(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101378321 B
(45)授权公告日 2011.09.28

(21)申请号 200810223369.3

(22)申请日 2008.09.26

(73)专利权人 北京数字太和科技有限责任公司
地址 100083 北京市海淀区花园路2号牡丹创业楼三层

(72)发明人 王兴军 陈晨 雷大明 闫峰冰 胡坚珉 梅红兵

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 宋志强 麻海明

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 1297635 A,2001.05.30, 全文.
WO 2005/034421 A3,2005.04.14, 全文.
CN 1885767 A,2006.12.27, 说明书第2页第24行-第3页第2行.

审查员 陈文军

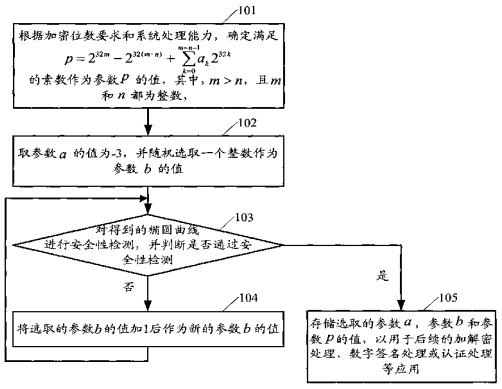
权利要求书 2 页 说明书 10 页 附图 2 页

(54)发明名称

一种安全处理的方法和装置

(57)摘要

本发明提供了一种安全处理的方法和装置，其中，方法包括：A、在椭圆曲线的有限域内确定满足多项式 $p=2^{hm}-2^{h(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{hk}$ 的素数作为参数p，其中，h为安全处理系统的处理位数，hm满足安全处理的加密位数要求，m>n，且m、n和k都为整数，$a_k \in \{-1,0,1\}$；B、利用确定的参数p确定椭圆曲线 $y^2=x^3+ax+b \bmod p$ 中的参数a和参数b；C、利用确定出的椭圆曲线参数进行数据安全处理。采用本发明提供的方法和装置能够获取到满足加密位数要求和安全性要求的椭圆曲线参数，并且提高了效率，减少了占用的系统资源，使得基于椭圆曲线参数的安全处理过程更加高效。



CN 101378321 B

1. 一种安全处理的方法，其特征在于，该方法包括：

A、在椭圆曲线的有限域内确定满足多项式$p=2^{hm}-2^{h(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{hk}$的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，m ＞ n，且 m、n 和 k 都为整数，$a_k \in \{-1,0,1\}$；

B1、确定参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值；

B2、利用确定的参数 a、参数 b 和参数 p 的值对对应的椭圆曲线 $y^2 = x^3+ax+b \bmod p$ 进行安全性检测，并判断是否通过安全性检测，如果是，则执行步骤 B4，否则，执行步骤 B3；

B3、选取另外一个整数作为参数 b 的值，转至执行步骤 B2；

B4、存储确定出的椭圆曲线参数 a、参数 b 和参数 p 的值；

C、利用确定出的椭圆曲线参数 a、参数 b 和参数 p 的值进行数据安全处理。

2. 根据权利要求 1 所述的方法，其特征在于，步骤 A 中所述确定满足多项式$p=2^{hm}-2^{h(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{hk}$的素数作为参数 p 的值包括：在确定满足多项式$p=2^{hm}-2^{h(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{hk}$的素数中，选择使得所述多项式中非零项最少的素数作为确定的参数 p 的值。

3. 根据权利要求 1 所述的方法，其特征在于，步骤 B3 中所述选取另外一个整数作为参数 b 具体包括：随机选取另外一个整数作为参数 b 的值；或者，对参数 b 的值进行加 1 或者减 1 处理后作为当前参数 b 的值。

4. 根据权利要求 1 所述的方法，其特征在于，所述数据安全处理具体包括：数据加解密处理、数字签名验证处理或数据认证处理。

5. 一种安全处理的装置，其特征在于，该装置包括：

第一参数确定单元，用于在椭圆曲线的有限域内确定满足多项式$p=2^{hm}-2^{h(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{hk}$的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，m ＞ n，且 m、n 和 k 都为整数，$a_k \in \{-1,0,1\}$；

包含第三参数确定子单元和安全检测子单元的第二参数确定单元，其中，

所述第三参数确定子单元，用于确定参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值；接收到重选通知后，选取另一个整数作为参数 b 的值；

所述安全检测子单元，用于利用所述第一参数确定单元和第三参数确定子单元确定的参数 a、参数 b 和参数 p 的值对对应的椭圆曲线 $y^2 = x^3+ax+b \bmod p$ 进行安全性检测，并判断是否通过安全性检测，如果是，则将确定出的参数 a、参数 b 和参数 p 的值发送给参数存储单元，否则，向所述第三参数选取子单元发送重选通知；

参数存储单元，用于存储所述安全检测子单元发送来的参数 a、参数 b 和参数 p 的值；

安全处理单元，用于从所述参数存储单元中获取参数 a、参数 b 和参数 p 的值以进行数据安全处理。

6. 根据权利要求 5 所述的装置，其特征在于，所述第一参数确定单元包括：

第一参数确定子单元，用于确定满足所述多项式$p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$的素数；

第二参数确定子单元，用于在所述第一参数确定子单元确定的素数中选择使得所述多项式中非零项最少的素数作为确定的参数 p 的值。

7. 根据权利要求 5 所述的装置，其特征在于，所述安全处理单元包括：加密子单元、解密子单元、数字签名验证子单元和数据认证子单元中的一种或任意组合。

一种安全处理的方法和装置

技术领域

[0001] 本发明涉及网络安全技术，特别涉及一种密码验证的方法和装置。

背景技术

[0002] 随着网络技术的不断发展，如何提高网络安全性成为越来越关注的问题，各种密钥算法应运而生。密钥算法主要分为：对称算法（symmetric algorithm）和公开密钥算法（public-key algorithm），在公开密钥算法中，目前应用比较广泛的是安全性较高的基于椭圆曲线参数的算法，即诸如加密解密、数字签名的验证等安全处理方式都基于椭圆曲线进行，该算法中椭圆曲线参数的选取对于保证密码验证处理的安全高效非常重要。

[0003] 在基于椭圆曲线参数的算法中采用的有限域上的椭圆曲线形式为：$y^2 = x^3+ax+b \bmod p$，其中，参数的选取主要是针对参数 p、a 和 b 的选取。现有技术的参数选取方法主要为：随机选取满足加密位数要求的素数作为参数 p 的值，在选取参数 p 的基础上以及在固定的参数 a 值为 -3 的前提下，随机选取使椭圆曲线满足安全性要求的参数 b 的值。由于在该算法中参数 p 的值是随机选取的，因此，在后续处理中对参数 p 进行取模运算时只能够使用除法运算，显然非常占用安全处理系统的资源，且无论在软件还是硬件的实现上效率都比较低。

发明内容

[0004] 有鉴于此，本发明实施例提供了一种安全处理的方法和装置，以便于使得基于椭圆曲线参数的安全处理过程更加高效。

[0005] 一种安全处理的方法，该方法包括：

[0006] A、在椭圆曲线的有限域内确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，m > n，且 m、n 和 k 都为整数，$a_k \in \{-1,0,1\}$；

[0007] B1、确定参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值；

[0008] B2、利用确定的参数 a、参数 b 和参数 p 的值对对应的椭圆曲线 $y^2 = x^3+ax+b \bmod p$ 进行安全性检测，并判断是否通过安全性检测，如果是，则执行步骤 B4，否则，执行步骤 B3；

[0009] B3、选取另外一个整数作为参数 b 的值，转至执行步骤 B2；

[0010] B4、存储确定出的椭圆曲线参数 a、参数 b 和参数 p 的值；

[0011] C、利用确定出的椭圆曲线参数 a、参数 b 和参数 p 的值进行数据安全处理。

[0012] 一种安全处理的装置，该装置包括：

[0013] 第一参数确定单元，用于在椭圆曲线的有限域内确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，m > n，且 m、n 和 k 都为整数，$a_k \in \{-1,0,1\}$；

[0014] 包含第三参数确定子单元和安全检测子单元的第二参数确定单元，其中，

[0015] 所述第三参数确定子单元，用于确定参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值；接收到重选通知后，选取另一个整数作为参数 b 的值；

[0016] 所述安全检测子单元，用于利用所述第一参数确定单元和第三参数确定子单元确定的参数 a、参数 b 和参数 p 的值对对应的椭圆曲线 $y^2 = x^3+ax+b \bmod p$ 进行安全性检测，并判断是否通过安全性检测，如果是，则将确定出的参数 a、参数 b 和参数 p 的值发送给参数存储单元，否则，向所述第三参数选取子单元发送重选通知；

[0017] 参数存储单元，用于存储所述安全检测子单元发送来的参数 a、参数 b 和参数 p 的值；

[0018] 安全处理单元，用于从所述参数存储单元中获取参数 a、参数 b 和参数 p 的值以进行数据安全处理。

[0019] 由以上技术方案可以看出，在本发明提供的方法和装置中，在椭圆曲线的有限域内确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，$m > n$，且 m、n 和 k 都为整数，$a_k \in \{-1,0,1\}$；利用确定的参数 p 的值确定椭圆曲线 $y^2 = x^3+ax+b \bmod p$ 中的参数 a 和参数 b 的值；利用确定出的椭圆曲线参数进行数据安全处理。采用本发明提供的方法和装置能够获取到满足加密位数要求和安全性要求的椭圆曲线参数，并且椭圆曲线参数 p 的选取方式能够使得对参数 p 的取模运算仅仅通过移位和加减法运算便可以完成，从而提高了效率，减少了占用的系统资源，使得基于椭圆曲线参数的安全处理过程更加高效。

附图说明

[0020] 图 1 为本发明实施例提供的方法流程图；

[0021] 图 2 为本发明实施例提供的装置结构图；

[0022] 图 3 为本发明实施例提供的一个应用系统图

[0023] 图 4 为本发明实施例提供的另一个应用系统图。

具体实施方式

[0024] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

[0025] 本发明提供的方法主要包括：在椭圆曲线的有限域内确定满足 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值；其中，h 为安全处理系统的处理位数，hm 满足安全系统加密位数要求，$m > n$，且 m 和 n 都为整数，$a_k \in \{-1,0,1\}$；利用确定的参数 p 确定其它的椭圆曲线参数，并利用确定的椭圆曲线参数进行数据安全处理。

[0026] 下面结合具体实施例对上述方法进行详细描述，图 1 为本发明实施例提供的方法流程图，如图 1 所示，该方法可以包括以下步骤：

[0027] 步骤 101：根据加密位数要求和系统处理能力，确定满足

$p = 2^{32m} - 2^{32(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{32k}$ 的素数作为参数 p 的值，其中，m > n，且 m 和 n 都为整数，$a_k \in \{-1, 0, 1\}$。

[0028] 该实施例中，系统的处理能力是以 32 位为例进行的描述，上述等式中的各项都是 2^{32} 的整数幂，这有利于在椭圆曲线上运算的软件和硬件实现，由于系统的处理能力都是 32 位，即软件和硬件的处理能力都是 32 位，因此，在这种情况下，后续对于参数 p 的取模运算只需要加减法和移位运算就能完成，加速了处理速度，也节省了占用的资源。在此进行以下简单分析：

[0029] 以 $p = 2^{256}-2^{224}-2^{96}+2^{64}-1$ 为例，对该 p 进行的取模运算。

[0030] 定义运算准则 $(x_k, x_{k-1}, \cdots, x_{k-n}) = x_k(2^{32})^n + x_{k-1}(2^{32})^{n-1} + \cdots + x_{k-n}$，以 x 为一个 512 位的数为例，按照上述定义的准则，该 512 位的 x 可以表示为 $x = (x_{15}, x_{14}, \cdots, x_1, x_0) = x_{15}*(2^{32})^{15} + x_{14}*(2^{32})^{14} + \cdots + x_1*2^{32} + x_0$，其中 x_k 的字长为 32 位。

[0031] 则 x mod p 运算存在着以下的快速算法：

[0032] 由于 $p = 2^{256}-2^{224}-2^{96}+2^{64}-1$ 时存在 $2^{256} = (2^{224}+2^{96}-2^{64}+1) \bmod p$，因此

[0033] $x \bmod p = [(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) + 2^{256} \times (x_{15}, x_{14}, x_{13}, x_{12}, x_{11}, x_{10}, x_9, x_8)] \bmod p = [(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) + (2^{224}+2^{96}-2^{64}+1)(x_{15}, x_{14}, x_{13}, x_{12}, x_{11}, x_{10}, x_9, x_8)] \bmod p = \{(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0) + (x_{15}, x_{14}, x_{13}, x_{12}, x_{11}, x_{10}, x_9, x_8) - (x_{13}, x_{12}, x_{11}, x_{10}, x_9, x_8, 0, 0) + (x_{12}, x_{11}, x_{10}, x_9, x_8, 0, 0, 0) + (x_8, 0, 0, 0, 0, 0, 0, 0) + 2^{256} \times [(0, x_{15}, x_{14}, x_{13}, x_{12}, x_{11}, x_{10}, x_9) + (0, 0, 0, 0, 0, x_{15}, x_{14}, x_{13}) - (0, 0, 0, 0, 0, 0, x_{15}, x_{14})]\} \bmod p$

[0034] 进一步地，2^{256} 可以用 $2^{256} = (2^{224}+2^{96}-2^{64}+1) \bmod p$ 继续代换，后续运算不再继续赘述，由此已经可见采用本发明提供的方式确定参数 p 时，取模运算仅仅通过移位和加减法运算便可以完成。

[0035] 在参数 p 的确定过程中，m 值的具体选取和加密位数要求相关，如果加密位数要求为 Q 位，则需要保证 32m = Q，并且，由于上述等式中的第二项即 $2^{32(m-n)}$ 的系数为 -1，这就能保证参数 p 的长度为 32m，从而保证加密位数要求。

[0036] 更优地，在确定参数 p 时，除了满足上述等式的条件之外，还可以进一步使之满足该参数 p 的汉明表示中汉明重量最小，即将满足上述等式的各参数 p 中其汉明表示的汉明重量最小的作为确定的参数 p 的值。其中，参数 p 的汉明表示为：，例如，如果 p 的值取 $2^{256}-2^{224}+2^{192}+2^{96}-1$，则其汉明表示为 (1,1,1,0,0,1,0,0,1)，其中每一个值对应多项式中的该项是否为非零项，1 代表为非零项，0 代表为零项。该汉明表示的汉明重量为 5，即该表示 p 的多项式中非零项的个数。取汉明重量最小的值作为参数 p 的值，可以尽可能的减少后续进行取模运算时的移位次数。

[0037] 步骤 102：取参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值。

[0038] 根据以往的经验，取参数 a 的值为 -3 可以使得椭圆曲线上的倍点运算存在快速算法，参数 a 的该种选择已经是现有技术，在此，不再对参数 a 的选择进行详细论述。

[0039] 步骤 103：利用选取的参数 a、参数 b 和确定的参数 p 对得到的椭圆曲线进行安全性检测，并判断是否通过安全性检测，如果是，则执行步骤 105，否则，执行步骤 104。

[0040] 在上述步骤中确定了参数 p，并选取了参数 a 和参数 b，此时，这些参数便对应了一条椭圆曲线，将该椭圆曲线进行安全性检测以确定该椭圆曲线是否符合安全性要求。对椭

圆曲线的安全性检测就是检测椭圆曲线是否满足 以下条件：

[0041] 1）该椭圆曲线不是奇异椭圆曲线；

[0042] 2）该椭圆曲线不是反常曲线；

[0043] 3）该椭圆曲线不是畸形曲线，也就是说，该椭圆曲线在有限域上的点个数（表示为 #E）与参数 p 的值不相等，否则将不能抵抗 Smart 攻击。

[0044] 4）该椭圆曲线不是超奇异椭圆曲线；

[0045] 5）#E 不能整除 p^q-1，其中，$1 \leqslant q \leqslant 20$，且 q 为整数；

[0046] 6）#E 的素因子要大于 2^{160}，并且大于 $4\sqrt{p}$，从而保证能够抵抗 Pollard ρ 方法的攻击。

[0047] 满足以上条件的椭圆曲线可以认为是符合安全性要求的椭圆曲线，椭圆曲线的安全性检测已经是现有技术中比较成熟的技术，因此，在此也不再赘述。

[0048] 步骤 104：将选取的参数 b 的值加 1 后作为新的参数 b 的值，转至执行步骤 103。

[0049] 如果在步骤 103 中，椭圆曲线没有通过安全性检测，则可以在选取的参数 b 周围选取一个新的值作为参数 b 的值，将对应的新的椭圆曲线进行安全性检测。除了将选取的参数 b 的值加 1 外，也可以将选取的参数 b 的值减 1 作为新的参数 b 的值。除此之外，本步骤中，也可以重新随机选取一个值作为参数 b 的值。但相比较随机选取，将参数 b 的值加 1 或减 1 后的值作为新的参数 b 的值的选取方式更加高效。

[0050] 步骤 105：存储选取的参数 a、参数 b 和参数 p 的值，以用于后续的加解密处理、数字签名验证处理或认证处理等安全处理的应用。

[0051] 在步骤 105 之后，系统已经选取出一组满足安全性要求的椭圆曲线参数，系统可以结束流程；由于步骤 101 中确定的参数 p 可能是多个，也可以继续在其它参数 p 的基础上进行参数 a 和参数 b 的选取；另外，在一个参数 p 的基础上，对应的满足要求的参数 a 和参数 b 也可能存在多个，因此，也可 以继续转至步骤 102 或者步骤 104 进行进一步的参数选取。

[0052] 下面以 256 位的加密位数要求且系统处理能力是 32 位为例，对上述过程举例进行说明。

[0053] 由于加密位数要求位 256 位，且系统处理能力是 32 位，因此，可以确定 m 值为：$m=\frac{256}{32}=8$。步骤 101 中所述的等式中 n 值可以是任意的小于 m 的整数值，在此，选取 n 为 1。此时，可以按照 $p=2^{256}-2^{224}+\sum_{k=0}^{6}a_k 2^{32k}$，其中 $a_k \in \{-1,0,1\}$ 进行选取，且从中选取汉明表示的汉明重量最小的素数值作为参数 p 的值。按照这个方法，最终满足要求的参数 p 的值存在两个：$p = 2^{256}-2^{224}+2^{192}+2^{96}-1$ 和 $p = 2^{256}-2^{224}-2^{96}+2^{64}-1$。

[0054] 在选取的参数 p 的基础上进一步选取参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值，然后对得到的椭圆曲线进行安全性检测，即按照图 1 所示流程中步骤 102 至步骤 105 所述的操作进行，最终可以得到多组参数值，在此列举几组。需要说明的是，下述参数中的 #E、G_x 和 G_y 都是在确定的参数 p、参数 a 和参数 b 的基础上得来的，其中，G_x 和 G_y 分别是对应的椭圆曲线上的基点的横、纵坐标值，#E、G_x 和 G_y 的计算方法为现有技术，在此不再赘述。

[0055] 当 $p = 2^{256}-2^{224}-2^{96}+2^{64}-1$ 时，我们选取的椭圆曲线参数可以是以下几组：

[0056] p = 1157920892103562487564203452140208927662503539919241914544211939332896849919999

[0057] a = -3

[0058] b = 6214869771149422589067081921460698341020333693753110831627926210140861544102 1

[0059] #E = 1157920892103562487564203452140208927665869610725528975516567560756189004071 37

[0060] G_x = 9015018092434264779075028824074455377502954105970455265735144494156269137942 3

[0061] G_y = 8570474071057249238776485362829263969911253594924544342837187102945018292397 2

[0062] p = 1157920892103562487564203452140208927662503539919241914544211939332896849919999

[0063] a = -3

[0064] b = 9346955949558728744478958129855136089511674431732409140088866431824100553886 8

[0065] #E = 1157920892103562487564203452140208927656867545064474153507998199997157251591 31

[0066] G_x = 8575738301777261296978250742987425255370433363516032838588613204031195480313 4

[0067] G_y = 9217098963063855056309760459344929402548983216729098516450845467038882076111 2

[0068] p = 1157920892103562487564203452140208927662503539919241914544211939332896849919999

[0069] a = -3

[0070] b = 8998332042364153575337358373807830526760167031476510446040482527160265997156

[0071] #E = 1157920892103562487564203452140208927666147750519081571361010974346895056460 99

[0072] G_x = 6111224006538563417967061555890649595552331913374396081137717019086258358 3609922

[0073] G_y = 1059959655581660450918369992915001428849593770696042049016007604537559937563 84

[0074] p = 1157920892103562487564203452140208927662503539919241914544211939332896849919999

[0075] a = -3

[0076] b = 4031919382645721512945612045775220801167357441126949353064988474399265609454 2

[0077] #E = 11579208921035624875642034521402089276621283043691677361213146849528704805134 9

[0078] G_x = 47266626582089733932685852294089808717323978735606844517482615535676582467 42

[0079] G_y = 11144891544896633312903290083850555619468220691093593207804195784435589398 5580

[0080] p = 11579208921035624875642034521402089276625035399192419145442119393328968499199 9

[0081] a = -3

[0082] b = 71640055610550276683574882541696585496586981791062476615259286960825046193023

[0083] #E = 11579208921035624875642034521402089276650333338590653606415259098884429076751 1

[0084] G_x = 79100669128038990215717705122435275106896485099559482383723013293363308332303

[0085] G_y = 13482594605039049602855096018721613449653660827386293993607346353984020201 40

[0086] p = 11579208921035624875642034521402089276625035399192419145442119393328968499199 9

[0087] a = -3

[0088] b = 10296091739464333823769364462564096298150038917085545969986868917765743629019 8

[0089] #E = 11579208921035624875642034521402089276608440137497025127927066211733781791148 3

[0090] G_x = 81695500457571986963013265788160149703094545340747851055773285725159788098365

[0091] G_y = 71955392163809874706547068756317182236715487114502243908418291379435304405380

[0092] p = 11579208921035624875642034521402089276625035399192419145442119393328968499199 9

[0093] a = -3

[0094] b = 18489689941420204368241421700897432613143811885007878745020507386576696749736

[0095] #E = 11579208921035624875642034521402089276622293330635488170731236382351150792746 9

[0096] G_x = 67134630147762612959728495718457344312267068242611025377021915149081883772756

[0097] G_y = 91132882667282454912682238421530748743164368535842684897777563504136038289748

[0098] p = 1157920892103562487564203452140208927662503539919241914544211939332896849919999

[0099] a = -3

[0100] b = 4981055172551326592236018378484181009805721926480086182962990960340908684620 4

[0101] #E = 1157920892103562487564203452140208927656699036971945034251004130064550821557 37

[0102] G_x = 1016618596704726523615356015472464217469023876716584061943471239160489416861 80

[0103] G_y = 4639418272490746040864158882282624174384551500545355928260950064554234314023 6

[0104] 当 p = $2^{256}-2^{224}+2^{192}+2^{96}-1$ 时，我们选取的椭圆曲线参数可以是：

[0105] p = 1157920892103562487626974469494075735300861434152903141955336313088670978539 51

[0106] a = -3

[0107] b = 6214869771149422589067081921460698341020333693753110831627926210140861544148 8

[0108] #E = 1157920892103562487626974469494075735302977536461238536184248843158899782154 97

[0109] G_x = 2922898022192909850622422047110202482161912816742191968962887761090840265067 9

[0110] G_y = 1108021727953010172133874466391340513016756177639242936465912111938691475794 30

[0111] p = 1157920892103562487626974469494075735300861434152903141955336313088670978539 51

[0112] a = -3

[0113] b = 9346955949558728744478958129855136089511674431732409140088866431824100553922 8

[0114] #E = 1157920892103562487626974469494075735304112635944707205411276766142452472390 99

[0115] G_x = 9601675300704280351173058694968634725162874440185868611541103881843101383551 0

[0116] G_y = 1120677649329023338836732903762023399225456870213395246863222921558860322563 2

[0117] p = 1157920892103562487626974469494075735300861434152903141955336313088670978539 51

[0118] a = -3

[0119] b = 8998332042364153575337358373807830526760167031476510446040482527160265996713

[0120] #E = 11579208921035624876269744694940757353030434363541511755560661410068237482342 1

[0121] G_x = 20934799618561647434293277298845216995181248040631260819429040954974867816 89

[0122] G_y = 87989849610661908807035924092732110602724565368268778279929036873562413354 8

[0123] p = 11579208921035624876269744694940757353008614341529031419553363130886709785395 1

[0124] a = -3

[0125] b = 40319193826457215129456120457752208011673574411269493530649884743992656094647

[0126] #E = 11579208921035624876269744694940757352985276391581042783652865798574747532770 7

[0127] G_x = 20170526057273077806392706069727317140544267161463891660993636405865492397414

[0128] G_y = 58376576542545060471950803148659109007415952864596546998720219468516365937330

[0129] p = 11579208921035624876269744694940757353008614341529031419553363130886709785395 1

[0130] a = -3

[0131] b = 71640055610550276683574882541696585496586981791062476615259286960825046192900

[0132] #E = 11579208921035624876269744694940757353027824406663026804483695059888724279702 9

[0133] G_x = 10446493953817552116074252870222272798385625457291197002846329794256298941386 5

[0134] G_y = 41571967263163112873390245640895162451034274154715647533154405775494050000162

[0135] p = 11579208921035624876269744694940757353008614341529031419553363130886709785395 1

[0136] a = -3

[0137] b = 10296091739464333823769364462564096298150038917085545969986868917765743629101 0

[0138] #E = 11579208921035624876269744694940757353023526212423259971568522531616666562242 33

[0139] G_x = 60324055842611589035324258032719970255959019661932612194050338358652486818255

[0140] G_y = 59789957327665548569469896777434623465035462094078504862924896631339070976960

[0141] 可以看出，采用本发明提供的方法能够获取到满足加密位数要求和安全性要求的椭圆曲线参数，并且经过试验证实采用本发明所提供的方法得到椭圆曲线参数的效率更高，占用系统资源更少。

[0142] 以上是对本发明所提供的方法进行的描述，下面对本发明提供的安全处理的装置进行详细描述。图 2 为本发明实施例提供的装置结构图，如图 2 所示，该装置可以包括：第一参数确定单元 200、第二参数确定单元 210 和安全处理单元 220。

[0143] 第一参数确定单元 200，用于在椭圆曲线的有限域内确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，m > n，且 m、n 和 k 都为整数，$a_k \in \{-1, 0, 1\}$。

[0144] 第二参数确定单元 210，用于利用第一参数确定单元 200 确定的参数 p 确定椭圆曲线 $y^2 = x^3 + ax + b \mod p$ 中的参数 a 和参数 b 的值。

[0145] 安全处理单元 220，用于利用第一参数确定单元 200 和第二参数确定单元 210 确定出的椭圆曲线参数 a、参数 b 和参数 p 的值进行数据安全处理。

[0146] 其中，第一参数确定单元 200 具体可以包括：第一参数确定子单元 201 和第二参数确定子单元 202。

[0147] 第一参数确定子单元 201，用于确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数。

[0148] 第二参数确定子单元 202，用于在第一参数确定子单元 201 确定的素数中选择使得多项式中非零项最少的素数作为确定的参数 p 的值。

[0149] 该装置中的第二参数确定单元 210 可以具体包括：第三参数确定子单元 211 和安全检测子单元 212。

[0150] 第三参数确定子单元 211，用于确定参数 a 的值为 -3，并随机选取一个整数作为参数 b 的值；接收到重选通知后，选取另一个整数作为参数 b 的值。

[0151] 安全检测子单元 212，用于利用第一参数确定单元 200 和第三参数确定子单元 211 确定的参数 a、参数 b 和参数 p 的值对对应的椭圆曲线进行安全性检测，并判断是否通过安全性检测，如果是，则将确定的参数 a、参数 b 和参数 p 的值发送给参数存储单元 230，否则，向第三参数选取子单元 211 发送重选通知。

[0152] 上述第三参数确定子单元 211 在选取另外一个整数作为参数 b 时，可以随机选取另外一个整数作为参数 b，或者，对参数 b 的值进行加 1 或者减 1 处理后作为当前参数 b 的值。

[0153] 另外，安全检测子单元 212 在将确定的参数 a、参数 b 和参数 p 的值发送给参数存储单元 230 时，还可以进一步向第三参数选取子单元 211 发送重选通知，继续进行其它组参数的选取。

[0154] 该装置还可以包括：参数存储单元 230，用于存储安全检测子单元发送来的参数 a、参数 b 和参数 p 的值。

[0155] 安全处理单元 220，用于从参数存储子单元 213 中获取参数 a、参数 b 和参数 p 以执行数据安全处理的操作。

[0156] 另外，安全处理单元 220 可以具体包括：加密子单元、解密子单元、数字签名验证子单元和数据认证子单元中的一种或任意组合。

[0157] 图 3 和图 4 是本发明实施例提供的两个应用系统图，如图 3 所示，利用本发明的方法和装置确定出的椭圆曲线参数可以存储在图中的装置 1 和装置 2 的椭圆曲线参数寄存器中，该椭圆曲线参数寄存器相当于图 2 所示装置中的参数存储单元 230，装置 1 和装置 2 之间在进行数据传输时，可以从椭圆曲线参数寄存器中获取相同的一组椭圆曲线参数用于进行数据的加解密处理，假设从装置 1 传输数据到装置 2，则装置 1 的控制器从椭圆曲线参数寄存器中获取一组椭圆曲线参数，并控制加密模块基于该组椭圆曲线参数进行数据的加密处理，将加密后的数据传输给装置 2；装置 2 中控制器从椭圆曲线参数寄存器中获取同一组的椭圆曲线参数，并控制解密模块基于该组椭圆曲线参数对接收到的数据进行解密。反之亦然，从装置 2 到装置 1 的数据传输不再赘述。椭圆曲线参数寄存器中可以存储多组可用的椭圆曲线参数，在使用时，只要保证两端的装置基于相同的椭圆曲线参数即可，当然，也可以在两端的椭圆曲线参数寄存器中只存储同一组椭圆曲线参数，两端的装置仅基于该组椭圆曲线参数进行加解密处理。

[0158] 图 4 是进行数字签名验证的系统图，如图 4 所示，本发明的方法和装置确定出的椭圆曲线参数可以存储在图中的装置 1 和装置 2 的椭圆曲线参数寄存器中，该椭圆曲线参数寄存器相当于图 2 所示装置中的参数存储单元 230。假设装置 1 为签名方，装置 2 为验证方，装置 1 中的控制器从椭圆曲线参数寄存器中获取一组椭圆曲线参数，并控制签名模块基于该组椭圆曲线参数形 成数字签名后发送给装置 2；装置 2 中的控制器从椭圆曲线参数寄存器中获取同一组椭圆曲线参数，并控制验证模块基于该组椭圆曲线参数对接收到的数字签名进行验证。同样，椭圆曲线参数寄存器中可以存储多组可用的椭圆曲线参数，在使用时，只要保证两端的装置基于相同的椭圆曲线参数即可，当然，也可以在两端的椭圆曲线参数寄存器中只存储同一组椭圆曲线参数，两端的装置仅基于该组椭圆曲线参数形成签名和验证签名。

[0159] 由以上描述可以看出，在本发明提供的方法和装置中，在椭圆曲线的有限域内确定满足多项式 $p = 2^{hm} - 2^{h(m-n)} + \sum_{k=0}^{m-n-1} a_k 2^{hk}$ 的素数作为参数 p 的值，其中，h 为安全处理系统的处理位数，hm 满足安全处理的加密位数要求，$m > n$，且 m、n 和 k 都为整数，$a_k \in \{-1, 0, 1\}$；利用确定的参数 p 确定椭圆曲线 $y^2 = x^3+ax+b \mod p$ 中的参数 a 和参数 b 的值；利用确定出的椭圆曲线参数进行数据安全处理。采用本发明提供的方法和装置能够获取到满足加密位数要求和安全性要求的椭圆曲线参数，并且椭圆曲线参数 p 的选取方式能够使得对参数 p 的取模运算仅仅通过移位和加减法运算便可以完成，从而提高了效率，减少了占用的系统资源，使得基于椭圆曲线参数的安全处理过程更加高效。

[0160] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

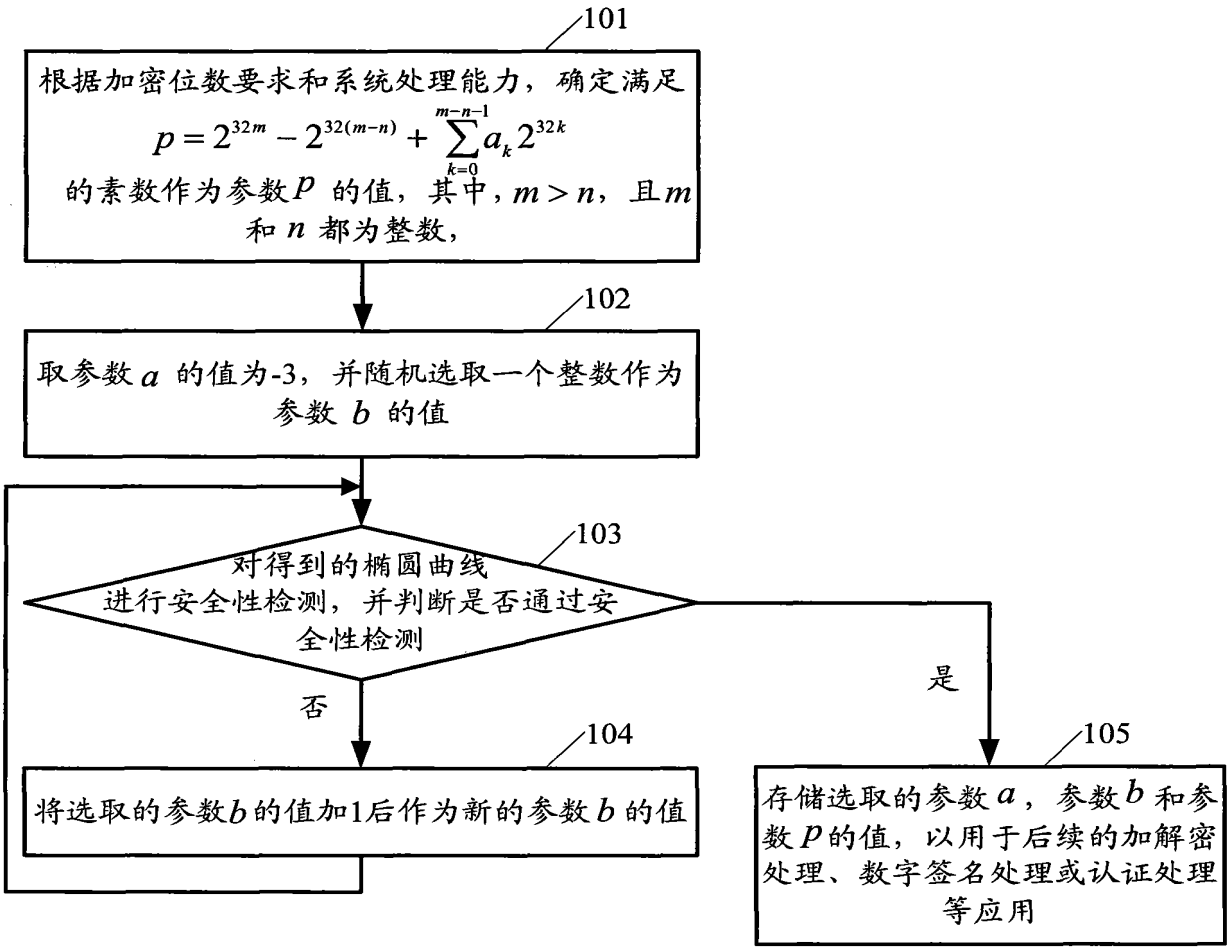

101
根据加密位数要求和系统处理能力，确定满足 $p=2^{32m}-2^{32(m-n)}+\sum_{k=0}^{m-n-1}a_k 2^{32k}$ 的素数作为参数 p 的值，其中，$m>n$，且 m 和 n 都为整数，
102
取参数 a 的值为-3，并随机选取一个整数作为参数 b 的值
103
对得到的椭圆曲线进行安全性检测，并判断是否通过安全性检测
否
是
104
将选取的参数 b 的值加1后作为新的参数 b 的值
105
存储选取的参数 a，参数 b 和参数 p 的值，以用于后续的加解密处理、数字签名处理或认证处理等应用

图 1

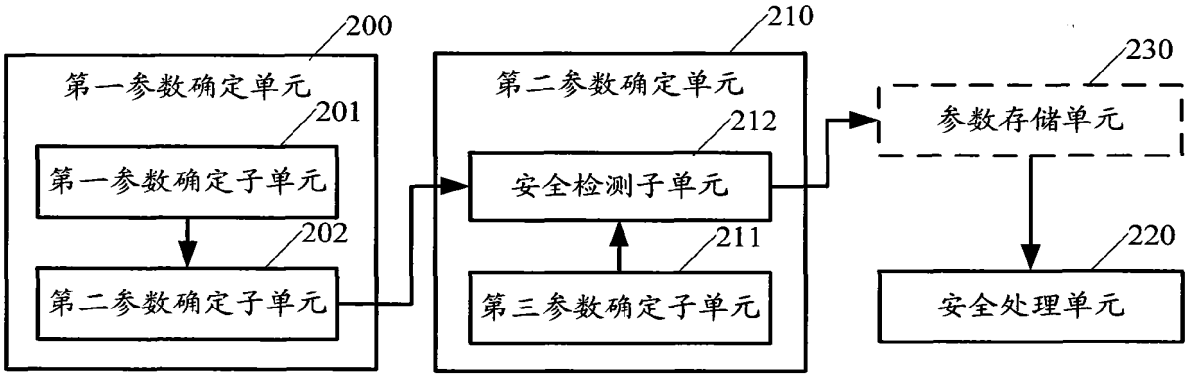

200
第一参数确定单元
201
第一参数确定子单元
202
第二参数确定子单元
210
第二参数确定单元
212
安全检测子单元
211
第三参数确定子单元
230
参数存储单元
220
安全处理单元

图 2

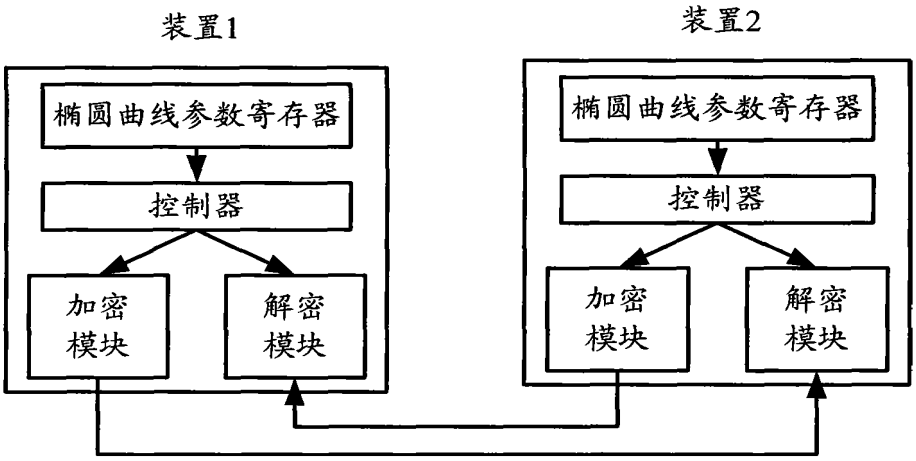

装置1
椭圆曲线参数寄存器
控制器
加密模块
解密模块
装置2
椭圆曲线参数寄存器
控制器
加密模块
解密模块

图 3

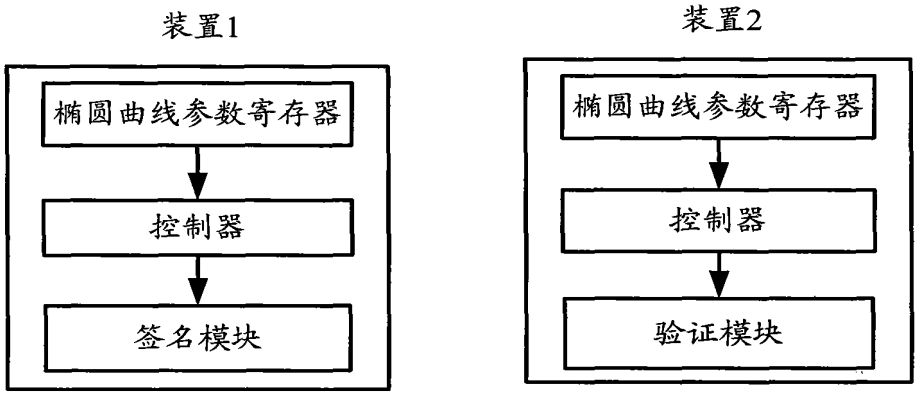

装置1
椭圆曲线参数寄存器
控制器
签名模块
装置2
椭圆曲线参数寄存器
控制器
验证模块

图 4