US 20130163760A1

(54) **METHOD OF ELLIPTIC CURVE CRYPTOGRAPHY USING EW-MOF ON SCALAR MULTIPLICATION**

(75) Inventors: **Hung-Nan Ye**, Hsinchu City (TW);
                 Kuo-Chen Wang, Hsinchu City (TW);
                 Rong-Hong Jan, Hsinchu City (TW)

(73) Assignee: **National Chiao Tung University**,
               Hsinchu City (TW)

Publication Classification

(57) **ABSTRACT**

A method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication. First, an elliptic curve and a base point on the elliptic curve are selected. Next, essential pre-computed points for a selected window size are calculated. Then, a private key is randomly generated and the mutual opposite form (MOF) is used to convert the private key's binary representation into a signed binary representation. Finally, a public key is calculated by using the enhanced window (EW) method. By greatly reducing the number of essential pre-computed points, the EW-MOF reduces average key generation time (including pre-computation time).
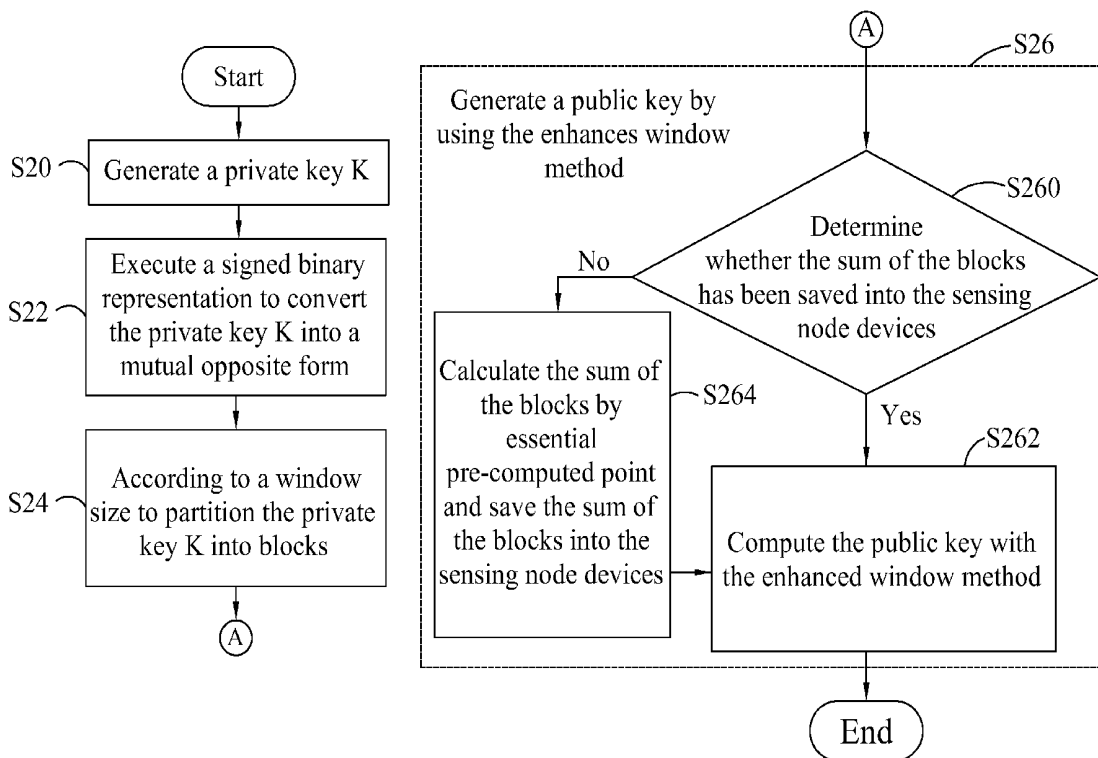
FIG. 1 (Prior Art)

FIG. 2

FIG. 3

Start

S10 — Select an elliptic curve

S12 — Select a base point P on the elliptic curve

S14 — Select a window size *w*, and executes essential pre-computed points pre-computation phase when a sensor node receives the elliptic curve and the base point

S16 — Save the essential pre-computed points after obtaining the essential pre-computed points

End

FIG. 4

Start

Generate a private key K — S20

Execute a signed binary representation to convert the private key K into a mutual opposite form — S22

According to a window size to partition the private key K into blocks — S24

(A)

(A)

Generate a public key by using the enhances window method — S26

Determine whether the sum of the blocks has been saved into the sensing node devices — S260

No

Calculate the sum of the blocks by essential pre-computed point and save the sum of the blocks into the sensing node devices — S264

Yes

Compute the public key with the enhanced window method — S262

End
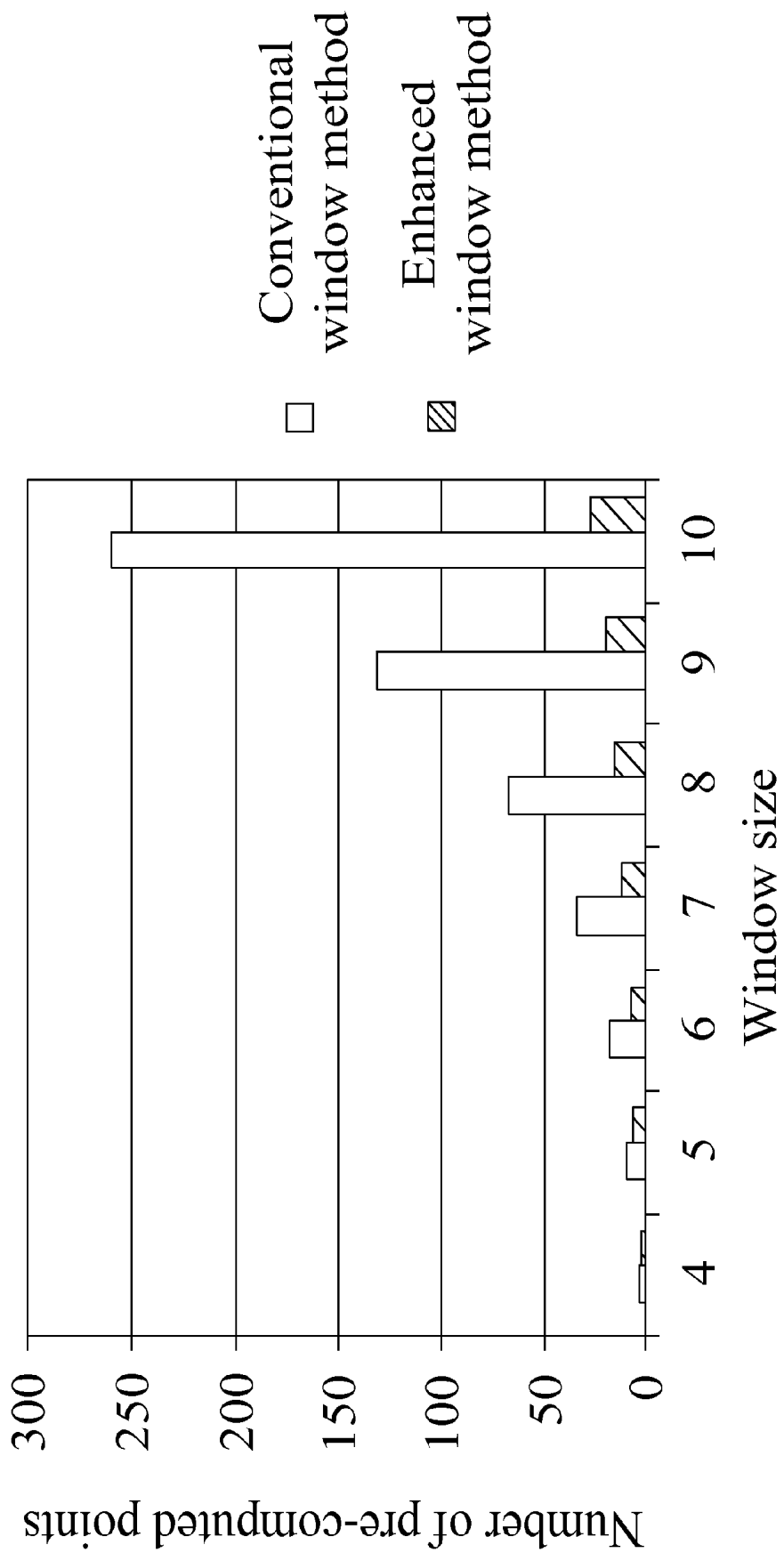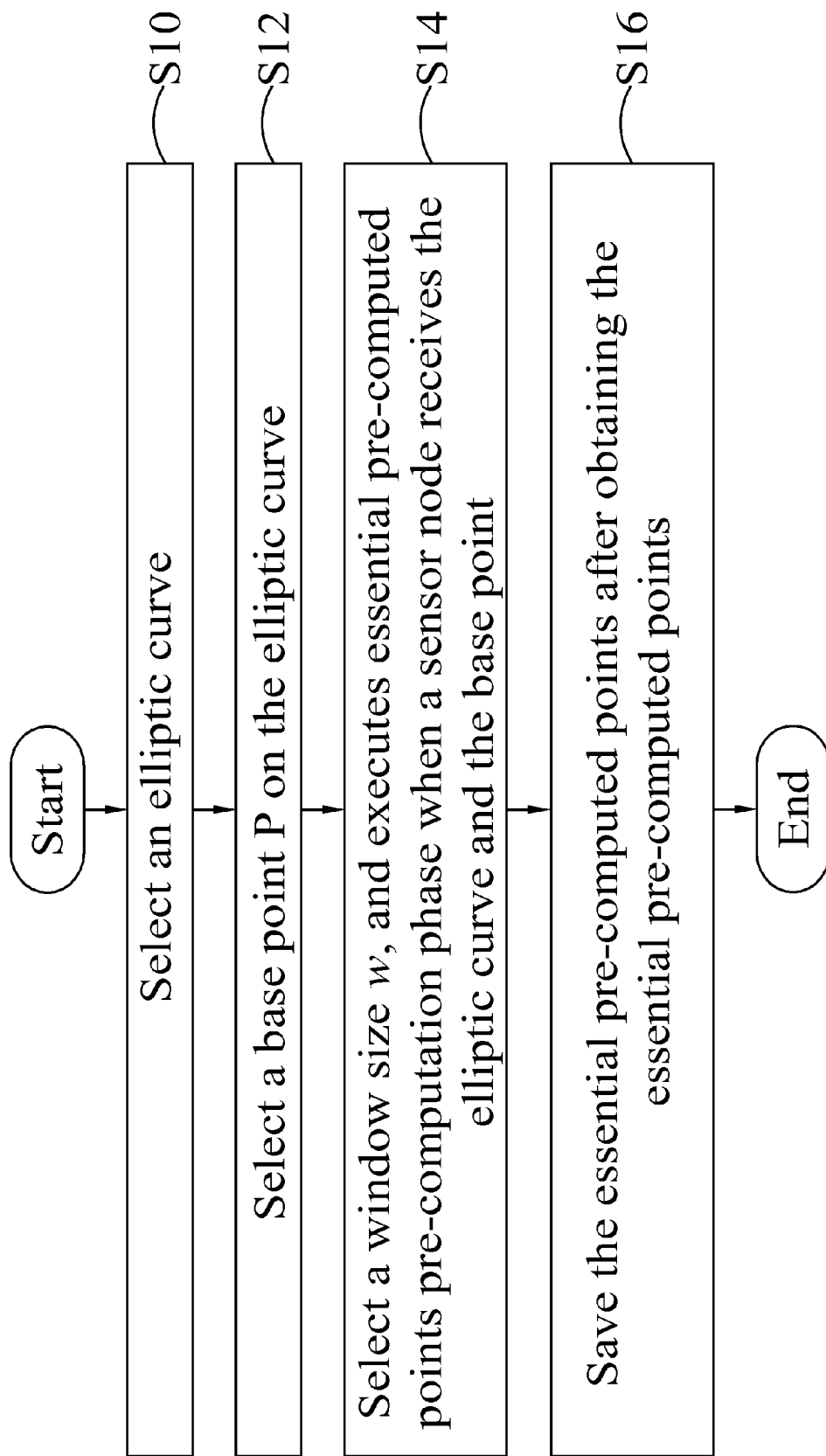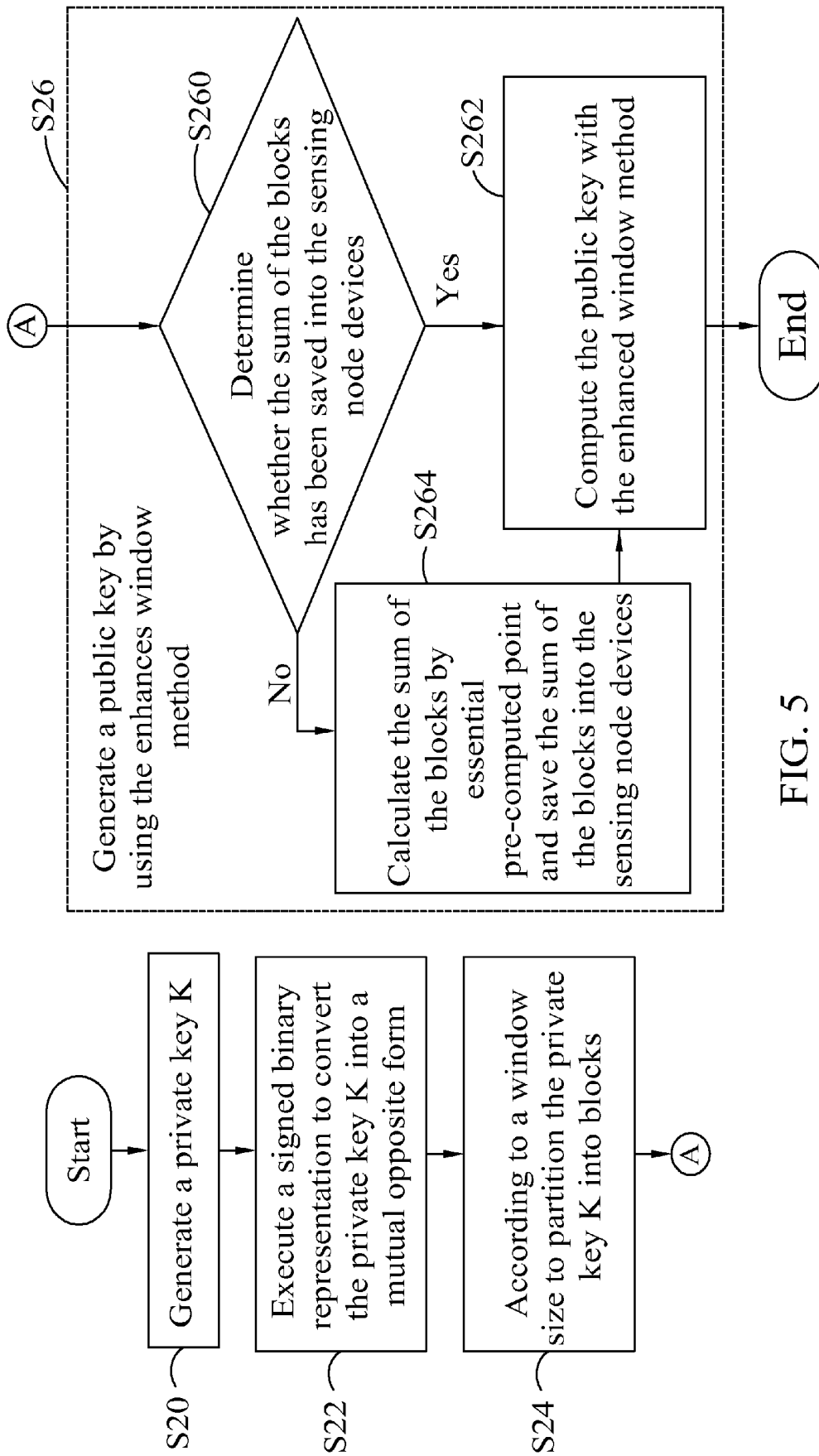
FIG. 5

METHOD OF ELLIPTIC CURVE CRYPTOGRAPHY USING EW-MOF ON SCALAR MULTIPLICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of Taiwan Patent Application No. 100148211, filed on Dec. 23, 2011, in the Taiwan Intellectual Property Office, the disclosure of which is incorporated herein in its entirety by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to the field of elliptic curve cryptographies, and more particularly to a method of elliptic curve cryptography (ECC) using enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication algorithm capable of randomly generating a private key and speeding up the public key generation.

[0004] 2. Description of the Related Art

[0005] In recent years, wireless (sensing) networks are used extensively in different areas such as military affairs, environmental surveillance and home care, and security becomes increasingly more important. Cryptography is a basic method providing safe services of the wireless (sensing) network. As a wireless (sensing) module in the wireless (sensing) networks has limited resources (or electric power), it is necessary to reduce the loads of computation, communication and memory for cryptography.

[0006] Based on the foregoing reason, research and development centers and related industries developed various cryptography mechanisms, such as RSA cryptography, DSA cryptography, and elliptic curve cryptography (ECC). The following table compares the number of bits in the encryption keys of the RSA cryptography and the elliptic curve cryptography under the same level of security:

RSA Cryptography (bits)	Elliptic Curve Cryptography (bits)
1024	160
2048	224
3072	256
7680	384
15360	512

[0007] In other words, the elliptic curve cryptography has much less bits in the key and a faster processing speed than those of other conventional cryptographs (such as RSA) under the same level of security. In other words, each bit of the key of the elliptic curve cryptography can provide much better security than that of the conventional cryptography, and thus the elliptic curve cryptography is very suitable to be used in various sensing node devices in the wireless (sensing) network such as a smart card, a mobile phone or a wireless mobile device used with an environment of limited electric power and memory space.

[0008] For example, the Elliptic Curve Diffie-Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA) are applied to various different sensing node devices in the elliptic curve cryptography, which scalar multiplication takes approximately 80% of the computation time, and such computation time will consume much electric power and shorten the service time of the sensing node device.

[0009] Further, the elliptic curve Diffie-Hellman algorithm is used as an example. In FIG. 1, a wireless sensing network includes a sensing node device A and a sensing node device B, wherein the private key, public key and secret key of the sensing node device A are K_A, Q_A and R_A respectively, and the private key, public key and secret key of the sensing node device B are K_B, Q_B and R_B respectively, wherein R_A and R_B are represented by the equations below:

$$R_A = K_A \times Q_B; \ R_B = K_B \times Q_A; \ \text{and} \ R_A = R_B$$

[0010] Further, Q=KP, wherein P and Q are two points on the elliptic curve, and K is a positive integer, and the following formula converts the private key K into a binary string list:

$$K = \sum_{j=0}^{L-1} k_j 2^i,$$

where

$$k_j \in \{1, 0\}$$

[0011] Assumed that D=6599=(1100111000111)$_2$, Q obtained from the computation process of K contains P, 2P, 3P, 6P, 12P, 24P, 25P, 50P, 51P, 102P, 103P, 206P, 412P, 824P, 1648P, 1649P, 3298P, 3299P, 6598P, 6599P; it is necessary to execute the computation for 19 times.

[0012] Wherein, the private key K is converted into a string list by using different conversion methods. If a mutual opposite form (MOF) is used, the private key K is converted into the string list as follows:

$$K = 6599 = \frac{\begin{array}{c} 1100111000111 \\ 1100111000111 \end{array}}{10\bar{1}0100\bar{1}00100\bar{1}} = (10\bar{1}0100\bar{1}00100\bar{1})_2$$

[0013] If a complementary recording method is used, the private key K is converted into the string list as follows:

$$K = 6599 = (1100111000111)_2$$

$$\bar{K} = (0011000111000)_2$$

$$K = 2^{13} - \bar{K} - 1 = (100\bar{1}1000\bar{1}\bar{1}100\bar{1})_2$$

[0014] If a non-adjacent form (NAF) is used, the private key K is converted into the string list as follows:

$$K = 6599 = (1100111000111)_2 = (10\bar{1}0100\bar{1}00100\bar{1})_2$$

[0015] The following table compares the aforementioned three conversion methods:

Conversion Method	Non adjacent Form (NAF)	Mutual Opposite Form (MOF)	Complementary Recoding
Hamming Weight	Large	Large	Small
Scanning Direction	From right to left	From right to left From left to right	From right to left From left to right
Average Execution Time	Large	Medium	Small

[0016] If a window method is used, the private key K is converted into the string list as follows:

[0017] If the window size w is equal to 2, the private key K is calculated as follows:

$$K=6599=(1100111000111)_2$$

$$w=2 \Rightarrow K=(11\ 00\ 11\ 1\ 000\ 11\ 1)_2$$

[0018] Therefore, the pre-computed point is 3 P.

[0019] If the window size w is equal to 3, then the private K is calculated as follows:

$$K=6599=(1100111000111)_2$$

$$w=3 \Rightarrow K=(11\ 00\ 111\ 000\ 111)_2$$

[0020] Therefore, the pre-computed points are 3P, 5P and 7P.

[0021] As shown above, although the window method requires calculating the pre-computed points, it can reduce the times of computation. In addition, the aforementioned mutual opposite form, complementary recording and non-adjacent form are used together with the window method, the pre-computed points are listed as follows.

[0022] A. If the mutual opposite form (MOF) is combined with the window method, and the window size w is 5, then the pre-computed points include 3P, 5P, 7P, 9P, 11P, 13P and 15P.

[0023] B. If the non-adjacent form (NAF) is combined with the window method, and the window size w is 5, then the pre-computed points include 3P, 5P, 7P, 9P, 11P, 13P, 15P, 17P and 21P.

[0024] C. If the complementary recording is combined with the window method, and the window size w is 5, then the pre-computed points include 3P, 5P, 7P, 9P, 11P, 13P, 15P, 17P, 21P, 23P, 25P, 27P, 29P and 31P.

[0025] The average execution time of using the non-adjacent form of the three conversion method is longer, and each conversion method combined with the window method and the complementary recording combined with the window method requires calculating most pre-computed points. If we can combine the mutual opposite form with the window method, we can shorten the average execution time significantly and reduce the computation and memory space, so as to decrease the consumption of electric power and memory of the sensing node device effectively.

SUMMARY OF THE INVENTION

[0026] In view of the aforementioned problems of the prior art, it is a primary objective of the invention to provide a method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication to overcome the problem of the conventional sensing node device that consumes much more electric power.

[0027] To achieve the foregoing objective, the present invention provides a method of ECC using EW-MOF on scalar multiplication applied in a wireless sensing network system including sensing node devices having a processing module and a storing module therein. First, an elliptic curve and a base point on the elliptic curve are selected by the processing module. Second, essential pre-computed points are calculated according to the selected window size by the processing module. Then, a private key is randomly generated by the processing module, and a mutual opposite form (MOF) is used to convert a binary representation of the private key into a signed binary representation. Finally, an enhanced win-

dow (EW) method is used to calculate a public key by the processing module. By decreasing the number of pre-computed points significantly, the method of the present invention can shorten the generation time (including the time for calculating the pre-computed points) of the public key.

[0028] Wherein, the enhanced window-based algorithm generates the essential pre-computed point by the following formula:

$$\{2P, 4P, 6P \ldots, (3+2S)P, (5+6S)P, (7+10S)P, \ldots\}$$

[0029] In the formula above, the numeric value of S is the number of even essential pre-computed points, and $S \geq 1$, and {the largest essential pre-computed point plus $(2S)P\} \geq (2^{2-1}-1)P$ (the largest pre-computed point).

[0030] Wherein, the window size (w) in the enhanced window-based algorithm is limited to a condition of window size $(w) \geq 4$.

[0031] Wherein, a private key is further converted into a binary string list, and the string list is represented by a signed binary string list according to a mutual opposite form coding method.

[0032] Wherein, each of the essential pre-computed points and the string list coded by the mutual opposite form are used to calculate and generate a public key.

[0033] To achieve the other foregoing objective, the present invention further provides a method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication applied in a wireless sensing network including sensing node devices having a processing module and a storing module therein. First, selecting an elliptic curve by the processing module. Second, selecting a base point P on the elliptic curve by the processing module, and P=(X, Y), wherein X and Y are coordinates of the elliptic curve. Then, using the selected window size to compute essential pre-computed points by the processing module, when the sensing node devices arranged in the wireless sensing network receives the elliptic curve and the base point. Finally, saving a numeric value of each of the essential pre-computed point into the storing module of each sensing node device, after each of the essential pre-computed points is computed.

[0034] In summation of the description above, the number of essential pre-computed points is reduced in advance and the private key can be represented by a string list coded by the mutual opposite form. As a result, the time required for randomly generating a private key and using the elliptic curve to derive the public key can be shortened effectively.

[0035] The aforementioned and other objects, technical characteristics, and advantages of the present invention will become apparent with the detailed description of preferred embodiments accompanied with related drawings as follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0036] FIG. 1 is a schematic view of a wireless sensing network;

[0037] FIG. 2 is a schematic view of the present invention of a wireless sensing network;

[0038] FIG. 3 is a histogram, comparing the quantity of pre-computed points under the condition of the same window size for an enhance window based method and a conventional window method;

[0039] FIG. 4 is a flow chart of applying the present invention in an initial parameter setting of a wireless sensing network; and

[0040] FIG. 5 is a flow chart of applying the present invention to generate a public key in a wireless sensing network.

DETAILED DESCRIPTION OF THE PREFERRED
EMBODIMENTS

[0041] The method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication of the present invention is described in details with reference to related figures as follows. It is noteworthy to point out that like elements illustrated in the drawings are represented by the same respective numerals, and all figures are drawn for the ease of explanation of the basic teachings of the present invention only, and thus are not drawn with the exact precision or scale ratio or intended for limiting the scope of the invention.

[0042] With reference to FIG. 2 for the schematic view of the present invention of a wireless sensing network system, the present invention discloses a method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication applied in the wireless sensing network system 1 including sensing node devices 10 having a processing module 11 and a storing module 12 therein. First, an elliptic curve and a base point on the elliptic curve are selected by the processing module 11. Next, essential pre-computed points are calculated according to a selected window size by the processing module 11. Then, saving a numeric value of each of the essential pre-computed point into the sensing node device 10 by the storing module 12, when each of the essential pre-computed points is computed. Then, a private key is randomly generated and the mutual opposite form (MOF) is used to represent a binary string list by a signed binary representation.

[0043] In the present invention, the essential pre-computed point generated by the enhanced window-based algorithm is a member of the following set:

$$\{2P, 4P, 6P \ldots, (3+2S)P, (5+6S)P, (7+10S)P, \ldots\}$$

[0044] Where, S is the number of even essential pre-computed points and $S \geq 1$, and {the largest essential pre-computed point plus $(2S)P\} \geq (2^{w-1}-1)P$ (the largest pre-computed point). The window size $(w) \geq 4$ is further limited in the enhanced window-based algorithm.

[0045] For example, if the enhanced window-based algorithm is used in the mutual opposite form (MOF), the window size is set to 6, and the largest essential pre-computed point is 31P, then the essential points are listed below of S equals to 1, 2 or 3 respectively.

[0046] If S=1, then the essential point belongs to {2P, 5P, 11P, 17P, 23P, 29P}.

[0047] Since $(29P+2P) \geq 31P$, therefore the number of essential points is 6.

[0048] If S=2, then the essential point belongs to {2P, 4P, 7P, 17P, 27P}.

[0049] Since $(27P+4P) \geq 31P$, therefore the number of essential points is 5.

[0050] If S=3, then the essential point belongs to {2P, 4P, 6P, 9P, 23P, 37P}.

[0051] Since $(37P+6P) \geq 31P$, therefore the number of essential points is 6.

[0052] The conventional window algorithm requires calculating a total number of 15 essential points, respectively: 3P, 5P, 7P, 9P, 11P, 13P, 15P, 17P, 19P, 21P, 23P, 25P, 27P, 29P and 31P, and the enhanced window-based algorithm requires cal-

culating at least 5 essential pre-computed points, respectively: {2P, 4P, 7P, 17P, 27P}. Obviously, the enhanced window-based algorithm of the present invention can reduce the number of pre-computed points effectively.

[0053] With reference to FIG. 3 for the graph that compares the quantity of pre-computed points under the condition of the same window size for an enhance window based method and a conventional window method, the enhanced window-based algorithm generates much less essential pre-computed points than the conventional window algorithm when the window size gets larger. Obviously, the enhanced window-based algorithm of the present invention is a main factor of improving the conventional elliptic curve cryptography.

[0054] The present invention further represents a private key by a binary string list, and represents the string list by a signed binary representation through a mutual opposite form (MOF). In summary, the number of essential pre-computed points is reduced in advance and a private key is represented a string list coded by the mutual opposite form (MOF). In other words, the time required for randomly generating a private key and using the elliptic curve to derive the public key can be shortened effectively.

[0055] With reference to FIG. 4 for a flow chart of applying a method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication in accordance with the present invention for an initial parameter setting in a wireless sensing network, the application comprises the following steps:

[0056] (S10) Select an elliptic curve, wherein the elliptic curve adopts a finite field such as a prime field (GF(p)), and the elliptic curve satisfies the following equation: $y^2 = x^3 + ax + b$, where $a, b \in GF(p)$, and $4a^3 + 27b^2 \neq 0$.

[0057] (S12) Select a base point P of the elliptic curve, wherein P=(X, Y), and X and Y are coordinates of the base point P in compliance with the elliptic curve.

[0058] (S14) Select a window size, and compute essential pre-computed points according to the window size when a sensing node device arranged in the wireless sensing network receives the elliptic curve and the base point.

[0059] (S16) Save the numeric value of each essential pre-computed point into the sensing node device when the essential pre-computed point is computed.

[0060] With reference to FIG. 5 for a flow chart of generating a public key in a wireless sensing network by using a method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication in accordance with the present invention, the method comprises the following steps:

[0061] (S20) Randomly generate a private key K.

[0062] (S22) Convert the private key K into a binary string list, and use a mutual opposite form (MOF) to represent the string list by a signed binary representation.

[0063] (S24) Generate essential pre-computed points according to a selected window size, and save the essential pre-computed points in the sensing node device.

[0064] (S26) Generate a public key, by using the essential pre-computed points and a private key both generated by the enhanced window-based algorithm and used a mutual opposite form to code the string list to represent for.

[0065] As described above, the time required for computing a public key derived by the elliptic curve can be reduced, since less essential pre-computed points are required and the private key is represented by a string list coded by the mutual opposite form.

4

[0066] In the present invention, the Step (S26) further comprises the following steps:

[0067] (S260) Determine whether each essential pre-computed point generated by the enhanced window-based algorithm this time has been saved into the sensing node device. If yes, then go to the next step, or else go to Step (S264).

[0068] (S262) Directly use the essential pre-computed points generated by the enhanced window-based algorithm and the mutual opposite form to code the string list for the calculation to generate a public key.

[0069] (S264) Generate other essential pre-computed points which have not been saved but will be used according to the pre-computed points in the Step (S24), and save the generated pre-computed points into sensing node device, and process the step (S262).

[0070] Therefore, the sensing node device saves its generated essential pre-computed points, and only generates essential pre-computed points which have not been saved, so that the sensing node device can further save electric power consumption.

[0071] In summation of the description above, the method of elliptic curve cryptography (ECC) using the enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication in accordance with the present invention has one or more of the following advantages:

[0072] The enhanced window-based algorithm of the invention can reduce the number of pre-computed points effectively.

[0073] The scalar multiplication algorithm of the present invention further reduces the time required for randomly generating a private key, using the mutual opposite form to code the private key and then generating a public key by using a small number of the essential pre-computed points.

[0074] While the invention has been described by means of specific embodiments, numerous modifications and variations could be made thereto by those skilled in the art without departing from the scope and spirit of the invention set forth in the claims.

What is claimed is:

1. A method of elliptic curve cryptography (ECC) using enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication, comprising the steps of:

    using an enhanced window-based algorithm to compute essential pre-computed points by a sensing node device arranged in a wireless sensing network according to a selected window size; and

    saving the essential pre-computed points by the sensing node device when the essential pre-computed points are computed;

    wherein the essential pre-computed points are saved into the sensing node device, so as to reduce the average time required for randomly generating a private key, and using the elliptic curve to derive a public key can be shortened effectively.

2. The method of ECC using EW-MOF on scalar multiplication as recited in claim 1, wherein the enhanced window-based algorithm generates the essential pre-computed points by the following formula:

$$\{2P, 4P, 6P \ldots, (3+2S)P, (5+6S)P, (7+10S)P, \ldots \};$$

wherein S is the number of even essential pre-computed points and $S \geqq 1$, and {the largest essential pre-computed point plus $(2S)P$} $\geqq (2^{w-1}-1)P$ (the largest pre-computed point).

3. The method of ECC using EW-MOF on scalar multiplication as recited in claim 2, wherein the window size (w) in the enhanced window-based algorithm is limited to a condition of window size (w)$\geqq$4.

4. The method of ECC using EW-MOF on scalar multiplication as recited in claim 3, wherein a private key is further converted into a binary string list, and the string list is represented by a signed binary string list according to a mutual opposite form coding method.

5. The method of ECC using EW-MOF on scalar multiplication as recited in claim 4, wherein each of the essential pre-computed points and the string list coded by the mutual opposite form are used to calculate and generate the public key.

6. A method of elliptic curve cryptography (ECC) using enhanced window-based mutual opposite form (EW-MOF) on scalar multiplication applied in a wireless sensing network including sensing node devices having a processing module and a storing module therein, comprising the steps of:

    selecting an elliptic curve by the processing module;

    selecting a base point P on the elliptic curve by the processing module, and P=(X, Y), wherein X and Y are coordinates of the elliptic curve;

    using the selected window size to compute essential pre-computed points by the processing module, when the sensing node devices arranged in the wireless sensing network receive the elliptic curve and the base point; and

    saving a numeric value of each of the essential pre-computed point into the sensing node devices by the storing module, after each of the essential pre-computed point is computed.

7. The method of ECC using EW-MOF on scalar multiplication as recited in claim 6, wherein the elliptic curve adopts a finite field, and the elliptic curve satisfies the equation of $y^2=x^3+ax+b$; where, a,b$\in$ GF(p), and $4a^3+27b^2\neq0$.

8. The method of ECC using EW-MOF on scalar multiplication as recited in claim 7, further comprising steps of generating a public key, comprising:

    randomly generating a private key;

    converting the private key into a mutual opposite form by executing a signed binary representation;

    according to a window size to partition the private key into blocks; and

    saving sum of the blocks for the computation to generate the public key.

9. The method of ECC using EW-MOF on scalar multiplication as recited in claim 8, wherein the step of generating the public key further comprises the steps of:

    determining whether the sum of the blocks has been saved into the sensing node devices;

    calculating the sum of the blocks by essential pre-computed point and save the sum of the blocks into the sensing node devices, if the sum of the blocks has not been saved in sensing node devices; and

    generating the public key by using the enhances window method by the sensing node devices, if the sum of the blocks has been saved in sensing node devices.

* * * * *