The abstract of the document is as follows:

A method, apparatus and computer program product are provided to more efficiently perform aspects of elliptic curve cryptography such as by more efficiently multiplying an integer k by a point P on an elliptic curve by decomposing the integer into integers k1 and k2. In this regard, respective bounds for k1 and k2 may be determined (100, 102) and, subject to the respective bounds, k1 and k2 may then be determined (114, 116) such that the product of k and the point P on the elliptic curve may be determined based upon k1 and k2 without requiring the point P to be multiplied by k.
METHOD, APPARATUS AND COMPUTER PROGRAM PRODUCT FOR EFFICIENT
ELLIPTIC CURVE CRYPTOGRAPHY

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Application No. 61/100,926, filed September 29, 2008, the contents of which are incorporated herein in their entirety.

TECHNOLOGICAL FIELD

[0002] Embodiments of the present invention relate generally to public key cryptography and, more particularly, to methods, apparatus and computer programs products for efficiently implementing elliptic curve cryptography.

BACKGROUND

[0003] Various techniques have been employed to increase the security associated with the communication of messages and to correspondingly decrease the risk that unintended recipients can comprehend and make use of the messages. Accordingly, a variety of cryptographic techniques have been developed such that messages between two or more parties may be encrypted. While the authorized parties can decrypt the messages and utilize the messages for their intended purpose, the use of encryption decreases the risk that unintended recipients can similarly make use of the messages.

[0004] One cryptographic technique relies upon public key cryptography. In public key cryptography, a first party has a pair of cryptographic keys - a public key and private key. The private key remains a secret to the first party, but the public key may be distributed to other parties. Thus, messages received by the first party that have been encrypted with the public key of the first party can only by decrypted utilizing the corresponding private key. Since the first party will be the only party having the private key, the first party is the only one that can decrypt the message. While the public and private keys are related mathematically, the private key cannot, as a practical matter, be derived from the public key.

[0005] One approach to public key cryptography is elliptic curve cryptography. Elliptic curve cryptography is based on the algebraic structure of elliptic curves over finite fields. Indeed, elliptic curve cryptography is becoming an increasingly common algebraic setting for public key cryptography due, for example, to the relatively short parameter and key lengths. For example,
the Bluetooth™ wireless protocol has a pairing method that uses elliptic curve cryptography over a prime field.

While elliptic curve cryptography offers various advantages including advantages relating to relatively short parameter and key lengths, elliptic curve cryptography may suffer from having field operations that are more complicated and slower than are desired. As such, a variety of techniques have been developed in an effort to improve the performance of elliptic curve cryptography. In this regard, elliptic curve cryptography utilizes the integer multiples of points on an elliptic curve and, as such various representations of the integer have been developed in order to increase the computational speed. For example, the binary representation of the integer may be utilized in order to reduce the relatively large multiplication task to a series of point doublings and multiplication. Alternatively, curve endomorphism may be utilized. In this regard, the efficiency offered by curve endomorphism can be appreciated by considering E to be an elliptic curve over Fq with P being a point on the curve that generates a relatively large subgroup of order n on E. Additionally, Φ can be an endomorphism over Fq and λ can be a root of the characteristic polynomial of Φ modulo n. As such the multiplication by λ of the point P can be computed as Φ(P). In many cases, Φ(P) can be computed relatively rapidly. Then, if any positive integer k less than n can be decomposed in the form as k = k1 + k2·λ (mod n) wherein k1 and k2 are shorter than k, then kP can be efficiently computed as kP = k1 + k2· Φ(P), wherein "..." denotes integer multiplication. If k1 and k2 are about the same size, then various methods for simultaneous scalar multiplication can be efficiently used.

In order to increase the efficiency of elliptic curve cryptography, techniques have been developed for computing, given a positive integer n and positive integers λ and k less than n, a decomposition of k = k1 + k2·λ. In this regard, the values k1 and k2 can be determined utilizing the LLL algorithm or, as described by the European Patent Application to Robert Gallant et al. bearing Publication No. EP 1 141 820, by first computing two relatively short vectors v1 and v2 using the extended Euclidean algorithm. The resulting system of linear equations is then solved by linear algebra to determine fractions q1 and q2, which are then rounded to the nearest integers, designated, for example, as b1 and b2, respectively. Then the two components of the vector (k,0) - (blv1 + b2v2) may be computed, k1 may be obtained as the first component and k2 may be obtained as the second component of this vector.

While these techniques permit the determination of k1 and k2 into which the positive integer k is decomposed, these techniques do not provide any bounds upon the size of k1 and k2. For efficient simultaneous scalar multiplication, however, it is desired that the
decomposition of \( k \) in terms of \( k_1 \) and \( k_2 \) be balanced, meaning that \( k_1 \) and \( k_2 \) are of about equal size. By failing to have bounds on the size of \( k_1 \) and \( k_2 \), such prior techniques may fail to operate in the most optimal manner. As such, it would be desirable to provide an improved elliptic curve cryptographic technique in which the sizes of \( k_1 \) and \( k_2 \) are known to be relatively equally small for given \( n \) and \( \lambda \). Also while the foregoing techniques allow efficient implementation on some computation environments, they require division of integers and rounding fractions, which may not be readily available in every computation platform. As such, it would also be desirable to provide an improved elliptic curve cryptographic technique which is configured to be supported by a relatively wide range of computation platforms.

BRIEF SUMMARY

A method, apparatus and computer program product are therefore provided in order to more efficiently perform aspects of elliptic curve cryptography. In particular, methods, apparatus and computer program products are provided that may more efficiently multiply an integer \( k \) by a point \( P \) on an elliptic curve by decomposing the integer \( k \) into integers \( k_1 \) and \( k_2 \). In accordance with a method of one embodiment, respective bounds for \( k_1 \) and \( k_2 \) are then determined. Subject to the respective bounds, \( k_1 \) and \( k_2 \) may then be determined such that the product of \( k \) and the point \( P \) on the elliptic curve may be determined based upon \( k_1 \) and \( k_2 \) without requiring the point \( P \) to be multiplied by \( k \). In order to determine the respective bounds, an extended Euclidean algorithm may be run for a number of points \( n \) on the elliptic curve and a multiplier \( \lambda \) to generate sequences of quotients and remainders such that the \( m \)th remainder is identified to bound \( k_1 \) based upon the relationship of the \( m \)th remainder to \( n \). Additionally, a sequence of integers \( t \) may be determined based upon the sequence of quotients such that the bound for \( k_2 \) may be defined based upon a relationship of at least two of the integers \( t \) to \( n \).

According to another embodiment of the present invention, an apparatus is provided that includes a processor that may be configured to more efficiently multiply an integer \( k \) by a point \( P \) on an elliptic curve by decomposing the integer \( k \) into integers \( k_1 \) and \( k_2 \). In accordance with one embodiment, the processor may also be configured to determine respective bounds for \( k_1 \) and \( k_2 \). Subject to the respective bounds, the processor may be configured to determine \( k_1 \) and \( k_2 \) such that the product of \( k \) and the point \( P \) on the elliptic curve may be determined based upon \( k_1 \) and \( k_2 \) without requiring the point \( P \) to be multiplied by \( k \). In order to determine the respective bounds, the processor may be configured to run an extended Euclidean algorithm for a number of points \( n \) on the elliptic curve and a multiplier \( \lambda \) to generate sequences...
of quotients and remainders such that the m\textsuperscript{th} remainder is identified to bound k\textsubscript{1} based upon the relationship of the m\textsuperscript{th} remainder to n. Additionally, the processor may be configured to determine a sequence of integers t based upon the sequence of quotients such that the bound for k\textsubscript{2} may be defined based upon a relationship of at least two of the integers t to n.

According to yet another embodiment of the present invention, a computer program product is provided for more efficiently multiplying an integer k by a point P on an elliptic curve. The computer program product includes a computer-readable storage medium and a plurality of computer-readable instructions stored upon the computer-readable storage medium. The computer-readable instructions may include first computer-readable instructions for decomposing the integer k into integers k\textsubscript{1} and k\textsubscript{2}, second computer-readable instructions for determining bounds for k\textsubscript{1} and k\textsubscript{2} and third computer-readable instructions for determining k\textsubscript{1} and k\textsubscript{2}, subject to the respective bounds, such that the product of k and the point P on the elliptic curve may be determined based upon k\textsubscript{1} and k\textsubscript{2} without requiring the point P to be multiplied by k. In order to determine the respective bounds, the second computer-readable instructions may be configured to run an extended Euclidean algorithm for a number of points n on the elliptic curve and a multiplier \(\lambda\) to generate sequences of quotients and remainders such that the m\textsuperscript{th} remainder is identified to bound k\textsubscript{1} based upon the relationship of the m\textsuperscript{th} remainder to n. Additionally, the second computer-readable instructions may be configured to determine a sequence of integers t based upon the sequence of quotients such that the bound for k\textsubscript{2} may be defined based upon a relationship of at least two of the integers t to n.

BRIEF DESCRIPTION OF THE DRAWINGS

Having thus described some embodiments of the invention in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. 1 is a block diagram of a system for employing elliptic curve cryptography according to one embodiment of the present invention;

FIG. 2 is a schematic block diagram of a mobile terminal according to one embodiment to the present invention; and

FIG. 3 is a flow chart of the operations performed in accordance with one embodiment to the present invention.
DETAILED DESCRIPTION

[0016] Some embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. Indeed, various embodiments of the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like reference numerals refer to like elements throughout. As used herein, the terms "data," "content," "information" and similar terms may be used interchangeably to refer to data capable of being transmitted, received and/or stored in accordance with embodiments of the present invention. Moreover, the term "exemplary", as used herein, is not provided to convey any qualitative assessment, but instead merely to convey an illustration of an example. Thus, use of any such terms should not be taken to limit the spirit and scope of embodiments of the present invention.

[0017] FIG. 1 illustrates a generic system diagram in which a device such as a mobile terminal 10, which may benefit from embodiments of the present invention, is shown in an exemplary communication environment. As shown in FIG. 1, an embodiment of a system in accordance with an example embodiment of the present invention may include a first communication device (e.g., mobile terminal 10) and a second communication device 20 capable of communication with each other via a network 30.

[0018] The network 30 may include a collection of various different nodes, devices or functions that may be in communication with each other via corresponding wired and/or wireless interfaces. As such, the illustration of FIG. 1 should be understood to be an example of a broad view of certain elements of the system and not an all inclusive or detailed view of the system or the network 30. Although not necessary, in some embodiments, the network 30 may be capable of supporting communication in accordance with any one or more of a number of first-generation (1G), second-generation (2G), 2.5G, third-generation (3G), 3.5G, 3.9G, fourth-generation (4G) mobile communication protocols, Long Term Evolution (LTE), and/or the like.

[0019] One or more communication terminals such as the mobile terminal 10 and the second communication device 20 may be in communication with each other via the network 30 and each may include an antenna or antennas for transmitting signals to and for receiving signals from a base site, which could be, for example a base station that is a part of one or more cellular or mobile networks or an access point that may be coupled to a data network, such as a local area network (LAN), a metropolitan area network (MAN), and/or a wide area network (WAN), such
as the Internet. In turn, other devices such as processing elements (e.g., personal computers, server computers or the like) may be coupled to the mobile terminal 10 and the second communication device 20 via the network 30. By directly or indirectly connecting the mobile terminal 10 and the second communication device 20 and other devices to the network 30, the mobile terminal 10 and the second communication device 20 may be enabled to communicate with the other devices or each other, for example, according to numerous communication protocols including Hypertext Transfer Protocol (HTTP) and/or the like, to thereby carry out various communication or other functions of the mobile terminal 10 and the second communication device 20, respectively.

Furthermore, although not shown in FIG. 1, the mobile terminal 10 and the second communication device 20 may communicate in accordance with, for example, radio frequency (RF), Bluetooth (BT), Infrared (IR) or any of a number of different wireline or wireless communication techniques, including LAN, wireless LAN (WLAN), Worldwide Interoperability for Microwave Access (WiMAX), WiFi, ultra-wide band (UWB), Wibree techniques and/or the like. As such, the mobile terminal 10 and the second communication device 20 may be enabled to communicate with the network 30 and each other by any of numerous different access mechanisms. For example, mobile access mechanisms such as wideband code division multiple access (W-CDMA), CDMA2000, global system for mobile communications (GSM), general packet radio service (GPRS) and/or the like may be supported as well as wireless access mechanisms such as WLAN, WiMAX, and/or the like and fixed access mechanisms such as digital subscriber line (DSL), cable modems, Ethernet and/or the like.

In example embodiments, either of the first communication device and the second communication device 20 may be mobile or fixed communication devices. Thus, for example, the mobile terminal 10 and the second communication device 20 could be, or be substituted by, any of personal computers (PCs), personal digital assistants (PDAs), wireless telephones, desktop computers, laptop computers, mobile computers, cameras, video recorders, audio/video players, positioning devices, game devices, television devices, radio devices, or various other like devices or combinations thereof.

FIG. 2 illustrates a schematic block diagram of an apparatus for facilitating elliptic curve cryptography according to an exemplary embodiment of the present invention. The apparatus 50 of FIG. 2 may be employed, for example, on or as a communication device (e.g., the mobile terminal 10 and/or the second communication device 20) or a variety of other devices, both mobile and fixed (such as, for example, any of the devices listed above). Alternatively,
embodiments may be employed on a combination of devices. Accordingly, some embodiments
of the present invention may be embodied wholly at a single device (e.g., the mobile terminal 10)
or by devices in a client/server or distributed computing relationship. Furthermore, it should be
noted that the devices or elements described below may not be mandatory and thus some may be
omitted in certain embodiments.

[0023] As shown, the apparatus 50 may include or otherwise be in communication with a
processor 70, a user interface 72, a communication interface 74 and a memory device 76. The
memory device 76 may include, for example, volatile and/or non-volatile memory. The memory
device 76 may be configured to store information, data, applications, instructions or the like for
enabling the apparatus to carry out various functions in accordance with exemplary embodiments
of the present invention. For example, the memory device 76 could be configured to buffer input
data for processing by the processor 70. Additionally or alternatively, the memory device 76
could be configured to store instructions for execution by the processor 70. As yet another
alternative, the memory device 76 may be one of a plurality of databases that store information
and/or media content.

[0024] The processor 70 may be embodied in a number of different ways. For example,
the processor 70 may be embodied as various processing means such as a processing element, a
coprocessor, a controller or various other processing devices including integrated circuits such as,
for example, an ASIC (application specific integrated circuit), an FPGA (field programmable gate
array), a hardware accelerator, or the like. In an exemplary embodiment, the processor 70 may be
configured to execute instructions stored in the memory device 76 or otherwise accessible to the
processor 70.

[0025] Meanwhile, the communication interface 74 may be any means such as a device or
circuitry embodied in either hardware, software, or a combination of hardware and software that
is configured to receive and/or transmit data from/to a network and/or any other device or module
in communication with the apparatus. In this regard, the communication interface 74 may
include, for example, an antenna (or multiple antennas) and supporting hardware and/or software
for enabling communications via Bluetooth signaling protocol or with a wireless communication
network. In fixed environments, the communication interface 74 may alternatively or also
support wired communication. As such, the communication interface 74 may include a
communication modem and/or other hardware/software for supporting communication via cable,
digital subscriber line (DSL), universal serial bus (USB) or other mechanisms.
[0026] The user interface 72 may be in communication with the processor 70 to receive an indication of a user input at the user interface 72 and/or to provide an audible, visual, mechanical or other output to the user. As such, the user interface 72 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen, a microphone, a speaker, or other input/output mechanisms. In an exemplary embodiment in which the apparatus is embodied as a server or some other network devices, the user interface 72 may be limited, or eliminated. However, in an embodiment in which the apparatus is embodied as a communication device (e.g., the mobile terminal 10), the user interface 72 may include, among other devices or elements, any or all of a speaker, a microphone, a display, and a keyboard or the like.

[0027] Referring now to Figure 1, the system of one embodiment may be configured to support communications between the mobile terminal 10 and the second communications device 20 that are encrypted in accordance with a public key cryptographic technique. More particularly, the system of one embodiment may be configured to support encryption of the communications between the mobile terminal 10 and the second communications device 20 (or between any other communications devices) in accordance with elliptic curve cryptography. For example, the mobile terminal 10 and the second communications device 20 may be configured to communicate with one another via the Bluetooth™ signaling protocol and, as such, mobile terminal 10 and/or the second communications device 20 may employ elliptic curve cryptography in order to secure the Bluetooth™ communications therebetween. As noted above, however, the mobile terminal 10 and the second communications device 20 may communicate via a wide variety of other networks and signaling protocols, if so desired.

[0028] As described below and in accordance with one embodiment, the apparatus 50 and, in particular, the processor 70 may be configured to support elliptic curve cryptography by determining the values of k1 and k2 into which the integer multiplier k may be decomposed in such a manner that bounds on the sizes of the integers k1 and k2 may also be determined. In accordance with elliptic curve cryptography, a point on an elliptic curve may be multiplied by a previously unknown integer multiplier k. In order to increase the speed at which this multiplication is performed, the multiplier λ may be provided and k may be decomposed into smaller integers k1 and k2 such that the multiplication of the point on the elliptic curve by the integer multiplier k can be equivalently and more quickly computed by combining the results of two multiplication operations, namely, the multiplication of point p by k1 and the multiplication of point p by the product of λ and k2.
In order to determine the values \( k_1 \) and \( k_2 \) as well as their respective bounds, the apparatus 50 and, more typically, the processor 70 of one embodiment may perform the operations set forth in Figure 3. As shown in Figure 3, the operations may be generally divided into a first step and a second step. If desired, the first step may be determined in advance of the encryption operation and may be determined once for all future unknown values \( k \). As such, the first step is not dependent upon the value of \( k \). The apparatus 50 may perform the operations of step 1 and then store the results, such as in memory device 76, in order to expedite the subsequent processing. Alternatively, the apparatus 50 can perform the operations of step 1 in line and immediately preceding the operations of step 2 so as to avoid storing the results.

In the first step, \( \lambda \) and \( n \) may be provided whereby \( 0 < \lambda < n \). As noted above, \( n \) represents the number of points on the elliptic curve and \( \lambda \) is the solution modulo \( n \) to a characteristic polynomial of an endomorphism which acts as multiplication by \( \lambda \) on an elliptic curve. As shown in operation 100, the extended Euclidean algorithm may then be run for the integers \( n \) and \( \lambda \) in order to find their greatest common divisor. The extended Euclidean algorithm may produce a sequence of quotients and a corresponding sequence of remainders by initially dividing \( n \) by \( \lambda \) to produce a quotient and a remainder and then repeatedly dividing the divisor from the prior iteration by the remainder from the prior iteration. As a result of this repeated division, a sequence of positive quotients \( q_1, q_2, \ldots, q_m \) are generated. In addition, a decreasing sequence of positive remainders \( r_1, r_2, \ldots, r_m \) where \( r_0 = n \) and \( r_1 = \lambda \) are generated as follows

\[
r_{i+1} = q_ir_i + r_{i+1}, \quad i = 1, \ldots, m.
\]

wherein \( m \) is an arbitrary fixed positive integer. Additionally, as shown in operation 102, a sequence of integers \( t_i \) wherein \( i = 1, 2, \ldots, n+1 \) is generated as follows:

\[
t_{i+1} = t_i - q_it_i, \quad \text{and}
\]

\[
V \equiv t_i \lambda \quad (\text{mod } n), \quad \text{for all } i = 1, \ldots, m.
\]

As such, \( t_0 = 0 \), \( t_1 = 1 \), and \( t_i < 0 \), for \( i \) even, and \( t_i > 0 \), for \( i \) odd.

Based upon these sequences, the number of points on the elliptic curve \( n \) can be expressed in a number of different manners. For example, \( n = k_2|T_i + |T_2, n = k_3|T_2 + k_2|T_3, \) and \( n = k_4|T_3 + k_3|T_4, \) where \( |\cdot | \) denotes the absolute value of integer \( t \), and more generally, for any fixed positive integer \( m \) it holds that \( n = v_{m+\sqrt{r_m + v_{m+\sqrt{r_m}}}} \). The sequence of remainders is then reviewed in order to determine two sequential values, such as \( r_m \) and \( r_{m+1} \) which are both close to the square root of \( n \). The expression for \( n \) that relies upon these two sequential values in the sequence of remainders which are close to the square root \( \sqrt{n} \) is then determined, that is, \( n = \)
In the foregoing equation, $t_m$ and $t_{m+1}$ are also sequential values from the sequence of integers $t$, such that $t_m$ and $t_{m+1}$ are also close in value to the square root of $\lambda$. In one embodiment, the various possibilities for $r_m, r_{m+1}, t_m$ and $t_{m+1}$ may be considered with those values selected that allow all of these conditions ($r_m, r_{m+1}$ and the sum of $t_m$ and $t_{m+1}$ to be close to the square root of $\lambda$) to be as close to being satisfied as possible.

Regardless of the value of the previously unknown integer $k$, the results of this first step provide bounds for the two integers $k_1$ and $k_2$ into which $k$ may be decomposed. In this regard, $k_1$ is a positive integer that is less than $r_m$, while $k_2$ is an integer between $-\sqrt{n}$ and $|t_m| + |t_{m+1}|$. As a result, the largest possible values of $k_1$ and $|k_2|$ are close to the square root of $\lambda$.

Additionally, $k_1$ and $|k_2|$ may also have about the same value, that is both $k_1$ and $|k_2|$ may be close to the square root of $\lambda$.

Thereafter, once $k$ is provided such that $0 < k < n$, the apparatus 50 and, more typically, the processor 70 repeatedly divides $k$ by the sequence of remainders. In this regard, $k$ is initially divided by $r_i$. The remainder from this division is then divided by $r_2$. The remainder from this second division is then divided by $r_3$. This process is repeated at least until $r_m$ is employed as the divisor. See operations 104, 106, 108, 110 and 112. The remainder from the division by $r_m$ is then taken as $k_1$. See operation 114. As such, $k_1$ is nonnegative and necessarily less than $r_m$.

The apparatus 50 and, more particularly, the processor 70 are also configured to determine $k_2$ as shown at operation 116. $k_2$ can be determined in various manners including, for example, one technique which makes use of the quotients from the subsequent divisions. In this regard, $a_i$ is defined to be the quotient when $k$ is divided by $r_i$. Likewise, $a_2$ is defined to be the quotient when the remainder from the first division, that is, the division in which $r_i$ is the divisor, is divided by $r_2$. This process is repeated for $r_i = 1, 2 \ldots m$ to thereby define quotients $a_1, a_2, \ldots a_m$, respectively, whereby $a_m$ is the quotient from the division operation in which $r_m$ is the divisor. As such, $k_2$ may be determined as a sum of $a_1 + a_2 - t_2 + a_3 - t_3 + \ldots + a_m - t_m$. As will be noted, the absolute value of $k_2$ is therefore always less than the bound determined in step 1 of $|t_m| + |t_{m+1}|$.

Alternatively, $k_2$ may be determined by subtracting $k_1$ from $k$ and then multiplying the result by the inverse of $\lambda$ modulo $n$. In this regard, the inverse of $\lambda$ may be determined by running the extended Euclidean algorithm with the integers $n$ and $\lambda$ until the remainder is equal to 1 with the inverse of $\lambda$ then equaling the corresponding value from the sequence of values, that is, the $t$ value that corresponds to the remainder being equal to 1.
Based upon the values of $k_1$ and $k_2$, the multiplication of a point $P$ on an elliptic curve by $k$ can be equivalently and more efficiently computed by multiplication of the point on the elliptic curve by $k_1$ added to the multiplication of the point on the curve by $\lambda$ multiplied by $k_2$, that is, $kP = k_1P + (k_2\lambda)P$. Based upon the multiplication of the point on the elliptic curve by $k$, messages, such as messages transmitted between mobile terminal 10 and the second communications device 20, can be subjected to elliptic curve cryptography in order to provide the desired security.

As described above, Figure 3 is a flowchart of a system, method and program product according to some exemplary embodiments of the invention. It will be understood that each block or step of the flowchart, and combinations of blocks in the flowchart, can be implemented by various means, such as hardware, firmware, and/or software including one or more computer program instructions. For example, one or more of the procedures described above may be embodied by computer program instructions. In this regard, the computer program instructions which embody the procedures described above may be stored by a memory device of a mobile terminal or other apparatus employing embodiments of the present invention and executed by a processor in the mobile terminal or other apparatus. As will be appreciated, any such computer program instructions may be loaded onto a computer or other programmable apparatus (e.g., hardware) to produce a machine, such that the instructions which execute on the computer (e.g., via a processor) or other programmable apparatus create means for implementing the functions specified in the flowchart block(s) or step(s). These computer program instructions may also be stored in a computer-readable memory that can direct a computer (e.g., the processor or another computing device) or other programmable apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block(s) or step(s). The computer program instructions may also be loaded onto a computer or other programmable apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block(s) or step(s).

Accordingly, blocks or steps of the flowchart support combinations of means for performing the specified functions, combinations of steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that one or more blocks or steps of the flowchart, and combinations of blocks or steps in the
flowchart, can be implemented by special purpose hardware-based computer systems which perform the specified functions or steps, or combinations of special purpose hardware and computer instructions.

[0039] In an exemplary embodiment, an apparatus for performing the method of Figure 3 above may comprise a processor (e.g., the processor 70) configured to perform some or each of the operations (100-1 16) described above. The processor may, for example, be configured to perform the operations (100-1 16) by performing hardware implemented logical functions, executing stored instructions, or executing algorithms for performing each of the operations. Alternatively, the apparatus may comprise means for performing each of the operations described above. In this regard, according to an example embodiment, examples of means for performing operations 100-1 16 may comprise, for example, the processor 70 and/or an algorithm executed by the processor for bounding and determining k1 and k2 described above.

[0040] Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these inventions pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Moreover, although the foregoing descriptions and the associated drawings describe exemplary embodiments in the context of certain exemplary combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative embodiments without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.
WHAT IS CLAIMED IS:

1. An apparatus comprising at least one processor and at least one memory including 
computer program code, the at least one memory and the computer program code configured to, 
with the processor, cause the apparatus to at least perform: 
decomposing an integer k into integers k1 and k2; 
determining respective bounds for the integers k1 and k2; and 
determining the integers k1 and k2 subject to the respective bounds such that a product of 
the integer k and a point P on an elliptic curve is determinable based upon the integers k1 and k2.

2. An apparatus according to Claim 1 wherein the computer program code is further 
configured to cause the apparatus to determine the product of the integer k and the point P on the 
elliptic curve by summing a product of the integer k1 and the point P and a product of the point P, 
the integer k2 and a multiplier λ.

3. An apparatus according to Claim 1 wherein the computer program code is further 
configured to cause the apparatus to determine respective bounds for the integers k1 and k2 by 
applying an extended Euclidean algorithm for a number of points n on an elliptic curve and a 
multiplier λ to generate sequences of quotients and remainders r\(_1\), r\(_2\), ..., r\(_m\), r\(_{m+1}\), ..., and by 
determining the r\(_m\) remainder to bound the integer k1 based upon a relationship of the r\(_m\) 
remainder to n.

4. An apparatus according to Claim 3 wherein the computer program code is further 
configured to cause the apparatus to determine respective bounds for the integers k1 and k2 by 
determining a sequence of integers t\(_1\), t\(_2\), .. based upon the sequence of quotients and by defining 
the bound for the integer k2 based upon a relationship of at least two of the integers t to n.

5. An apparatus according to Claim 3 wherein the computer program code is further 
configured to cause the apparatus to determine the integer k1 by: 
dividing k by r\(_i\) to produce a quotient a\(_i\) and a reminder; 
for each i=2, 3, .. m, dividing the remainder from a prior division by r\(_{i+1}\) by X\(_i\)to produce a 
quotient a\(_i\) and a remainder; and
defining the integer $k_1$ to equal the remainder from the prior division by $r_m$.

6. An apparatus according to Claim 5 wherein the computer program code is further configured to cause the apparatus to determine the integer $k_2$ by:
   - determining a sequence of integers $t_1, t_2, \ldots$ based upon the sequence of quotients; and
   - defining the integer $k_2$ to be a sum of $a_i t_i + a_2 t_2 + \ldots + a_m t_m$.

7. An apparatus according to Claim 3 wherein the computer program code is further configured to cause the apparatus to determine the integer $k_2$ by determining a result of reducing $k$ by $k_1$ and then multiplying the result by an inverse of $\lambda$ modulo $n$.

8. A method comprising:
   - decomposing an integer $k$ into integers $k_1$ and $k_2$;
   - determining respective bounds for the integers $k_1$ and $k_2$; and
   - determining, via a processor, the integers $k_1$ and $k_2$ subject to the respective bounds such that a product of the integer $k$ and a point $P$ on an elliptic curve is determinable based upon the integers $k_1$ and $k_2$.

9. A method according to Claim 8 further comprising determining the product of the integer $k$ and the point $P$ on the elliptic curve by summing a product of the integer $k_1$ and the point $P$ and a product of the point $P$, the integer $k_2$ and a multiplier $\lambda$.

10. A method according to Claim 8 wherein determining respective bounds for the integers $k_1$ and $k_2$ comprises:
   - applying an extended Euclidean algorithm for a number of points $n$ on an elliptic curve and a multiplier $\lambda$ to generate sequences of quotients and remainders $r_1, r_2, \ldots, r_m, r_{m+1}, \ldots$; and
   - determining the $r_m$ remainder to bound the integer $k_1$ based upon a relationship of the $r_m$ remainder to $n$.

11. A method according to Claim 10 wherein determining respective bounds for the integers $k_1$ and $k_2$ comprises:
   - determining a sequence of integers $t_1, t_2, \ldots$ based upon the sequence of quotients; and
defining the bound for the integer \( k_2 \) based upon a relationship of at least two of the integers \( t \) to \( n \).

12. A method according to Claim 10 wherein determining the integer \( k_1 \) comprises:
   dividing \( k \) by \( r_1 \) to produce a quotient \( a_1 \) and a reminder;
   for each \( i=2, 3, \ldots m \), dividing the remainder from a prior division by \( r_{i-1} \) by \( X_i \) to produce a quotient \( a_i \) and a remainder; and
   defining the integer \( k_1 \) to equal the remainder from the prior division by \( r_m \).

13. A method according to Claim 12 wherein determining the integer \( k_2 \) comprises:
   determining a sequence of integers \( t_1, t_2, \ldots \) based upon the sequence of quotients; and
   defining the integer \( k_2 \) to be a sum of \( a_1 t_1 + a_2 t_2 + \ldots + a_m t_m \).

14. A method according to Claim 10 wherein determining the integer \( k_2 \) comprises:
   determining a result of reducing \( k \) by \( k_1 \) and then multiplying the result by an inverse of \( \lambda \) modulo \( n \).

15. A computer program product comprising a computer-readable storage medium bearing computer program code embodied therein for use with a computer, the computer program code comprising:
   code configured to decompose an integer \( k \) into integers \( k_1 \) and \( k_2 \);
   code configured to determine respective bounds for the integers \( k_1 \) and \( k_2 \); and
   code configured to determine the integers \( k_1 \) and \( k_2 \) subject to the respective bounds such that a product of the integer \( k \) and a point \( P \) on an elliptic curve is determinable based upon the integers \( k_1 \) and \( k_2 \).

16. A computer program product according to Claim 15 wherein the computer program code further comprises code configured to determine the product of the integer \( k \) and the point \( P \) on the elliptic curve by summing a product of the integer \( k_1 \) and the point \( P \) and a product of the point \( P \), the integer \( k_2 \) and a multiplier \( \lambda \).

17. A computer program product according to Claim 15 wherein the code configured to determine respective bounds for the integers \( k_1 \) and \( k_2 \) further comprises:
code configured to apply an extended Euclidean algorithm for a number of points on an elliptic curve and a multiplier λ to generate sequences of quotients and remainders \( r_1, r_2, \ldots, r_m, r_{m+1}, \ldots \); and

code configured to determine the \( r_m \) remainder to bound the integer \( k_1 \) based upon a relationship of the \( r_m \) remainder to \( n \).

18. A computer program product according to Claim 17 wherein the code configured to determine respective bounds for the integers \( k_1 \) and \( k_2 \) further comprises:

code configured to determine a sequence of integers \( t_1, t_2, \ldots \) based upon the sequence of quotients; and

code configured to define the bound for the integer \( k_2 \) based upon a relationship of at least two of the integers \( t \) to \( n \).

19. A computer program product according to Claim 17 wherein the code configured to determine the integer \( k_1 \) further comprises:

code configured to divide \( k \) by \( r \) to produce a quotient \( a_i \) and a remainder; for each \( i = 2, 3, \ldots, m \), code configured to divide the remainder from a prior division by \( r_{i-1} \) by \( T_i \) to produce a quotient \( a_i \) and a remainder; and

code configured to define the integer \( k_1 \) to equal the remainder from the prior division by \( r_m \).

20. A computer program product according to Claim 19 wherein the code configured to determine the integer \( k_2 \) further comprises:

code configured to determine a sequence of integers \( t_1, t_2, \ldots \) based upon the sequence of quotients; and

code configured to define the integer \( k_2 \) to be a sum of \( a_1 t_1 + a_2 t_2 + \ldots + a_m t_m \).
FIG. 2
Run the Extended Euclidean algorithm for \( n \) and \( l \) to generate sequences of quotients and remainders \( r_1, r_2, \ldots \).

Determine a sequence of integers \( t_0, t_1, t_2, \ldots \) from the quotients.

Set \( i = 1 \).

Divide \( k \) by \( r_i \) to produce a quotient \( a_i \) and a remainder.

Divide the remainder from the division by \( r_{i-1} \) by \( r_i \).

Set \( k_1 \) equal to the remainder from the division by \( r_m \).

Determine \( k_2 \).

FIG. 3
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, XPAIP, XPESP, XPIEE, XPIETF, XPIPOM, XPI3E, XPMISC, XPRD, COMPDX, INSPEC

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>


Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

**Date of the actual completion of the international search**

23 December 2009 (23.12.2009)

**Date of mailing of the international search report**

29 December 2009 (29.12.2009)

**Name and mailing address of the ISA/FI**

National Board of Patents and Registration of Finland

P O Box 1160, FI-00101 HELSINKI, Finland

**Facsimile No.** +358 9 6939 5328

**Authorized officer**

Vesa-Matti Louekoski

**Telephone No.** +358 9 6939 500

Form PCT/ISA/210 (second sheet) (July 2008)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISBN: 978-3-540-00622-0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOI: 10.1007/3-540-36492-7_2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract; sections 2.1, 2.2, 3.2, 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISBN: 978-3-540-00622-0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOI: 10.1007/3-540-36492-7_3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract; sections 1, 2.1, 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISBN: 978-3-540-42456-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOI: 10.1007/3-540-44647-8_1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>section 4</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>EP 1141820 B1 (CERTICOM CORP) 06 November 2002 (06.1.2002)</td>
<td>1-20</td>
</tr>
<tr>
<td></td>
<td>whole document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISBN: 978-3-642-02383-5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOI: 10.1007/978-3-642-02384-2_24, sections 1-3</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family members(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002057796 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002044649 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2002533787T T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69903854T T2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0039668 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2353395 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 1851500 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2257008 A1</td>
</tr>
<tr>
<td>Classification of Subject Matter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Int.Cl.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G06F 7/72 (2006.01)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H04L 9/30 (2006.01)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G06F 21/00 (2006.01)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>