

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 7/72 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200680031833.8

[43] 公开日 2008 年 8 月 27 日

[11] 公开号 CN 101253473A

[22] 申请日 2006.7.11

[21] 申请号 200680031833.8

[30] 优先权

[32] 2005.8.30 [33] DE [31] 102005041102.9

[86] 国际申请 PCT/EP2006/064099 2006.7.11

[87] 国际公布 WO2007/025796 德 2007.3.8

[85] 进入国家阶段日期 2008.2.29

[71] 申请人 西门子公司

地址 德国慕尼黑

[72] 发明人 B·迈耶 A·卡格尔

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 卢江 刘春元

权利要求书 2 页 说明书 8 页

[54] 发明名称

用于对椭圆弧上的点进行标量乘法的方法

[57] 摘要

一种用于通过特征数 $p > 3$ 的质数体 F_p 的最终扩展体 K 对椭圆弧上的点进行标量乘法的方法, 其中特征数 p 具有很小的汉明加权, 扩展体 K 的多项式的表达式具有级数为 d 的不可约分多项式 $F(x) = X^d - 2$ 。

1. 一种用于通过特征数 $p > 3$ 的质数体 F_p 的最终扩展体 K 对椭圆弧上的点进行标量乘法的方法, 其中该标量乘法在用于对消息加密、对消息解密、由消息产生签名或者对消息进行签名验证计算的密码算法内执行, 其特征在于,

特征数 p 具有汉明加权 ≤ 4 ,

扩展体 K 在多项式的表达式中具有级数为 d 的不可约分多项式 $F(x) = X^d - 2$ 。

2. 根据权利要求 1 所述的方法, 其特征在于, 所述特征数 p 具有为 3 的汉明加权。

3. 根据权利要求 2 所述的方法, 其特征在于, 选择特征数 $p = 2^n \pm 2^m \pm 1$, 其中 n 和 m 是自然数。

4. 根据权利要求 1 至 3 中任一项所述的方法, 其特征在于, 所述不可约分的多项式的级数 d 是质数。

5. 根据权利要求 1 至 4 中任一项所述的方法, 其特征在于, 所述椭圆弧通过 $y^2 = x^3 + ax + b$ 和 $4a^3 + 27b^2 \neq 0$ 给出。

6. 根据权利要求 5 所述的方法, 其特征在于, 所述椭圆弧是 Koblitz 弧。

7. 根据权利要求 6 所述的方法, 其特征在于, 所述标量乘法借助 Frobenius 自同态在标量的幂级数表达中执行。

8. 根据权利要求 7 所述的方法, 其特征在于, 事先计算和存储幂级数的幂。

9. 根据权利要求 1 至 8 中任一项所述的方法, 其特征在于, 将特征数 p 的位长和级数 d 与执行标量乘法的处理器相匹配。

10. 根据权利要求 9 所述的方法, 其特征在于, 这样选择特征数 p 和级数 d , 使得为处理器的总线宽度提供的算术运算可直接用于标量乘法。

11. 根据权利要求 9 或 10 所述的方法, 其特征在于, 这样选择特征数 p 和级数 d , 使得通过扩展体的模块化乘法的中间乘积的所有系数都不溢出地存储在处理器的寄存器中。

12. 根据上述权利要求之一所述的方法, 其特征在于, 借助单指

令多数据流扩展指令集并行执行标量乘法的各运算部分。

13. 根据上述权利要求之一所述的方法在非对称密码应用中的采用。

用于对椭圆弧上的点进行标量乘法的方法

技术领域

本发明涉及一种用于对椭圆弧上的点进行标量乘法 (Skalarmultiplikation) 的方法, 尤其是质数体 (Primkörper) F_p 的最终扩展体 K 上的椭圆弧, 其中特征数 $p > 3$ 。

背景技术

在密码技术中, 对称方法和非对称方法是不同的。对称方法仅使用一个秘密密钥, 既用于加密又用于解密。该密钥必须通过安全信道发布给两个通信用户。在非对称方法中使用两个密钥, 一个公共密钥, 一个私有密钥。公共密钥可以发布给所有用户而不会危及数据交换的安全性。因此密钥交换在非对称方法中不像在对称方法中会出现问题。非对称方法的缺点是它比相应的对称方法慢成百上千倍。

椭圆弧从 1985 年以来一直用于非对称加密方法。基于椭圆弧的加密方法的主要优点是, 与其他方法如 RSA 相比可以使用更小的密钥, 但仍能达到相同的安全水平。160 位的密钥长度抵抗攻击的安全性与 RSA 方法中 1024 位密钥的安全性相同。对密钥的每一位, 椭圆弧加密方法都提供目前所有公知方法中最高的安全性。椭圆弧加密方法因此尤其适合于具有极度有限带宽的信道。缺点是, 加密和解密的计算比其他方法费事。因此为了在密码方法中使用, 重要的是最佳地选择密码系统的常数。

假定 K 是特征数 $p > 3$ 的最终体, 而且 $a, b \in K$ 。体 K 上的椭圆弧是等式 $y^2 = x^3 + ax + b$ 和 $4a^3 + 27b^2 \neq 0$ 的零值集合。椭圆弧在引入非最终远程点作为中性元素的情况下是加性组。假定 $G \subset E$ 是具有第一阶的子组。然后每个非平凡点 $P \in G$ 都是 P 的发生器。因此每个点 $Q \in G$ 是标量乘法的结果 $Q = sP$, 其中 $s \in \{0, \dots, \text{ord}(P) - 1\}$ 。如果标量 s 是正整数, 则该标量乘法是一个点 P 自身的 s 次重复相加。

标量乘法目前对于具有特定特性的弧来说是数学上的单向函数。它可以用多项式时间计算, 但是按照目前的现有技术只能颠倒为指数

时间。将标量乘法颠倒到椭圆弧也称为离散的对数问题 (ECDLP)，并且是基于椭圆弧的密码系统的数学基础。目前公知的用于在适用于加密的椭圆弧上计算离散对数的方法具有复杂度 $O(2^{0.5n})$ ，其中 n 是 $G \subset E$ 的级数的二进制长度。为了满足当前的安全要求，建议选择至少一个位长 $n > 160$ 。

一个点 P 的标量乘法通常通过椭圆弧的点的相加和加倍来执行。相加和加倍的计算规则由对体 K 的元素的元素运算组成。为了高效率地执行该标量乘法，需要体 K 中的优化算术运算。

在选择基础体 K 时的最重要因素是所提供的硬件平台的体系结构。如果在硬件平台上提供长数算术运算并且集成了协处理器以加快体 K 中的算术运算，则可以为体 K 采用质数体 (Primkoerper)。具有协处理器和长数算术运算的芯片卡例如可以非常高效率地处理具有位长从 160 位到 600 位的质数的椭圆弧。

相反，在不具有专用计算装置的硬件环境中，如总线宽度仅为 8 位或 16 位而且没有协处理器的嵌入式系统，长数算术运算必须通过相应的软件指令才能执行。因此密码方法必须完全用软件来实现，而且很难或需要很多经验才能优化。

这种用于标量乘法的软件解决方案的效率可以在由硬件提供的优化可能得到利用时显著提高，所述由硬件提供的优化可能例如是 Pentium 4 处理器的 SSE2 单元或者信号处理器的同时相加和相乘。

选择质数体的替换方案是，可以为体 K 选择质数体 F_p 的扩展体。借助二进制长度仅为 20 至 30 位并具有不可约分的级数为 d 的多项式的较小质数 p ，可以构造出更小的体 F_p 。扩展体的体元素在此是系数也是来自体 F_p 、即多项式的多项式。通过这种方式，虽然质数 p 较小但是可以达到较大的有效位数，这样该位数能实现足够高的安全性。因此本发明的多项式算术运算可以与各处理器的总线宽度相匹配，从而在各处理器中提供的算术运算可以最佳地使用并且不需要长数算术运算。在该多项式算术运算中，如在乘以两个 n 位数时需要进行 n^2 次乘法。有利的是在该多项式算术运算中，通过采用专用算法来极大地减少运算的总次数。

为了在两个多项式相乘时又返回到体中，其中该乘法的结果是级数最大为 $2d-2$ 的多项式，必须简化该多项式。一方面在最终体 F_p 中简

化以 p 为模的多项式的系数，另一方面简化以不可约分多项式为模的该多项式本身。

通过精心选择扩展体 F_p ，可以将两种简化的代价降至最小。在此，通过两个主要的特性来表征关于特征数 $p > 3$ 和多项式展开的最大级数为 $d-1$ 的质数体 F_p 的优选扩展体 (OEF)：

1. 质数 p 是以 $p=2^n \pm c$ ，其中 $\log(c) < n/2$ 形式存在的伪 Mersenne 质数。这种特征使得可以快速简化体 F_p 。

2. 存在不可约分的多项式 $F(x) = X^d - w \in F_p[X]$ 。该特性使得可以快速简化多项式环 $F_p[X]$ ，因为待简化的系数可以通过 F_p 中的乘法和加法简化。

最佳的扩展体还可以是类型 1 或类型 2：

类型 1：对于质数 p ， $p=2^n \pm 1$ ，即 $c=1$ 。

类型 2：对于不可约分的多项式 $F(X)$ ， $F(x) = X^d - 2$ ，即 $w=2$ 。

从数学上可以证明，最佳的扩展体是类型 1 或类型 2，但是不能同时拥有两个特性。类型 1 的最佳扩展体使得可以高效率在质数体 F_p 中进行算术运算，而类型 2 的最佳扩展体则可以高效地简化多项式环 $F_p[X]$ 。在两种情况下都不能推断出，在简化 F_p 或简化多项式环 $F_p[X]$ 的过程中必须要用质数体 F_p 的元素进行乘法。

如果体 K 是质数体 F_p ，则可以通过选择专门的质数 p 来加快简化质数体 F_p 的元素的乘积。乘法所需要的运算次数不仅仅取决于两个因子的位数，还取决于因子的表达式的汉明 (Hamming) 加权。数 Z 的汉明加权意思是 Z 的被置位的个数。11101 的汉明加权例如是 4。通过精心选择数的表达式，可以在两个数相乘时节省计算运算次数：数 63 的二进制形式是表达式 111111，其中汉明加权是 6。幂为 2 的乘法通过向左移位来实现，从而在这种情况下总共需要 5 次移位运算和 5 次相加。但是数 63 也可以表示为 $2^6 - 1$ 。在这种表达式中该数的汉明加权重仅为 2，从而可以用 6 个比特位的向左移位和一次减法来进行与 63 的乘法。与此相反，在与数 10 相乘时，虽然位数较少但是也需要两次移位运算和一次加法。一次乘法的开销因此强烈取决于其汉明加权。在 National Institute of Standards and Technology (NIST, USA) 推荐的质数体上的椭圆弧列表中，注意到质数具有汉明加权重为 3 的表达式 $p=2^n \pm 2^m \pm 1$ ，由此实现了高效的简化。

不可约分的多项式 X^d-2 就简化来说具有最佳的形式。该多项式只包含两项, X^d 和一个恒定的加法因子。该因子 2 也是最佳选择的, 因为要简化的系数只需要移动一位就可以与 2 相乘。表达式 $p=2^n\pm 1$ 中的质数就简化来说同样是最佳的, 因为只存在与 2^n 的一个加法项。不幸的是这两种类型无法彼此组合, 从而在选择扩展体时总是需要平衡开销。

通过扩展体定义的椭圆弧的系数 a 和 b 一般是多项式。对于 Koblitz 弧, a 和 b 位于基本体中并且是级数为 0 的多项式。向位于该弧上的点赋予为 p 的幂, 会将该点基于 Frobenius 的同形态在最终体中又映射为相同的弧。如果 a 和 b 是多项式, 则该点被映射到另一个弧。在椭圆弧上的 Frobenius 自同态在自同态环中, 即对于 Koblitz 弧可以表达出涉及 Frobenius 自同态的全部标量, 由此获得非常快速的标量乘法算法。

发明内容

本发明要解决的技术问题在于, 在没有附加的协处理器的标准处理器上用软件高效地通过特征数 $p>3$ 的最终扩展体实现椭圆弧的点的标量乘法。

该技术问题通过一种用于通过特征数 $p>3$ 的质数体 F_p 的最终扩展体 K 对椭圆弧上的点进行标量乘法的方法来解决, 其中该标量乘法在用于对消息加密、对消息解密、由消息产生签名或者对消息进行签名验证计算的密码算法内执行, 而且特征数 p 具有汉明加权 ≤ 4 , 扩展体 K 在多项式的表达式中具有级数为 d 的不可约分多项式 $F(x)=X^d-2$ 。由此该最佳的扩展体是类型 2 的扩展体, 并就多项式环 $F_p[X]$ 的简化来说具有最佳的简化特性。由于最佳的类型 1 扩展体和类型 2 扩展体是彼此排斥的, 因此不能以 $p=2^n\pm 1$ 的形式表达该质数。但是为了实现质数体 F_p 中的高效算术运算, 要求质数 p 具有很小的汉明加权。通过二进制表达式中的很小的汉明加权, 强烈减少了运算的次数, 加快了标量乘法的计算。

根据优选的实施方式, 所述特征数 p 具有为 3 的汉明加权。对于小于 3 的汉明加权获得类型 1 的最佳扩展体。但由于已经选择类型 2 的最佳扩展体, 因此汉明加权不可能小于 3。如果汉明加权为 4 或者更

大，则另外获得对标量乘法的算法的效率产生影响的和项。

根据优选的实施方式，这样选择特征数，使得 $p=2^n \pm 2^m \pm 1$ ，其中 n 和 m 是自然数。如果以这种形式选择特征数，则特征数的汉明加权重为 3。所有运算可以通过比特位置的移位以及加法或减法来高效地实现。

根据优选的实施方式，所述不可约分的多项式的级数 d 是质数。如果 d 是偶数，则存在可以简化该不可约分多项式的二项式。如果级数 d 是质数，则可以防止已知的攻击，这种攻击可能在级数为非质数时出现。

根据优选的实施方式，通过 $y^2 = x^3 + ax + b$ 和 $4a^3 + 27b^2 \neq 0$ 给出椭圆弧。这不会限制本方法用于其它弧。系数 a 和 b 的条件必须得到满足，由此椭圆弧没有单数点，否则就不适用于密码应用。

根据优选的实施方式，椭圆弧是 Koblitz 弧。Koblitz 弧允许借助体 F_p 上的 Frobenius 自同态来实现快速的标量乘法。

根据优选的实施方式，所述标量乘法借助 Frobenius 自同态在标量的幂级数表达中执行。由此标量乘法可以作为较短的标量乘法的和来实现。

根据优选的实施方式，事先计算和存储幂级数的幂。标量乘法算法的效率由此可以进一步提高。

根据优选的实施方式，将特征数 p 的位长和级数 d 与执行标量乘法的处理器相匹配。在字宽为 8 位的处理器中，质数 p 可以包括 5 到 6 位，这可以表示直到 31 的质数。为了实现足够的安全性，不可约分多项式的级数 d 在此必须选择为高于具有更大位长的质数的级数。为了实现具有至少 160 位的体，需要级数 $d = 23$ 或 29 。在字宽为 16 位的处理器中，特征数 p 可以具有 12 到 13 位的位长，不可约分多项式的级数由此可以更小，例如 $d = 11$ 。

根据优选的实施方式，这样选择特征数 p 和级数 d ，使得为处理器的总线宽度提供的算术运算可直接用于标量乘法。通过这种方式可以在进行乘法运算时存储中间结果，而不需要简化特征数 p 。此外不需要实施长数算术运算。

根据优选的实施方式，借助单指令多数据流 (Streaming Single Instruction Multiple Data, SIMD) 扩展指令集 (SSE) 并行执行标量乘法的各运算部分。通过并行处理和利用其他在硬件平台上提供的

优化可能，可以不采用协处理器就剧烈减少所需要的计算时间。

根据本发明，上述方法在非对称密码应用中使用。这种应用可以实现密钥交换、数字签名等，其中计算时间和对硬件的要求都处于用户可接受的水平。

具体实施方式

下面借助实施例详细解释本发明。

为了加快标量乘法的计算，必须对应于现有的硬件平台优化最佳扩展场上的椭圆弧以及场算术运算。这是通过对计算开销的优化来实现的，该计算开销是在最佳的扩展体不满足类型 1 或类型 2 的条件时所必要的。如果选择了类型 2 的最佳扩展体，由此产生的涉及类型 1 的非最佳形式就可以通过精心选择质数 p 得到足够的补偿。相反，如果不可约分的多项式 $F(X)$ 不是最佳的，则意味着更多的计算开销，因为该多项式在计算时更频繁地受到影响，并根据不同的级数 d 而相应地具有很多系数。

因此，为了补偿涉及类型 1 的质数的非最佳形式，作为质数 p 选择二进制表达式具有非常小的汉明加权的数。形式为 $p=2^n \pm 2^m \pm 1$ 的质数具有最小可能的汉明加权、即 3。附加的和项 2^m 不像非最佳简化多项式那样容易影响计算时间。

质数 p 还可以这样选择，使得可以在寄存器中保持尽可能多的中间结果，而不必简化质数 p 。由此可以允许相加性的常数存在而不会对计算时间上造成大的负面影响，因为只需要简化一次就结束。

在实施例中，作为目标平台使用具有 SSE2 单元的 32 位 Pentium 4 处理器。为了不用长数算术运算或协处理器也能实施，将质数 p 的位长选择在 20 到 30 位之间。这与推荐的 160 位的位长相比，减小了 5 到 8 倍。

简化多项式选择为 $F(x)=X^d-w$ ，其中 $d=11$ ， $w=2$ 。质数选择为 $p=2^{29}-2^9+1$ ，其中 $n=29$ ， $m=9$ ， $c=511$ 。质数 p 由此只具有 29 位的位长。

在定义最佳扩展体时简化所需要的与 $c=51$ 的乘法由于汉明加权为 3 而可以非常高效地用快速运算实现逐位的移位、加法和减法。

通过本发明可以找到最佳的扩展体，该最佳扩展体统一了类型 1

和类型 2 的最佳扩展体的优点。质数体 F_p 的元素的乘积的简化以及 F_p 上的多项式环的乘积的简化可以不采用处理器的乘法指令来进行。与相加性的常数 $c=\pm 2^m \pm 1$ 的乘法由于汉明加权较小而可以通过一次移位运算和一次减法或加法来实现。模数 p 的简化可以只通过 4 次移位运算、两次减法和两次加法实现。此外, 运算数的系数的部分乘积的所有中间和在 64 位寄存器中没有溢出地存储起来。模数 p 的简化在计算该乘积的系数结束时只进行一次。

借助 Intel 的 SSE2(流 SIMD 扩展 2)汇编指令集, 可以在 Pentium 4 处理器中并行地通过体 F_p 计算体算术运算的各个部分。单指令多数据 (SIMD) 概念和 128 位寄存器允许同时计算两个分乘积, 如在下面的程序段中展示的。

```
movd xmm0, [edi]      ; 加载操作数a
punpcklqdq xmm0, xmm0 ; 使操作数a加倍
movdqu xmm6, [esi]    ; 加载操作数b和c
pmuludq xmm6, xmm0    ; 计算a × b和a × c
paddq xmm1, xmm6      ; 将a × b和a × c与前面的结果相加
```

下面的程序段利用具有很小汉明加权的表达式 $p=2^{29}-2^9+1$, 以同时简化两个中间结果:

```
movdqa xmm7, xmm1     ; 掩蔽两个较低的29位
pand xmm1, [mask]
psrlq xmm7, 29 ; 将较高的29位向右移位
psubq xmm1, xmm7      ; 相减
psllq xmm7, 9         ; 将较高的9位向左移位
paddq xmm1, xmm7      ; 相加
```

```
movdqa xmm6, xmm1     ; 重复简化步骤
pand xmm1, [mask]
psrlq xmm6, 29
psubq xmm1, xmm6
psllq xmm6, 9
paddq xmm1, xmm6
```

```
mask dd 0xffffffff, 0x00000000, 0xffffffff, 0x00000000
```

借助用于 4 个双字的 SSE2 指令, 甚至可以在 F_p 中的加法和减法时同时计算和简化 4 个系数。

作为椭圆弧, 选择具有以 p 为模的 Koblitz 弧 $y^2 = x^3 + ax + b$, 其中

参数 $a=468383287$, $b=63579974$ 。系数 a 和 b 是随机获得的, 而且级数为 0, 从而为一个点赋予为 p 的幂会将该点又映射为同一弧。通过这种方式可以为非常快速的标量乘法算法采用 Frobenius 自同态。为了进一步加快运算, 为此所需要的数 2 的幂要提前计算并存储在表格中。

最佳的扩展体可以类似地选择用于具有其它总线宽度的硬件平台。质数 p 这样选择, 使得一方面获得类型 2 的最佳简化多项式, 即 X^d-2 , 另一方面质数 p 具有最小的汉明加权, 从而在二进制表达式中具有尽可能少的和项。对于 16 位的处理器, 质数 p 例如具有 11 或 13 位的位长。

通过采用上述的最佳扩展体和精心地选择质数 p , 减少了对椭圆弧上的点计算标量乘法的计算时间, 从而可以更快地执行使用最佳扩展体上的椭圆弧的密码方法。另外, 由于用于标量乘法的方法可以通过相应选择质数的位长而可伸缩, 并由此可以与不同的处理器总线宽度匹配, 因此该方法可用于不同的硬件平台。尤其是在没有长数算数或协处理器的硬件平台中, 可以用很少的计算时间采用基于椭圆弧的非对称方法。