahaya Garba Shawai    is a staff of the National Open University of Nigeria. He is a Doctoral Researcher at The Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia. He obtained his masters in the field of e-learning and mobile learning, in which he published more than 7 research papers in some reputable journals such as Theoretical and Applied Information Technology, and international journal articles. Most of the journals were Scopus-based. His research interest for his Ph.D. program was cryptography-based chaotic systems in conjunction with differential equations. He can be contacted at email: yshawai@noun.edu.ng.






Mohd Noor Derahman    is a lecturer at the Department of Communication Technology and Network, Faculty of Computer Science, and Information Technology, Universiti Putra Malaysia. His research interests include software-defined networking and resource optimization. He can be contacted at email: mnoord@upm.edu.my.






Abd Rasid Mamat    received a Ph.D. in Computer Science from Universiti Sultan Zainal Abidin in 2022, where he currently serves as a Senior Lecturer. His main research areas include image processing, content-based image retrieval, and decision support systems. arm@unisza.edu.my.






Siti Dhalila Mohd Satar    received her M.Sc. degree from Universiti Teknologi Malaysia in 2012. She is a Lecturer at Universiti Sultan Zainal Abidin and her research interests are access control security systems, security services (including digital forensics, steganography, network security, and biometrics), and data security. Currently, she is pursuing her Ph.D. study at Universiti Putra Malaysia, Malaysia. sitidhalila@unisza.edu.my.



Ahmad Faisal Amri Abidin    is a Senior Lecturer of Computer Science at Universiti Sultan Zainal Abidin. His research interests are secure protocols, trust computing, and trust in social networks. He has worked extensively on trust in generic social networks, which he leveraged and integrated the sixth degree of separation theory to gain trust. He maintains interests in various aspects of hacking and security countermeasures including confidentiality, integrity, and availability of data and information systems. Currently, he directs the Computer Security and Networking Lab and is affiliated with the Facilities and Technical Management of the Faculty of Informatics and Computing. He can be contacted at email: faisalamri@unisza.edu.my.



Mohd Fadzil Abdul Kadir    received a Ph.D. in engineering (system engineering) from the Mie University, Mie, Japan, in 2012. Since 2006, he has been with the Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, where he is currently a Senior Lecturer. His main areas of research interest are digital image processing, pattern recognition, information security, and cryptography. He is also a member of the Malaysia Board of Technologists. He can be contacted at email: fadzil@unisza.edu.my.