Advanced Science and Technology Letters
Vol.44 (Networking and Communication 2013), pp.44-48
http://dx.doi.org/10.14257/astl.2013.44.11

# An Efficient Scalar Multiplication Algorithm for Elliptic Curve Cryptography Using a New Signed-Digit Representation

Abdalhossein Rezai[1] and Parviz Keshavarzi[2]

[1]Academic Center for Education, Culture and Research (ACECR), Isfahan University of Technology (IUT) branch, 8415681167, Isfahan, Iran
rezaie@acecr.ac.ir
[2]Electrical and Computer Engineering Faculty, Semnan University, 3513119111, Semnan, Iran
pkeshavarzi@semnan.ac.ir

**Abstract.** This paper presents and evaluates a novel encoding algorithm to reduce the Hamming weight of the scalar. The scalar multiplication is modified to utilize this new scalar representation. The results show that the computation cost (the number of required clock cycles) in the proposed scalar multiplication is effectively reduced in comparison with other modified binary scalar multiplication algorithms.

**Keywords:** Network security, cryptography algorithm, Elliptic Curve Cryptography (ECC), scalar multiplication, signed-digit representation.

## 1 Introduction

Public-Key Cryptography (PKC) algorithms and protocols play an important role in the network security [1-2]. Amongst PKC algorithms and protocols, Elliptic Curve Cryptography (ECC) algorithms and protocols have the advantage of providing an equal level of security using smaller key size [3-4].

Scalar multiplication is an important operation in ECC, but it is a time-consuming operation. Integer representation has an important role to enhance the performance of scalar multiplication [5]. There are several papers investigated this issue, such as scalar multiplication algorithm using complement [6], modified complementary [7], and hybrid complementary and 1's complement [8]. Although these modifications enhanced the efficiency of this operation, but the improvement of the performance of this operation is a challenging issue. This paper presents and evaluates a novel scalar multiplication algorithm which reduces the computation cost (the number of required point addition/subtraction).

The rest of this paper is organized as follows: section 2 outlines the preliminaries of the proposed algorithms. Section 3 presents the proposed algorithms. Section 4 evaluates the proposed scalar multiplication, and finally the conclusion is given in section 5.

ISSN: 2287-1233 ASTL

## 2 Preliminaries

### 2.1 The Scalar Multiplication Algorithm:

Scalar multiplication, which is defined by Q=kP where P and Q are the elliptic curve points and k is a scalar, is an important operation in ECC. The binary method is a widely used method for performing the scalar multiplication. Algorithm 1 shows the binary scalar multiplication algorithm.

**Algorithm 1: The binary scalar multiplication algorithm**

```
INPUT: $k=(k_{n-1}k_{n-2}...k_1k_0)_2$ ;P=(x,y);
OUTPUT: Q=(x',y')=kP;
Q ← 0;
For i= n-1 Downto 0
      Q=2Q;
      If $k_i$=1 then  Q ← Q+P;
Return Q;
```

This algorithm scans the scalar bits from the left-to-right. When $k_i \neq 0$, the point addition and point doubling operations are performed, while for $k_i = 0$, the point doubling operation is only performed. So, the integer representation plays an important role in the performance of this algorithm. Two important integer representations will be described in the next sections.

### 2.2 The Complementary Recoding

A complementary representation of an integer $k = \Sigma_{i=0}^{n-1} k_i.2^i$, $k_i \in \{0,1\}$is a unique representation which satisfies the following equation [5-7]:

$$k = \Sigma_{i=0}^{n-1} k_i.2^i = 2^n - \bar{k} - 1 \quad (1)$$

where $\bar{k}$ is 1's complement of k and it is shown as $\bar{k} = \bar{k}_{n-1}\bar{k}_{n-2}\cdots\bar{k}_1\bar{k}_0$ in which

$$\begin{cases} \bar{k}_i = 0 \text{ if } k_i = 1 \\ \bar{k}_i = 1 \text{ if } k_i = 0 \end{cases} \quad \text{for } i = 0,1,\ldots,n-1 \quad (2)$$

### 2.3 The Canonical Recoding (CR)

The canonical recoding (CR) algorithm is shown in algorithm 2.

**Algorithm 2: The CR algorithm**

```
Input: A=$(a_{n-1}a_{n-2}\ldots a_1a_0)_2$
Output: D=$(d_nd_{n-1}\ldots d_1d_0)_{SD}$
$c_0$:= 0;
For i = 0 to n
      $c_{i+1}$:= $\lfloor(a_i + a_{i+1} + c_i)/2\rfloor$;
      $d_i$ := $a_i + c_i - 2c_{i+1}$;
Return D;
```

The average Hamming weight of an n-bit canonical recoded integer is $\frac{n}{3}$ [5].

# 3 The Proposed Algorithms

## 3.1 The Proposed Encoding Algorithm

The proposed encoding algorithm utilized two recoding methods: complementary and canonical recoding. Algorithm 3 is proposed for converting an n-bit integer k from its binary representation to the proposed representation.

**Algorithm 3: The proposed encoding algorithm**

```
Input: $k = (k_{n-1}, k_{n-2}, \ldots, k_1, k_0)_2$;
Output: $B = (b_n, b_{n-1}, \ldots, b_1, b_0)_{SD}$;
If $H(k)>n/2$ Then $A=\bar{k}$ Else $A=k$;
$D=CR(A)$;
If $H(k)>n/2$ Then $B = 2^n - D - 1$ Else $B=D$;
Return B;
```

In this algorithm, H(k) denotes the Hamming weight of k and the output is $B = (b_n, b_{n-1}, \ldots, b_1, b_0)_{SD}$.

## 3.2 The Proposed Scalar Multiplication Algorithm

In this section, the binary scalar multiplication is modified to use the proposed encoding algorithm. The proposed scalar multiplication is shown in algorithm 4.

**Algorithm 4: The proposed binary scalar multiplication algorithm**

```
Input: $k = (k_{n-1}, k_{n-2}, \ldots, k_1, k_0)_2$, $P=(x, y)$;
Output: $Q=(x', y')=kP$;
$Q=0$;
Compute B by applying algorithm 3 to k;
For i=n Downto 0
    $Q=2Q$;
    If ($b_i>0$) Then $Q=Q+P$;
    Else If ($b_i<0$) Then $Q=Q-P$;
Return Q;
```

The inputs of algorithm 3 are scalar $k = (k_{n-1}, k_{n-2}, \ldots, k_1, k_0)_2$ and elliptic curve point P, the output is elliptic curve point Q=kP. The point doubling operation is executed per iteration, while the point addition/subtraction operation is only executed for $b_i \neq 0$.

## 4 Comparison

Our analysis shows that the average Hamming weight of the proposed scalar multiplication is $\frac{3n}{13}$. The computation cost (the number of required point addition/subtraction operation) for the proposed scalar multiplication algorithm and two recent modifications of the binary scalar multiplication are computed and summarized in Fig. 1 for various operand size.

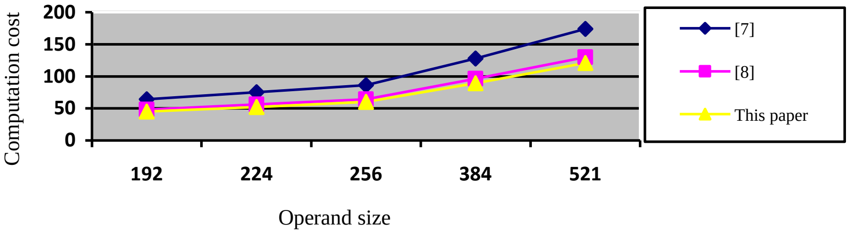

**Fig. 1.** The comparison of the computation cost

Based on our analysis which is shown in Fig. 1, the computation cost (the number of required point addition/subtraction operation) in the proposed scalar multiplication algorithm is reduced in comparison with two recent modifications of the binary scalar multiplication algorithm [7-8].

## 5 Conclusion

Scalar multiplication is a fundamental operation in ECC algorithms and protocols. This paper presents and evaluates a novel and efficient scalar multiplication algorithm based on a new scalar signed-digit representation. In this new scalar multiplication, the canonical recoding algorithm is applied to the complementary recoded scalar to reduce the Hamming weight. The results show that using the proposed scalar multiplication, the computation cost is considerably reduced in comparison with other modifications of the binary scalar multiplication algorithm [7-8].

## References

1. Rezai, A., Keshavarzi, P., Moravej, Z.: Secure SCADA communication by using a modified key management scheme. ISA Trans. 52(4), 517--524 (2013).
2. Rezai, A., Keshavarzi, P.: A new CMM-NAF modular exponentiation algorithm by using a new modular multiplication algorithm. Trends Applied Sci. Res., 7(3), 240--247 (2012).

3. Mahdizadeh, H., Masoumi, M.: Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF($2^{163}$). IEEE Trans.VLSI Syst. DOI: 10.1109/TVLSI.2012.2230410, (2013).
4. Rezai, A., Keshavarzi, P.: High-performance implementation approach of elliptic curve cryptosystem for wireless network applications. In Proc. IEEE Int. Conf. Consum. Electron. Commun. Netw., pp. 1323--1327, IEEE Press (2011).
5. Rezai, A., Keshavarzi, P.: CCS Representation: A new non-adjacent form and its application in ECC. J. Basic Appl. Sci. Res., 2(5), 4577-- 4586 (2012).
6. Chang, C., Kuo, Y., Lin, C.: Fast algorithms for common multiplicand multiplication and exponentiation by performing complements. In Proc. 17th IEEE Int. Conf. Advanced Inf. Netw. Appl. (AINA 2003), pp. 807--811.IEEE Press (2003).
7. Balasubramaniam P., Karthikeyan, E.: Elliptic curve scalar multiplication algorithm using complementary recoding. Appl. Math. Comput., 190(1), 51--56 (2007).
8. Huang X., Shahand, P., Sharma, D.: Minimizing Hamming weight based on 1's complement of binary numbers over GF($2^m$). In proc. IEEE. 12th Int. Conf. Advanced Commun. Tech. (ICACT 2010), pp. 1226--1230, IEEE Press (2010).