ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Shorter Addition-Subtraction Chain With Signed Composition Method

MAMohamed[1], A Ahmad[2], R R Mohamed[3], MRM Said[4]
[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, 22200, Malaysia
[1]mafendee@unisza.edu.my
[2]Department of Computer Science, National Defence University of Malaysia, Sungai Besi, 57000, Malaysia
[3]Department of System and Networking, Universiti Tenaga Nasional, Kajang, 43000, Malaysia
[4]Institute of Mathematical Research, Universiti Putra Malaysia, Serdang, 43400, Malaysia

***Abstract*—Addition chain is considered as the solution to large number operation of scalar multiplication in elliptic curve cryptosystem. Recently, a decomposition method was introduced as a new technique to generate addition chain with minimal possible terms. The method which is based on prime power input form was shown to outclass previous methods under certain condition. An earlier study shows that this method can also be used with non-prime integer such that found in composition method. As a result of no extra cost for point negation on elliptic curve, subtraction operation can be included during the generation of the chain as we found in signed decomposition method. As an alternative, in this paper, we proposed a signed composition method. Using this method, we study the properties of the chain against those generated by prime power equivalent. The comparative result between signed composition method against signed decomposition method shows that by allowing a subtraction information into the chain, the resulting chains are nearly of equal length which is very different from the unsigned case, where original decomposition method is by far has outperformed the composition method.**

Keywords-addition chain, binary method, double and add, non-adjacent form, complementary recoding

I. INTRODUCTION

The term addition chain refers to the sequence of integers $1 = a_0, a_1, \ldots, n$ starting from 1 and ending with n where only addition and doubling operations of two previous terms are allowed. The idea has been widely used to improved efficiency of huge number operation such that found in modern public key cryptography [1, 2]. The advent of elliptic curve cryptography (ECC) which allows negation of a point oncurve at no extra cost triggered the need to include subtraction operation during the construction of the so-called addition-subtraction chain. However, the problem of finding the optimal chain (or optimal sequence to be more precise) is unsolvable in areasonable time [3]. Therefore, many heuristic methods [4, 5, 6, 7] and metaheuristics [8, 9] methods were introduced, and each method works well only on some occasion.

Recently, a new method called decomposition method (DM) [10] was introduced as another partial solution to the infamous addition chain problem. This method takes an input of a prime factor in the form of rules as an alternative representation for numbers. The method was shown to perform better than previous methods under certain condition. Shortly after, the same author also developed a method taking theinput of composite form namely the composition method (CM) [11] which takes an integer input in the form of rules. However, these two methods were targeting unsigned binary input, that is to improve the addition chain. For a signed binary input or to improve addition subtraction chain, a signed decomposition method (SDM) [12], as an advancement to DM was also introduced. This method seems to outperformed previous methods for some selected inputs.

In this paper, we introduce a signed composition method (SCM). It mains objectives is to continue the work of composition method, that is to address the problem of addition-subtraction chain by allowing subtraction operation. SCM is compared mainly against SDM. For a given number range, the frequency of optimality is studied. We also study the properties of optimality as the number grows bigger. This paper is organized such a way that, Section 2 is dedicated to the introduction of the two different inputs forms. Section 3 shows the development of the idea of SCM. Section 4 suggests the algorithm for this new technique. Section 5 presents the analysis of the chain generated by SCM. Section 6 layouts the result to support our claim made earlier. Section 7 concludes the finding of this work.

II. INTEGER AND PRIME FACTOR

For each composite *n*, there exists an equivalent prime factor of the form $p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Decomposition method was originally designed for prime factor input form. Later it was shown that in some situation composite input produces shorter chain than prime input.

Unlike previous methods which take number as an input, for the purposes of better efficiency, ruleis taken as an input to this method. For every rule, there is a unique n and vice-versa [10].

[13] studied the properties of *n* in a collection of number range given by $2^m + 1 \leq n \leq 2^{m+1}$. For this reason, we assume a thorough consideration is necessary to examine every *n* in this form. For each number range, we determine the frequency of minimality as well as the average length of addition chains for SCM over other previous techniques.

III. SIGNED COMPOSITION METHOD

Signed Composition Method, an improved version of CM is introduced as a consequence of bringing in a subtraction operation to elliptic curve point operation at no extra cost. The idea is to reduce the number of addition operations. The development of SCM from CM can also be seen as comparable to the development of NAF from BM. Although in this case, rule is used instead of number.

SCM inherited most of its properties from SDM by considering n of SCM as a single *p* at prime layer of SDM. SCM generates an addition-subtraction chain similar to that of SDM [11]. The doubling, addition and subtraction operations satisfy the same set of conditions as that found in [11, 9]. The idea of closest value in determining the coming term in the chain is also applicable [11]. These conditions determine the permitted components within the generated rule. A proper definition for a signed rule was given for a prime *p* as in SDM. This definition can also be generalized for any integer *n*.

Definition 3.1. Let $n \in \mathbb{Z}$. A signed rule for any integer *n* is defined as a sequence of *dbl*'s followed by *add/sub*'s of the form

rule(n) = $dbl(a_0)$, $dbl(a_1)$, . . . , $dbl(a_{i-1})$, $add/sub(a_i, a_{j1})$, $add/sub(a_{i+1}, a_{j2})$, . . . , $add/sub(a_{r-1}, a_{jm})$

where

(1) $a_0, a_1 = dbl(a_0), a_2 = dbl(a_1), \dots, a_r = add/sub(a_{r-1}, a_{jm})$ is the respective addition chain for which

$0 \leqslant j_m < \dots < j_2 < j_1 \leqslant i - 1$,

(2) $a_{jk} > 0$ for all k such that $1 \leqslant k \leqslant m$.

Similar to CM, the property of uniqueness for SCM rule can easily be deduced from SDM rule [11].

Theorem 3.2. An addition subtraction chain $a_0, a_1, \dots, a_r$ for an integer *n* can be computed from a given signed rule and each rule is unique to each *n*.

Proof. As a result of generalization p to n from SDM [11].

This section unveils the necessary conditions for SCM, which are mostly related to SDM. SCM rule should be generated with some preset conditions similar to that of SDM. In so doing, the addition chain to be generated is maintained at the minimal length.

Note that, for simplicity, the term addition chain will be used as a generic term for both decomposition based method and composition based method, for unsigned and signed rules, although it should be understood that addition chain refers to anunsigned method and addition subtraction chain refers to signed method.

IV. ALGORITHM DEVELOPMENT

In this section, computer programs will be developed to simulate both CM/SCM and DM/SDM, where each one should work for two different input types. Fortunately, SCM can easily be coded by adding a small variation into CM. Even better, the code for CM/SCM can be in the same program because the additional part added for SCM will not be used for theunsigned rule. In other words, the input type decides on the method in used, and so are for the case of DM and SDM.

Algorithm 4.1. CM and *SCM.

A1. INPUT: rule(n)

A2. SET val[0] = 1

A3. for i from 0 to #(dbl + add) − 1 step-up by 1

A4. if rule[i] = dbl

A5. a_i+1 = 2.val[i][0]

A6. else if rule[i] = add

A7. a_i+1 = val[i] + val[j]

A8*. else if rule[i] = *sub*

A9*. a_{i+1} = val[i] − val[j]

A10. val[i + 1] = a_{i+1}

A11.OUTPUT: $a_0, a_1, \ldots, a_r = n$

Algorithm 4.1 is designed to simulate composition based methods taking unsigned and signed inputs. Those lines with (*) are specially dedicated to SCM for signed rules. If unsigned input rule is used, the sub operation will be ignored. The output is a complete chain for CM or SCM. The length of an addition chain can therefore be determined. Observe that, the number of times the loop gets executed is equal to f = #(*dbl* + *add*) which is exactly the length of an addition chain.

Algorithm 4.2. DM and *SDM.

A1. INPUT: rule($p_1, p_2, \ldots, p_s$), $e_1, e_2, \ldots, e_s$

A2. SET val[0] = a_0

A3. SET v = 0

A4. for l from 0 to s − 1 step-up by 1

A5. for k from 0 to e_i − 1 step-up by 1

A6. for i from 0 to #(*dbl* + *add*)$_i$ − 1 step-up by 1

A7. if rule[i] = *dbl*

A8. a_v+kc_i+i+1 = 2.val[i]

A9. else if rule[i] = *add*

A10. a_v+kc_i+i+1 = val[i] + val[j]

A11*. else if rule[i] = *sub*

A12*. a_v+kc_i+i+1 = val[i] − val[j]

A13. val[i + 1] = a_v+kc_i+i+1

A14. val[0] = val[i + 1]

A15. v = a_v+kc_i+i+1

A16.OUTPUT: $a_0, a_1, \ldots, a_r = n$

Meanwhile, Algorithm 4.2 takes primes rule($p_1, p_2, \ldots, p_s$) both unsigned and signed. Those lines with(*) are rightfully dedicated to SDM. There will be one rule assigned for each prime, p_i for $1 \leqslant i \leqslant s$. This rule is executed e_i number of times. For each i, let c_i = #(*dbl* + *add*)$_i$ be the number of doubling and addition operations for p_i. The output is the complete chain for DM or SDM. The length of this chain can therefore be determined. The code seems a bit more complicated with 3 nested loops but the complexity is approximated to #(*dbl* + *add*)$_i$.e_i.s which is again in the similar magnitude as that of f.

V. ANALYSIS

In this section, some properties on the boundary related to CM and SCM will be studied. This can be considered as a continuation to the studies of DM [9] and SDM [11]. In some cases, theorems related to DM can easily be generalized to CM by means of substituting n for p. At times, n is considered as in the same layer as p, although in this case there is only one layer available. For all n, it is obvious that $l_{CM}(n) \geqslant l(n)$ where $l_{CM}(n)$ denotes the length of an addition chain generated by CM.

Lemma 5.1. Given an integer n, $m + 1 \leqslant l_{CM}(n) \leqslant 2m$ for $2^m + 1 \leqslant n \leqslant 2^{m+1}$.

Proof. Since $n > 2^m$, let $n = 2^m + 2^r$ be the simplest form of n. It is known that $l_{CM}(2^m) = m$ since the shortest path is achieved through m doublings. Therefore, for $l_{CM}(2^m + 2^r)$ only one other step is needed,so that $l_{CM}(n) = m + 1$. In case $r = 0$, one small step is needed. Equally, if $r = m$ one-star step is needed. Here it is clear that CM is optimal when n has at most two non-zeros. For the worst case scenario, consider n to be any integer within the range. Again CM executes m number of doublings which generate m number of terms excluding a_0. Addition operations follow through and in the worst case all terms $a_{m-1}, a_{m-2}, \ldots, a_0$ are consumed giving another m number of operations. Hence $m + 1 \leqslant l_{CM}(n) \leqslant 2m$.

Lemma 5.1 shows that $l_{CM}(n)$ and $l_{DM}(n)$ are devoted to the same boundaries. Similarly, for SCM, a result from SDM studied earlier can be used to study $l_{SCM}(n)$. [5] stated for every integer n, the optimal length of an addition-subtraction chain is always shorter if not equal to the optimal length of an addition chain such that $l^-(n) \leqslant l(n)$. Let $l_{SCM}(n)$denotes the length of an addition subtraction chain generated by SCM. As a consequence, the following assertion is made true.

Lemma 5.2. Let n be an integer, $l_{SCM}(n) \leqslant l_{CM}(n)$.

Proof. The proof is deducible from [5].

The relationship of the four different chains follows these inequalities $l^{-}(n) \leqslant l(n)$and $l_{SCM}(n) \leqslant l_{CM}(n)$.It is not necessary that $l_{SCM}(n) \leqslant l(n)$ (or otherwise) always be the case for all n.The boundary for methods developed so far has been equivalent to that of an optimal chain. The following section investigates into individual chain basis in determining the strength of each methods among themselves.

VI. RESULTS

Initially, [10] studied the property of an optimal chain $l(n)$for every n such that $2^m + 1 \leqslant n \leqslant 2^{m+1}$in relations to m. The studies comprise the analysis on the lower bound and upper bound of $l(n)$. With regardto his works, this section studies the properties of $l_{CM}(n)$and $l_{DM}(n)$, ($l_{SCM}(n)$and $l_{SDM}(n)$respectively) and the relations amongst them in asimilar fashion. By looking at the output, the scope and the outcomesof the studies can be divided into four tasks:

1. $l_{DM}(n)$against $l_{CM}(n)$; to determine which method outperforms the other, DM or CM.
2. $l_{SCM}(n)$against $l_{CM}(n)$; to determine the degree of improvement of SCM over CM.
3. $l_{SDM}(n)$against $l_{DM}(n)$; to determine the degree of improvement of SDM over DM.
4. $l_{SDM}(n)$ against $l_{SCM}(n)$; to determine which method surpasses the other, SDM or SCM.

Before going further, the following notations are required; $A_{DM}(n)$ and $A_{CM}(n)$ denotes an addition chain for n generated by DM and CM respectively, whereas $A_{SDM}(n)$ and $A_{SCM}(n)$ denotes an addition-subtraction chain for n generated by SDM and SCM respectively.

Based on the theoretical findings from previous studies as well as earlier discussion of this article, this section discusses the empirical studies on all (de)composition methods studied so far. For this purpose, two parameters are to be defined and their values are calculated based on the length of generated addition chains. Parameters are evaluated based on every m. Each m represents a set of data concerning the length of addition chains for all n such that $2^m + 1 \leqslant n \leqslant 2^{m+1}$. For every task listed, a favorable method is decided based on the measurement of the two parameters.

1. *Minimal chain*, $\mathcal{M}$. For a particular m, thecomparison will be made on the length of the two addition chains of the same n, the shorter chain will be taken into account. The method which produces more minimal chain is considered a preferable method for this particular range. Moreover, from the value of minimal chain, an ancillary graph is plotted to measure the percentage of betterment, ξ between them (for task (1) and task (4)) or percentage of improvement, ζ over their predecessor (for task (2) and task (3)). This value will be of some help in predicting the behavior of this relationship for $m > 25$.
2. *Average length*, $\mathcal{A}$. For a particular m, the length of all addition chains for each n, for each of the two methods are added together and divided by the number of chains. The method with smaller average length is considered as a preferable method. From the value of these average lengths, an ancillary graph is plotted to measure the percentage of betterment, ξ between them (for task (1) and task (4)) or percentage of improvement, ζ over their predecessor (for task (2) and task (3). This value will also assist in predicting the behaviour for $m > 25$.

The number range to be used for the purpose of data collection, defined by m is limited to $1 \leqslant m < 25$. This is due to the restriction imposed on computational resource including processing power and memory storage. The followings are results obtained for studies suggested earlier.

A. DM versus CM

In this subsection, DM is investigated against CM to determine which method is better than the other in relation to$m$. The first result is the counted number of minimal chain generated by each method. For a particular m, $l_{CM}(n)$and $l_{DM}(n)$are calculated for all n. Each pair is evaluated and the one with shorter chain is taken into account. For any m, we define

$$\begin{aligned} \mathcal{M}_{DM} &= \{A_{DM}(n) \mid l_{DM}(n) < l_{CM}(n)\} \\ \mathcal{M}_{CM} &= \{A_{CM}(n) \mid l_{CM}(n) < l_{DM}(n)\} \\ \mathcal{M}_{DRW} &= \{A_{DM}(n) = A_{CM}(n) \mid l_{DM}(n) = l_{CM}(n)\} \end{aligned} \quad (1)$$

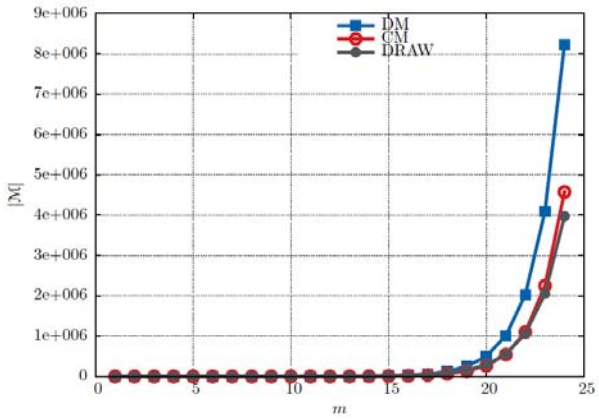

Figure 1: Number of minimal chains.

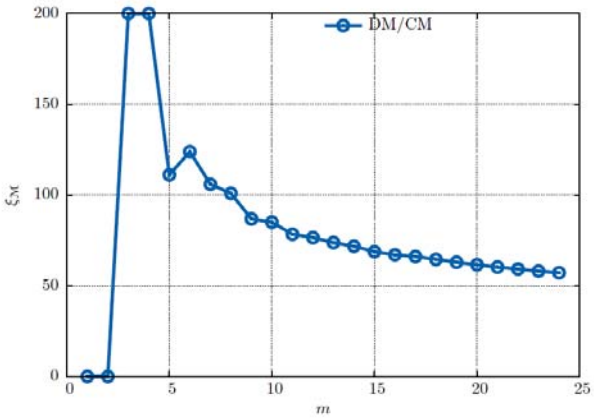

Figure 2: Percentage of betterment.

From Figure 1, observe that even from the beginning DM has begun to overtake CM such that $|\mathcal{M}_{\mathrm{DM}}|>|\mathcal{M}_{\mathrm{CM}}|$. This trend seems to be continuing for $m> 25$.

The second result is the calculated percentage of betterment, $\xi_{\mathcal{M}}$ between DM and CM obtained in terms of Equation 1. The calculation is achieved by the formula

$$\xi_{\mathcal{M}} = \frac{|\mathcal{M}_{\mathrm{DM}}|-|\mathcal{M}_{\mathrm{CM}}|}{(|\mathcal{M}_{\mathrm{DM}}|+|\mathcal{M}_{\mathrm{CM}}|)/2} * 100 \quad (2)$$

Note that the value of $\xi_{\mathcal{M}}$ can be positive as well as negative. A positive value shows that DM is better than CM while anegative value shows that CM is better than DM for that particular m.From Figure 2, $\xi_{\mathcal{M}}$ starts out at 200 percent and is flattening towards 50 percent as m grows larger. Most likely its value will stay above 0 percent for $m>> 25$, meaning $|\mathcal{M}_{\mathrm{DM}}|>|\mathcal{M}_{\mathrm{CM}}|$. In this case, DM is likely to remain as a preferable method. One interesting fact would be when the ratio is 0, meaning for this particular m, they are equally competitive in which they produce the same number of shorter chains than the other.

The third result is calculated for the average length of addition chains for integers in the same number range. For every m, the calculation with respect to DM and CM follows the formulae

$$\mathcal{A}_{DM} = \sum_{n=2^m+1}^{2^{m+1}} l_{DM}(n)/2^m$$
$$\mathcal{A}_{CM} = \sum_{n=2^m+1}^{2^{m+1}} l_{CM}(n)/2^m \quad (3)$$

Figure 3 shows that ACM is slightly bigger than ADM and the two plots seem to be increasingly separated as m grows.

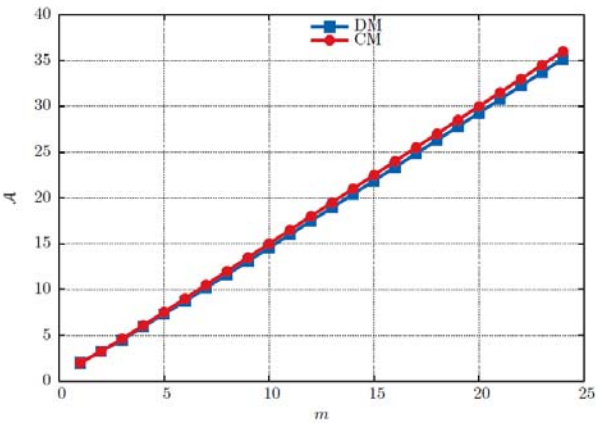

Figure 3: Average length of addition chains.

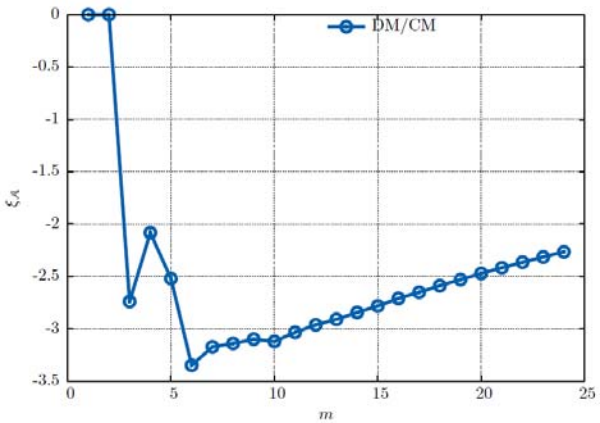

Figure 4: Percentage of betterment.

The fourth result is calculated for the percentage of betterment, $\xi_{\mathcal{A}}$ between the two methods, derived from the result in Equation 3. This value can be formulated as

$$\xi_{\mathcal{A}} = \frac{\mathcal{A}_{DM} - \mathcal{A}_{CM}}{(\mathcal{A}_{DM} + \mathcal{A}_{CM})/2} * 100 \qquad (4)$$

Note that the value of $\xi_{\mathcal{A}}$ can be positive as well as negative. Positive value shows that CM is better than DM while negative value shows that DM is better than CM for that particular m, both for having shorter average length. From Figure 4, it can be seen that $\xi_{\mathcal{A}}$ whose value not exceeding -5 percent is slowly increasing as m gets large. The plot shows that, DM is by far a better method than CM. Clearly, both part of tests agrees that DM is a preferable method for m< 25 and this trend shall remain for some larger m.

B. SCM versus CM

In this subsection, an improved method SCM is to be modeled against its predecessor CM. The objective is to find out how significant can the improvement be. As one might have known, SCM it at worst at par with CM.Theoretical studies show that $l_{SCM}(n) \leq l_{CM}(n)$, for all n. We define

$$\begin{aligned} \mathcal{M}_{CM} &= \{A_{CM}(n) \mid l_{CM}(n) < l_{SCM}(n)\} \\ \mathcal{M}_{SCM} &= \{A_{SCM}(n) \mid l_{SCM}(n) < l_{CM}(n)\} \\ \mathcal{M}_{DRW} &= \{A_{SCM}(n) = A_{CM}(n) \mid l_{SCM}(n) = l_{CM}(n)\} \end{aligned} \qquad (5)$$

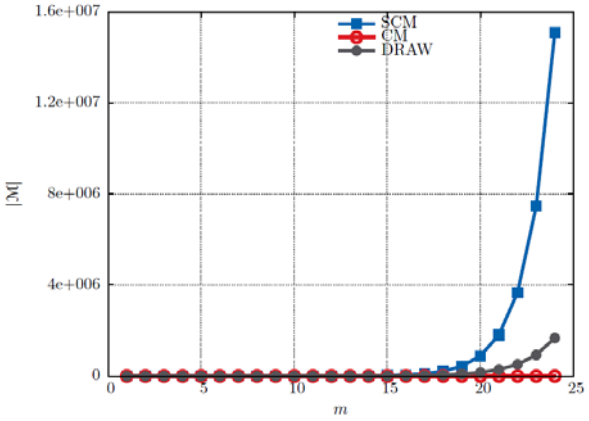

Figure 5: Number of improved chains.

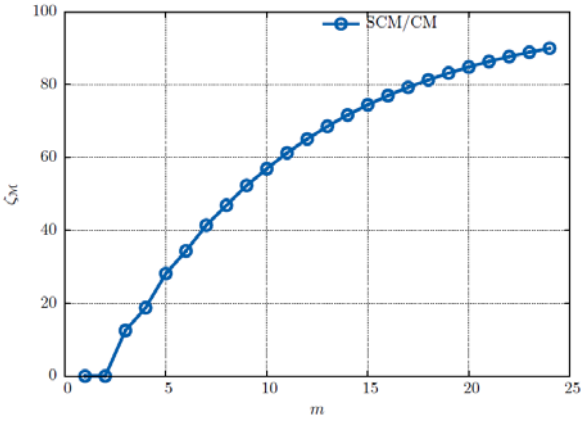

Figure 6: Percentage of improvement.

In this experiment, for each m, every $l_{SCM}(n)$is compared against $l_{CM}(n)$. Affirmatively, Figure 5 shows that $l_{SCM}(n) \leq l_{CM}(n)$for all cases of n. There exists no $A_{CM}(n)$ such that $l_{SCM}(n) > l_{CM}(n)$, as expected $\mathcal{M}_{CM} = \emptyset$.

The percentage of improvement, $\zeta_{\mathcal{M}}$ of SCM over CM can be calculated from Equation 5 using the formula

$$\zeta_{\mathcal{M}} = \frac{|\mathcal{M}_{SCM}|}{|\mathcal{M}_{SCM}| + |\mathcal{M}_{CM}| + \mathcal{M}_{DRW}} * 100 \qquad (6)$$

From Figure 6, $\zeta_{\mathcal{M}}$starts out at 0 percent and steadily curving towards 100 percent as m grows, although this value might not be achievable. Nevertheless, this tells that SCM will be much useful as m gets bigger.

For a particular m, the average length of addition chains for SCM and CM can be calculated respectively from the formulae

$$\begin{aligned} \mathcal{A}_{SCM} &= \sum_{n=2^m+1}^{2^{m+1}} l_{SCM}(n)/2^m \\ \mathcal{A}_{CM} &= \sum_{n=2^m+1}^{2^{m+1}} l_{CM}(n)/2^m \end{aligned} \qquad (7)$$

Figure 7 shows that $\mathcal{A}_{SCM}$ is always smaller than that of $\mathcal{A}_{CM}$. Moreover, the difference in the average length between the two increases with m as can be seen from the distance between the two. To see the percentage of improvement, $\zeta_{\mathcal{A}}$ another graph is plotted based on the formula

$$\zeta_{\mathcal{A}} = \frac{\mathcal{A}_{CM} - \mathcal{A}_{SCM}}{(\mathcal{A}_{CM} + \mathcal{A}_{SCM})/2} * 100 \qquad (8)$$

Note that the value of $\zeta_{\mathcal{A}}$ can be positive as well as negative.Positive value means that SCM hasimproved CM while negative value means that SCM has weakened CM for that particular m.

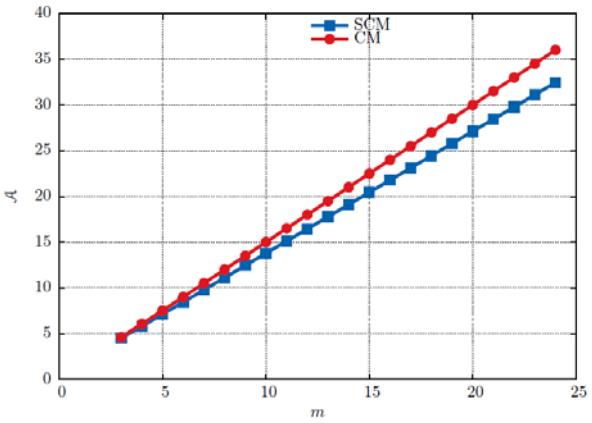

Figure 7: Average length of addition chains.

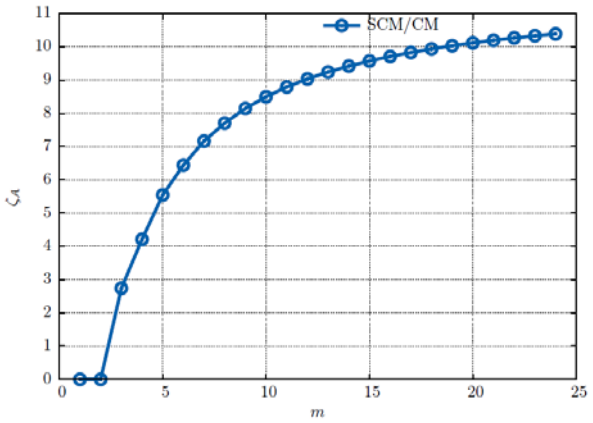

Figure 8: Percentage of improvement.

Figure 8 shows that $\zeta_{\mathcal{A}}$ is well over 10 percent as m gets larger. For m>> 25, the separation between the two plots is predicted to be more distant apart. Therefore, $\zeta_{\mathcal{A}}$ shall increase too.The first part of the results shows that the number of improved chain increases with m, whereas the second part shows that as the number of improved chains increases, the average chain is reaching 10 percent.

C. SDM versus DM

In this subsection, an investigation is carried out to determine the level of improvement introduced by SDM over DM. Earlier studies proved that $l_{SDM}(n) \leq l_{DM}(n)$, for all n on every m. We define

$$\begin{aligned} \mathcal{M}_{DM} &= \{A_{DM}(n) \mid l_{DM}(n) < l_{SDM}(n)\} \\ \mathcal{M}_{SDM} &= \{A_{SDM}(n) \mid l_{SDM}(n) < l_{DM}(n)\} \\ \mathcal{M}_{DRW} &= \{A_{SDM}(n) = A_{DM}(n) \mid l_{SDM}(n) = l_{DM}(n)\} \end{aligned} \quad (9)$$

The experiment compares $l_{SDM}(n)$to $l_{DM}(n)$. From Figure 9, the result shows that $l_{SDM}(n) \leq l_{DM}(n)$for all n. SDM is seen to be increasing with m. As anticipated, the plot labeled DM is always zero suchthat $\mathcal{M}_{DM} = \emptyset$.In terms of Equation 9 the percentage of improvement, $\zeta_{\mathcal{M}}$ introduced by SDM over DM is given by the formula

$$\zeta_{\mathcal{M}} = \frac{|\mathcal{M}_{SDM}|}{|\mathcal{M}_{SDM}| + |\mathcal{M}_{DM}| + \mathcal{M}_{DRW}} * 100 \quad (10)$$

Figure 10 shows that the number of improved chains is proportional to m. This value seems to be increasing towards 90 percent. SDM becomes more efficient a method as m gets large.For a particular m, the average length of addition chains within the same number range can be obtained respectively for SDM and DM from the formulae

$$\mathcal{A}_{SDM} = \sum_{n=2^m+1}^{2^{m+1}} l_{SDM}(n)/2^m$$

$$\mathcal{A}_{DM} = \sum_{n=2^m+1}^{2^{m+1}} l_{DM}(n)/2^m \quad (11)$$

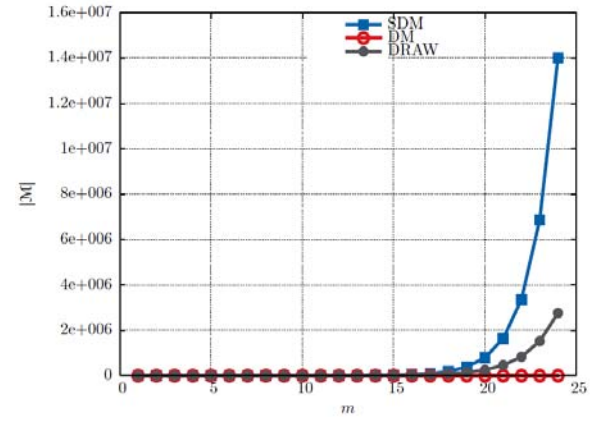

Figure 9: Number of improved chains.

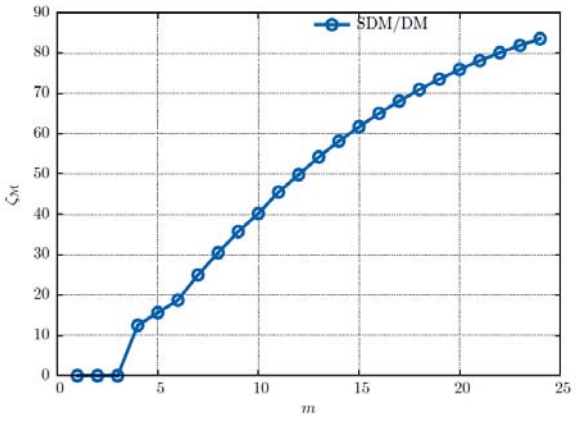

Figure 10: Percentage of improvement.

Figure 11 shows that $\mathcal{A}_{SDM}$ is always smaller than $\mathcal{A}_{DM}$. Moreover, the difference in the length between the two significantly increases with m as can be seen from the distance between the two.The percentage of improvement, $\zeta_{\mathcal{A}}$ calculated based on Equation 11 can be formulated as

$$\zeta_{\mathcal{A}} = \frac{\mathcal{A}_{DM} - \mathcal{A}_{SDM}}{(\mathcal{A}_{DM} + \mathcal{A}_{SDM})/2} * 100 \qquad (12)$$

Note that the value of $\zeta_{\mathcal{A}}$ can be positive as well as negative. Positive value means that SDM is an improvement on DM while negative value means that SDM has not improved DM for that particular m.Figure 12 shows that $\zeta_{\mathcal{A}}$ is just over 8 percent as m gets larger. For m>> 25, the separation between the two plots is predicted to be even more distant apart. Therefore, $\zeta_{\mathcal{A}}$ shall increase too.

The first part of the experiment shows that more percentage of chains get improved as m goes larger. The second part of experiment confirms that the number of chains improved contributes to some 8 percent of decrease in average length.

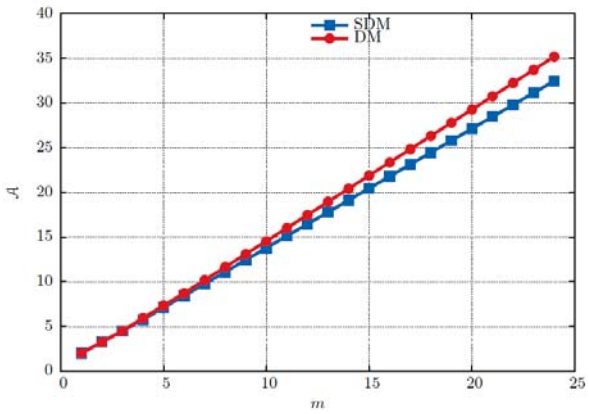

Figure 11: Average length of addition chains.

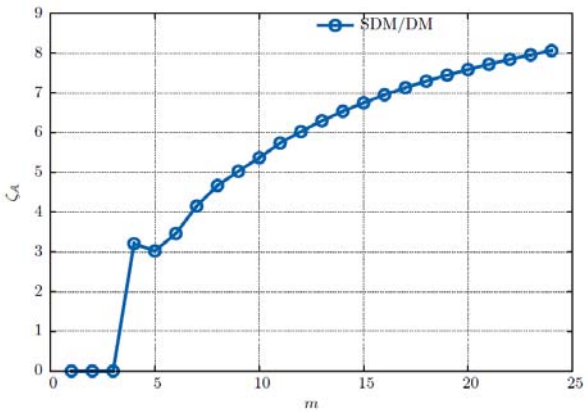

Figure 12: Percentage of improvement.

D. SDM versus SCM

In this subsection, a comparison between SDM and SCM is lookedat. The objective is to find out which method is better than the other in relation to$m$. We define

$$\mathcal{M}_{SDM} = \{A_{SDM}(n) \mid l_{SDM}(n) < l_{SCM}(n)\}$$
$$\mathcal{M}_{SCM} = \{A_{SCM}(n) \mid l_{SCM}(n) < l_{SDM}(n)\} \qquad (13)$$
$$\mathcal{M}_{DRW} = \{A_{SDM}(n) = A_{SCM}(n) \mid l_{SDM}(n) = l_{SCM}(n)\}$$

The first test measures the number of minimal chains for Equation 13, on every m basis. Figure 13 shows that the three values overlap. A close scrutiny reveals that from the beginning SDM has been in the lead until $m \leqslant 22$ at which SCM starts to take over. However, the difference is insignificant when compared to the total number of addition chains. This shows that SDM and SCM are equally competitive to one another.

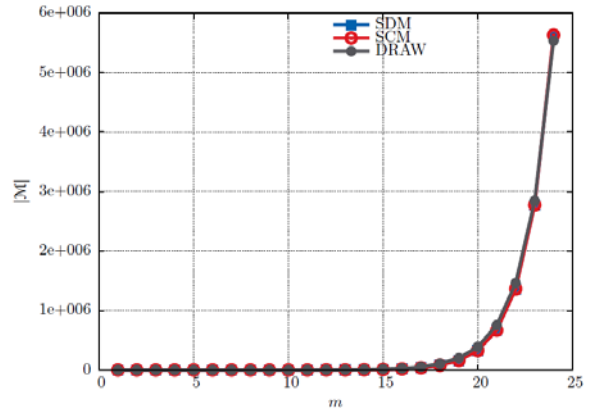

Figure 13: Number of minimal chains.

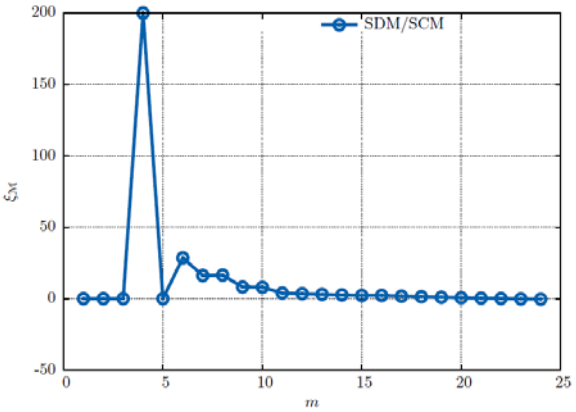

Figure 14: Percentage of betterment.

The second test calculates the percentage of betterment, $\xi_{\mathcal{M}}$ based on the result from Equation 13, defined by the following formula

$$\xi_{\mathcal{M}} = \frac{|\mathcal{M}_{\mathrm{SDM}}|-|\mathcal{M}_{\mathrm{SCM}}|}{(|\mathcal{M}_{\mathrm{SDM}}|+|\mathcal{M}_{\mathrm{SCM}}|)/2} * 100 \quad (14)$$

Note that the value of $\xi_{\mathcal{M}}$can as well be positive or negative. A positive value shows that SDM is better than SCM while anegative value shows that SCM is better than SDM for that particular *m*.From Figure 14, initially $\xi_{\mathcal{M}}$starts out at maximum value by favoring SDM and gradually decreases until *m* = 23 at which SCM begins to outperform SDM but at a very slow pace. For *m*> 20, $\xi_{\mathcal{M}}$stays below 1 percent. This result shows that SCM and SDM is equally competitive.

The third test calculates the average length of addition chains for integers defined by every *m*, and the respective formulae for SCM and SDM are given by

$$\mathcal{A}_{SCM} = \sum_{n=2^m+1}^{2^{m+1}} l_{SCM}(n)/2^m$$

$$\mathcal{A}_{SDM} = \sum_{n=2^m+1}^{2^{m+1}} l_{SDM}(n)/2^m \quad (15)$$

Figure 15 shows that $\mathcal{A}_{SCM}$ overlaps with $\mathcal{A}_{SDM}$ for all *m*< 25. A closer look reveals that SDMproduces more minimal chains than SCM only until *m* = 9, after which SCM begins to outperform SDM. However, the difference is very insignificant when compared to the total number of chains.

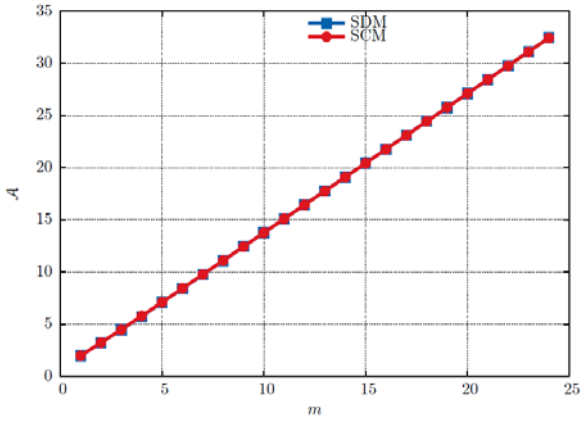

Figure 15: Average length of addition chains.

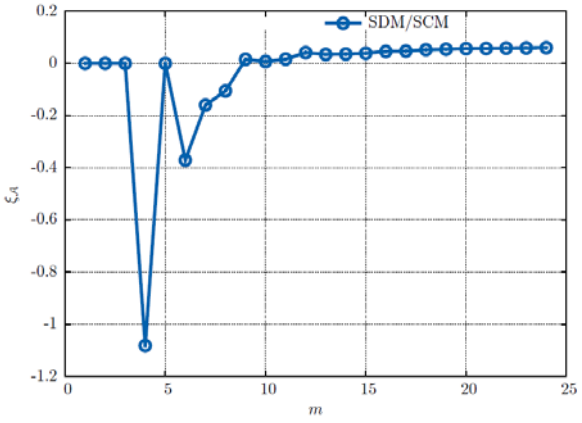

Figure 16: Percentage of improvement.

The fourth test measures the percentage of betterment, $\xi_{\mathcal{A}}$ based on Equation 15 using the following formula

$$\xi_{\mathcal{A}} = \frac{\mathcal{A}_{SDM} - \mathcal{A}_{SCM}}{(\mathcal{A}_{SDM} + \mathcal{A}_{SCM})/2} * 100 \quad (16)$$

Note that the value of $\xi_{\mathcal{A}}$ can be positive as well as negative. Positive value shows that SCM is better than SDM while negative value shows that SDM is better than SCM for that particular *m*, both for having shorter average length.

From Figure 16, there is a small swing around *y* = 0 axes for which SDM is a better method from $m \leqslant 8$, after which SCM becomes a better method.

Both parts of the result agree on that SDM is preferred to SCM for small *m*. For larger *m*, SCM is shown to be better than SDM. As a whole, for randomized input in this experiment, SCM is considered a preferable method to SDM. However, for a chosen input SDM remains the preferable method as it was proven that it could save up more terms when compared to NAF, than that of SCM which is at best only one term shorter.

VII. CONCLUSION

(Signed) Composition method is developed for taking composite unsigned and signed rule as their input. Theoretical foundation showed that CM and SCM are restricted to the same boundaries as that of DM and SDM respectively. An empirical investigation was conducted to cross-examine methods developed so far, although the test was limited to some integer size. Two parameters, minimal chain and average length were defined for the purpose of this assessment.

Our result shows that DM is found to be a preferable method to CM. The improved versions, SCM introduces 10 percent of improvement over CM whereas SDM introduces 8 percent of improvement over DM. Finally, SDM is shown to be considerably par with SCM although, at a very small percentage, the advantage was shown to favor SDM for small m and to SCM for large m. This work concludes the studies on decomposition-based and composition-based methods.

ACKNOWLEDGMENT

This research was supported bythe Malaysian Ministry of Higher Education [Grant No: FRGS/1/2015/ICT03/UNISZA/02/1(RR141)].

REFERENCES

[1] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computations, vol.48, no.177 (1987), pp. 203–209.
[2] V. S. Miller, Use of elliptic curves in cryptography, Proc. Of Crypto'85, vol.LNCS 218 (1985), pp. 417–426.
[3] P. Downey, B. Leong, and R. Sethi, Computing sequences with addition chains, SIAM J. Computing, vol.10, no.3 (1981), pp. 638–646.
[4] P. Balasubramaniam, and E. Karthikeyan, Elliptic curve scalar multiplication algorithm using complementary recoding. Applied Mathematics and Computation, vol.190 (2007), pp. 51–56.
[5] K. Okeya, K. Schmidt-Samoa, C. Spahn, and T. Takagi. Signed binary representations revisited. In Proc. CRYPTO '2004. LNCS 3152 (2004), pp. 123–139.
[6] F. Morain, and J. Olivos, Speeding up the computations on an elliptic curve using addition-subtraction chains, Theoretical Informatics and Applications, vol.24, no.6 (1990), pp. 531–544.
[7] D. E. Knuth, The art of computer programming, Volume 2: Seminumeral Algorithms, Addison-Wesley, 1981.
[8] S. Dominguez-Isidro, E, Mezura-Montes, N. Cruz-Corts, F. Rodrguez-Henrquez. Evolutionary Programming for the Length Minimization of Addition Chains. Engineering Applications of Artificial Intelligence. vol.37 (2015), pp. 125–134.
[9] N. Cruz-Corts, F. Rodrguez-Henrquez, R. Jurez-Morales, C.A. Coello-Coello. An Artificial Immune System Heuristic for Generating Short Addition Chains. IEEE Transaction on Evolutionary Computation. vol.12 no.1 (2008), pp. 1–24.
[10] M. A. Mohamed, M.R. M. Said, K.A. M. Atan, and Z. A. Zulkarnain. Shorter Addition Chain for Smooth Integers Using Decomposition Method. Int. J. Comp. Math. vol.88, no.11 (2011), pp. 2222–2232.
[11] M. A. Mohamed, K.A. M. Atan. Rule Based Representation of Integer for a New Addition Chain Method. Applied Mathematical Sciences, vol.6, no.30 (2012), pp. 1497–1503.
[12] M. A. Mohamed, M.R. M. Said. A Hybrid Addition Chain Method For Faster Scalar Multiplication. WSEAS Transactions on Communications. vol.14 (2015), pp. 153–158.
[13] A. T. Brauer. On addition chains. Bull. Amer. Math. Soc. vol.45 (1939), pp. 736–739.
[14] P. Erdos, Remarks on number theory III: On addition chains. Acta Arith. vol.6 (1960), pp. 77–81.