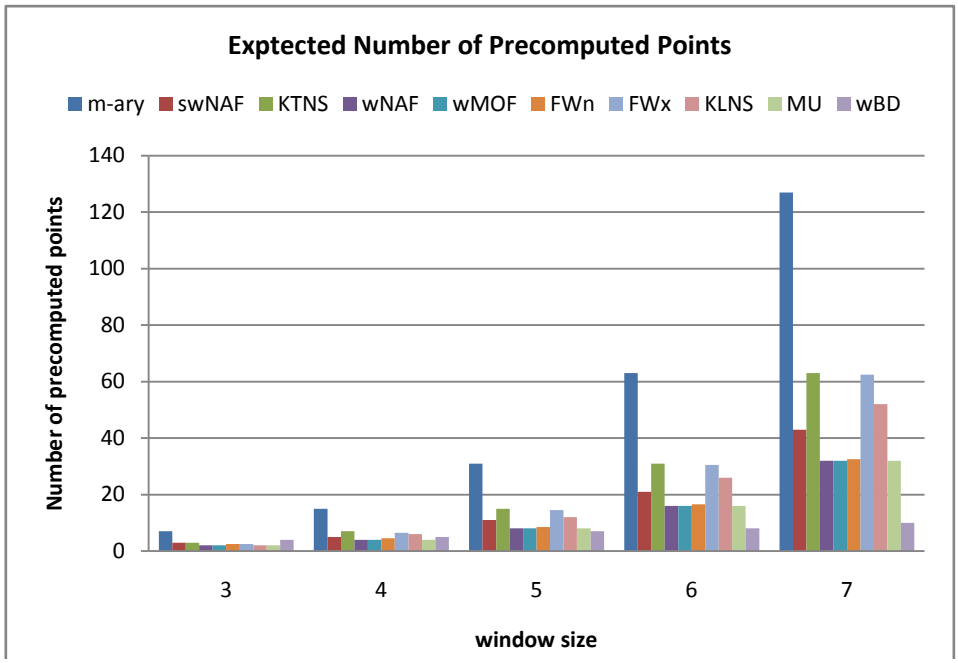


Figure 3 Expected Number of Precomputed Points for Window Methods

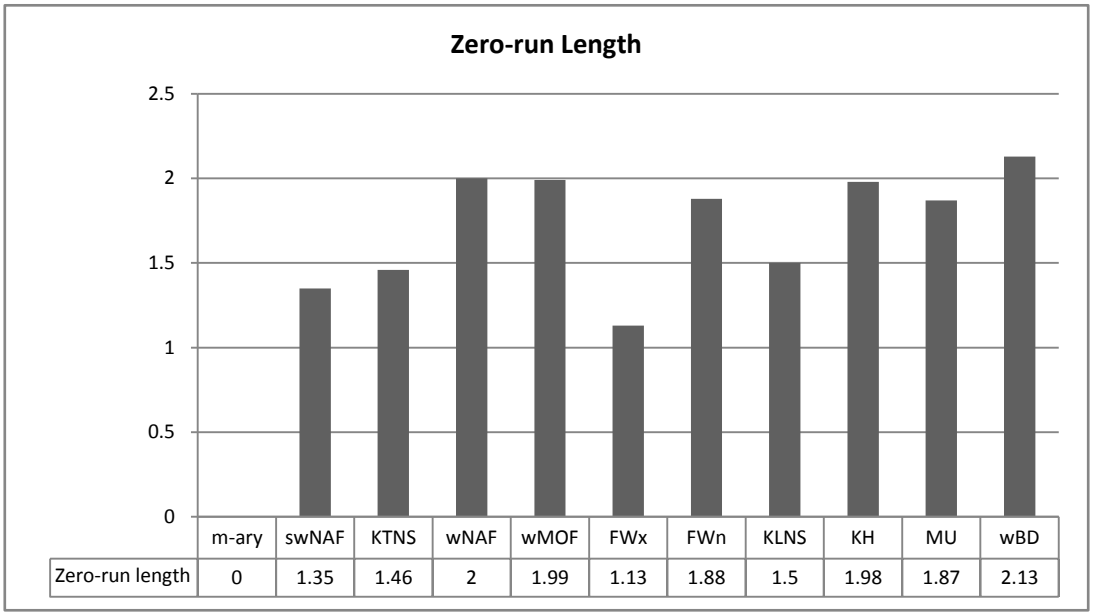
4.1 Zero-run Length

The zero-run length, which is denoted by $Z'(k)$, represents the average length of the zero runs (contiguous sequence of zeros) between windows in the exponent *k*. Increasing zero-run length will speed up the window methods[3]. The expected zero-run length of the binary representation is 1 [11], where it is 1.99 as measured in this study. The expected zero-run length of the NAF representation is 1.35 [11].Table 5 provides a summary of zero-run length for some investigated methods. The table includes mathematical representation and values of this metric. The values of wMOF and MU recoded keys are not determined in the literature. Whereas the formula of wBD method is phrased in the table and the value isexperimentally computed.

Table 5 Length of Zero Runs for Window Recoded Keys

Method	**Zero-run length $Z'(k)$**	**Value for $w = 5$**
m-ary	Zero	0
swNAF	$\frac{4}{3} - \frac{(-1)^w}{3.2^{w-2}}$	1.36
KTNS	1.42	1.42
wNAF	2 [11]	2
wMOF		
FW	$1 + \frac{m+1}{2^{w-1}}$ where m is an odd integer such that $1 \leq m \leq 2^{w-1} - 3$ for $w \geq 2$	1.13 min 1.88 max
KLNS	$1.5\ for\ 3 \leq w \leq 8$[11]	1.5
KH	$\frac{C}{2^{\lfloor \log_2 C \rfloor}} + 1C$ is the maximum number of points that can be stored	2
MU		
wBD	$\frac{\sum_{i=0}^{l-1} l_i z(i)}{\sum_{i=0}^{l-1} z(i)}, z(i) = \begin{cases} 1, & t_i = 0 \\ 0, & t_i \neq 0 \end{cases}$	

The experimental values of zero-run lengths are computed using 100,000 randomly generated keys of size 256 bit and $w = \{4, 5\}$. Figure 4represents the values of this metric that have been calculated. As it can be seen from the figure,wBD method has the maximum length of zero runs. Thisresults is considered an advantage of wBD method since it affects the speed of window method positively as mentioned by Koyoma[3].



	m-ary	swNAF	KTNS	wNAF	wMOF	FWx	FWn	KLNS	KH	MU	wBD
Zero-run length	0	1.35	1.46	2	1.99	1.13	1.88	1.5	1.98	1.87	2.13

Figure 4 Length of Zero Runs in Window Recoded Keys

4.2 Non-zero Density

The non-zero density ($N(k)$) is the ratio of number of non-zero digits to the bit-length of the key, while the hamming weight($W(k)$)is the number of non-zero digits in the recoded exponent. Fewer number of non-zero digits results in fewer number of EC addition required by a multiplication method. Thus, decreasing the value of $W(k)$ or $N(k)$ will increase the efficiency of the EC multiplication method.Most of the gained values are measured theoretically; i.e. by evaluating equations. The non-zero density has two mathematical representations: $N(k) = \frac{1}{w+Z'}$and $N(k) = \frac{W(k)}{n}$. In this section the former representation is used. Therefore, Table 6 shows the inverse of non-zero density ($\frac{1}{N(k)}$).

Table 6 Inverse of Non-zero Density for Some Window Methods

Method	1/Non-zero density
m-ary	w
swNAF	$w + \frac{4}{3} - \frac{(-1)^w}{3.2^{w-2}}$
KTNS	w + 1.42
wNAF	w + 1
wMOF	w + 1
FW	$w + 1 + \frac{m+1}{2^{w-1}}$ where m is an odd integer such that $1 \leq m \leq 2^{w-1} - 3$ for $w \geq 2$
KLNS	$w + \frac{4}{3} + \frac{(-1)^w}{3.2^{w-1}} - \left(\frac{1}{2}\right)^{w-3} + (2 + (-1)^w) \cdot \left(\frac{1}{2}\right)^{\frac{w}{2} - \frac{3}{4}(1-(-1))^w}$

	Or simply: $w + 1.5$
KH	$w + \beta + 1$, where $\beta = \frac{C}{2^{\lfloor \log_2 C \rfloor}} - 1$, and C is the maximum number of points that can be stored
MU	$w + 1$
wBD	$N(k) = \frac{\sum_{i=0}^{n-1} z(i)}{n}, n = \log_2 k,\ z(i) = \begin{cases} 0, & t_i = 0 \\ 1, & t_i \neq 0 \end{cases}$

The inverse of non-zero density is evaluated for $w = 5$ using the equations in Table 6 and the results are shown inFigure 5. It seems that fractional window method with *m* set to maximum value has the lowest value which means that it is expected to have the lowest number of EC additions. On the other hand, if the number of memory locations is limited to 8 locations, i.e. $m = 1$ for FW method, the lowest values are for KLNS and KTNS, while the value of wBD requires experimental computation. Therefore, wBD method in addition to other methods is verified by experimental computations.

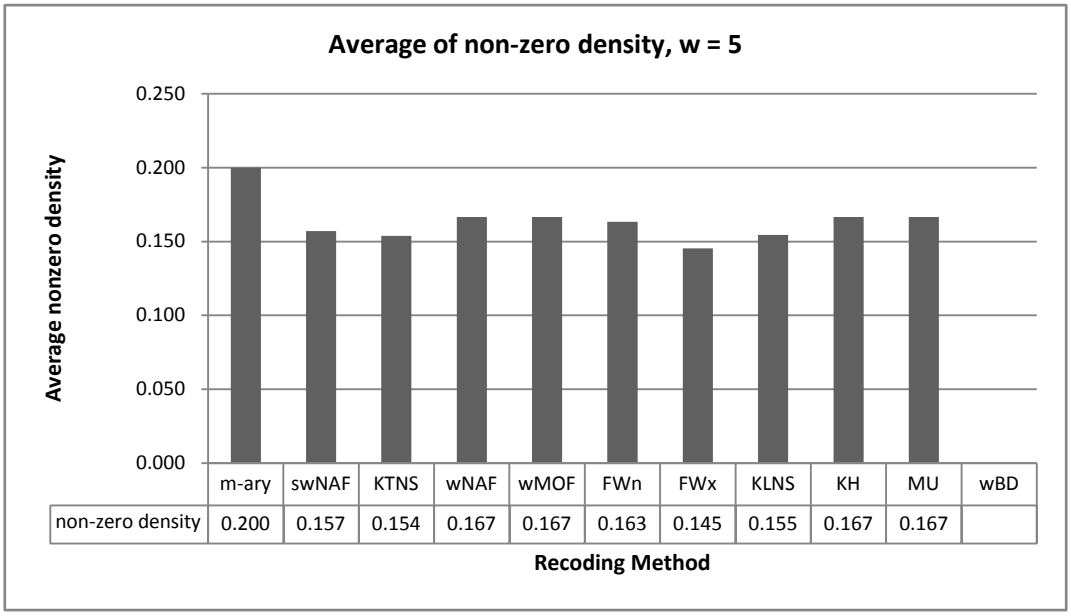


Figure 5 Non-zero Density of Various Recoded Keys – Calculated

An experiment is conducted for measuring the non-zero density for some recoding methods. Each column on the figure represents an average of 10,000 experiments. Randomly generated keys of 224 bit have been examined. The results are presented in Figure 6. Almost the same results are achieved for non-zero density by experimental results.

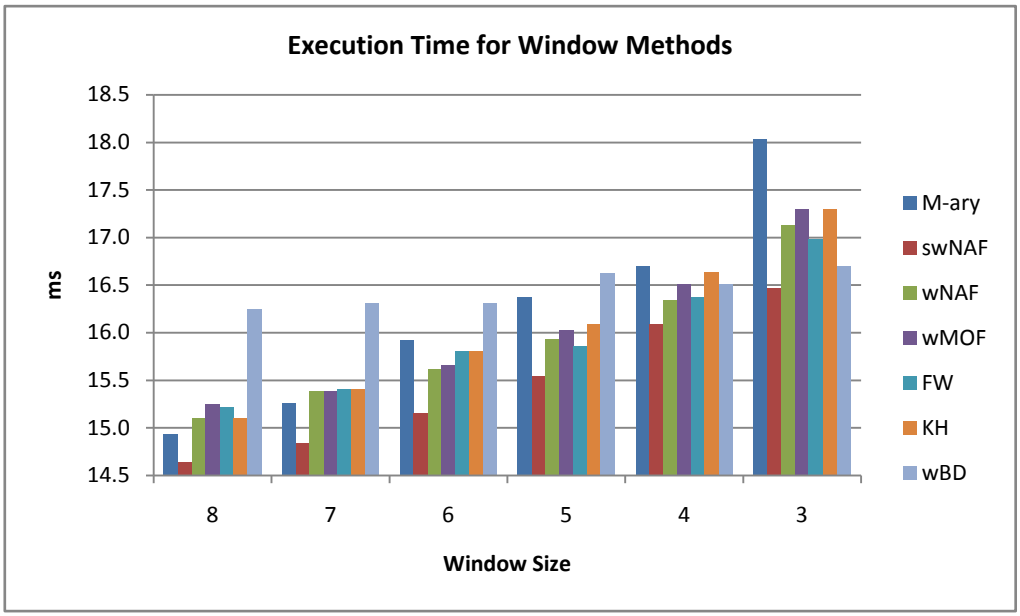


Figure 9 Time-Complexity for Various Window-Based EC Multiplication Methods

The time-complexity is measured and the results are shown in Figure 9. The execution time is measured over various windows sizes ($3 \leq w \leq 8$). The keys are randomly generated and stored in a text file in order not to include its generation time in the total execution time of the whole EC multiplication method. Each point represents the average of 10,000 experiments for each of the evaluated multiplication methods. According to Figure 9, the wBD method is comparable with other EC multiplication methods when $w \leq 4$, while the time-complexity is slightly higher than the other methods for $w \geq 5$.

5 Conclusion

A window-basedbig-digit EC multiplication method is proposed (wBD). One of the advantages of wBD multiplication method is itsbidirectional property. Thus, it is more suitable for memory limited devices. It is a one pass algorithm which means that its recoding process is considered as one the fast recoding methods that requires only one pass to recode the exponent k. The wBD multiplication algorithm is compared to current state of art algorithms based on some defined metrics such as number of precomputed points, EC-complexity and time-complexity.

Regarding precomputations, the precomputed window set is defined. It is found that the number of precomputed windows for wBD EC multiplication method is considered the lowest for various windows sizes. An EC multiplication method with lower number of precomputed points is more suitable for (devices equipped with small memory) limited memory devices.

The zero-run length of wBD keys is defined and the equation is presented in Table 5. The wBDkeys has the lowest zero-run length among other window methods. On the other hand, the nonzero density formula is identified and presented in Table 6. It has been calculated for window methods with $w = 5$. The result of this metric shows that wBD has the highest value which means that it will has the highest number of EC additions. Finally, the EC-complexity and time-complexity costs of elliptic curve methods are measured. Even though wBD multiplication method has a memory advantage against other examined methods, it is comparable with other window methods in terms of EC-complexity and time-complexity. Finally, Further improvement to wBD method may be achieved if more efforts are made to improve the efficiency of composite EC operations.

References

[1] H. Mimi, A. Samsudin, and S. Jahani, "Evaluating Composite EC Operations and their Applicability to the On-the-Fly and Non-Window Multiplication Methods," to appear 2013.

[2] J. A. Solinas, "Efficient Arithmetic on Koblitz Curves," *Designs, Codes and Cryptography,* vol. 19, pp. 195-249, 2000.

[3] K. Koyama and Y. Tsuruoka, "Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method," *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology,* pp. 345-357, 1993.

[4] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*: Cambridge University Press, 1999.

[5] K. Okeya, K. Schmidt-Samoa, C. Spahn, and T. Takagi, "Signed binary representations revisited," *Proceedings of CRYPTO'04,* vol. 3152, pp. 123-139, 2004.

[6] B. Möller, "Improved techniques for fast exponentiation," *ICISC'02: Proceedings of the 5th international conference on Information security and cryptology,* vol. 2587, pp. 298-312, 2002.

[7] K. Schmidt-Samoa, O. Semay, and T. Takagi, "Analysis of fractional window recoding methods and their application to elliptic curve cryptosystems," *IEEE Transactions on Computers,* vol. 55, pp. 48-57, Jan 2006.

[8] H. Darrel, J. M. Alfred, and V. Scott, *Guide to Elliptic Curve Cryptography*: Springer-Verlag New York, Inc., 2003.

[9] D. M. Gordon, "A survey of fast exponentiation methods," *Journal of Algorithms,* vol. 27, pp. 129-146, Apr 1998.

[10] F. Morain and J. Olivos, "Speeding up the Computations on an Elliptic Curve Using Addition-Subtraction Chains," *Rairo-Informatique Theorique Et Applications-Theoretical Informatics and Applications,* vol. 24, pp. 531-544, 1990.

[11] F. Y. Kong and D. X. Li, "A note on signed binary window algorithm for elliptic curve cryptosystems," *Cryptology and Network Security, Proceedings,* vol. 3810, pp. 223-235, 2005.

[12] A. Miyaji, T. Ono, and H. Cohen, "Efficient elliptic curve exponentiation," *ICICS '97: Proceedings of the First International Conference on Information and Communication Security,* vol. 1334, pp. 282-290, 1997.

[13] J. A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves," *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology,* vol. 1294, pp. 357-371, 1997.

[14] R. Avanzi, "A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue," *Selected Areas in Cryptography,* vol. 3357, pp. 130-143, 2005.

[15] J. A. Muir and D. R. Stinson, "New Minimal Weight Representations for Left-to-Right Window Methods," *CT-RSA'05: Proceedings of the 2005 international conference on Topics in Cryptology,* vol. 3376, pp. 366-383, 2005.

[16] M. Khabbazian, T. A. Gulliver, and V. K. Bhargava, "A new minimal average weight representation for left-to-right point multiplication methods," *Computers, IEEE Transactions on,* vol. 54, pp. 1454-1459, 2005.

[17] B. Möller, "Fractional windows revisited: Improved signed-digit representations for efficient exponentiation," *ICISC'04: Proceedings of the 7th international conference on Information Security and Cryptology,* vol. 3506, pp. 137-153, 2004.

[18] J. A. Muir and D. R. Stinson, "Minimality and other properties of the width-w nonadjacent form," *Mathematics of Computation,* vol. 75, pp. 369-384, 2006.

[19] S. Jahani and A. Samsudin, "ZOT-Binary: A New Numbering System with an Application on Big-Integer Multiplication," *Journal of Theoretical and Applied Information Technology (JATIT),* vol. 48, pp. 029 - 040, 2013.

[20] S. Jahani, "ZOT-MK: A New Algorithm for Big Integer Multiplication," MSc MSc, Department of Computer Science, Universiti Sains Malaysia, Penang, 2009.

[21] H. Mimi, A. Samsudin, and S. Jahani, "Elliptic Curve Point Multiplication Algorithm Using Precomputation," *Security and Communication Networks, to appear*, to appear 2013.

[22] M. Brown, D. Hankerson, J. Lopez, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," *Topics in Cryptology*, vol. 2020, pp. 250-265, 2001.

[23] P. Gallagher, D. D. Foreword, and C. F. Director, "FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS)," 2009.

[24] Shamus. (2010, December 16). *MIRACL Library*. Available: http://www.shamus.ie/