[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 7/72

[12] 发明专利申请公开说明书

[21] 申请号 02820507.3

[43] 公开日 2005 年 1 月 26 日

[11] 公开号 CN 1571952A

[22] 申请日 2002.7.31 [21] 申请号 02820507.3
[30] 优先权
[32] 2001. 8.17 [33] FR [31] 01/10873
[86] 国际申请 PCT/FR2002/002769 2002.7.31
[87] 国际公布 WO2003/017087 法 2003.2.27
[85] 进入国家阶段日期 2004.4.16
[71] 申请人 格姆普拉斯公司
地址 法国热姆诺
[72] 发明人 M·若耶
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 罗 朋

权利要求书 3 页 说明书 12 页 附图 1 页

[54] 发明名称 用于椭圆曲线上的点的通用计算方法

[57] 摘要

本发明提出了一个用于由 Weierstrass 方程定义的椭圆曲线上的点的通用计算方法。按照本发明，可以用完全相同编程的计算装置来执行涉及点的相加的运算和涉及点的加倍的运算。计算装置特别是包括一个中央处理单元(2)和一个与之连接的存储单元(4，6，8)。所述发明可以用于例如芯片卡内的密码计算。

ISSN1008-4274

知识产权出版社出版

1.一种其间对在由一个Weierstrass方程定义的椭圆曲线上的点执行通用计算操作的密码方法，其特征是：用完全相同编程的计算装置执行点的相加运算和点的加倍运算，所述计算装置特别包括一个中央处理单元(2)和一个与之配合的存储器(4，6，8)。

2.一种按照权利要求1所述的方法，其特征是：为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，将第一点P1的仿射坐标和第二点P2的仿射坐标分别存储在存储器(4，6，8)的第一和第二寄存器内，第一点和第二点都属于由以下类型的Weierstrass方程定义的椭圆曲线：

$$Y^2+a1\times X\times Y+a3\times Y=X^3+a2\times X^2+a4\times X+a6$$

(X，Y)为曲线上的点的仿射坐标，而a1、a2、a3、a4、a5、a6为这条椭圆曲线的参数，

所述编程的计算装置用下式计算定义一个作为加法结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2+a1\times\lambda-a2-X1-X2$$

$$Y3=-(\lambda+a1)\times X3-\mu-a3$$

其中：

$$\lambda=(X1^2+X1\times X2+X2^2+a2\times X1+a2\times X2+a4-a1\times Y1)/(Y1+Y2+a1\times X2+a3)$$

$$\mu=Y1-\lambda\times X1$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器(6，8)的第三寄存器内。

3.一种按照权利要求1所述的方法，其特征是：为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，第一点P1的仿射坐标和第二点P3的仿射坐标分别存储在存储器(4，6，8)的第一和第二寄存器内，第一点和第二点

都属于由以下类型的Weierstrass方程定义的在特征数不为2或3的域上的椭圆曲线：

$$Y^2=X^3+a\times X+b$$

(X，Y)为曲线上的点的仿射坐标，而a、b为椭圆曲线的参数，

所述编程的计算装置用下式计算定义一个作为加法结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2-X1-X2$$

$$Y3=\lambda\times(X1-X3)-Y1$$

其中：

$$\lambda=(X1^2+X1\times X2+X2^2+a)/(Y1+Y2)$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器(6，8)的第三寄存器内。

4.一种按照权利要求1所述的方法，其特征是：为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，将第一点P1的仿射坐标和第二点P2的仿射坐标分别存储在存储器(6，8)的第一和第二寄存器内，第一点和第二点都属于由以下类型的简化Weierstrass方程定义的在特征数不为2或3的域上的椭圆曲线：

$$Y^2+XY=X^3+a\times X^2+b$$

(X，Y)为曲线上的点的仿射坐标，而a、b为椭圆曲线的参数，

所述编程的计算装置用下式计算定义一个作为加法结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2+\lambda+a+X1+X2$$

$$Y3=\lambda \times (X1+X3)+X3+Y1$$

其中：

$$\lambda=(X1^2+X1\times X2+X2^2+aX1+aX2+Y1)/(Y1+Y2+X2)$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器(6，8)的第三寄存器内。

5.一种按照权利要求1至4中的一个权利要求所述的方法，其特征是：所述第一点、第二点和第三点都在由射影坐标定义的椭圆曲线上。

6.一种按照权利要求5所述的方法，其特征是：所述第一点、第二点和第三点都在由Jacobi射影坐标定义的椭圆曲线上。

7.一种按照权利要求5所述的方法，其特征是：所述第一点、第二点和第三点都在由齐次射影坐标定义的椭圆曲线上。

8.一种按照权利要求1至7中的一个权利要求所述的方法，在所述方法期间执行对椭圆曲线上的点的标量相乘运算。

9.一种包括编程成实现按照权利要求1至7中的一个权利要求所述的方法的计算装置的电子组件，所述计算装置特别包括一个中央处理单元(2)和一个与之配合的存储器(4，6，8)。

10.一种电子组件，所述电子组件包括实现一种采用按照权利要求1至7中的一个权利要求所述的方法的密码算法的装置。

11.一种芯片卡，所述芯片卡包括一个按照权利要求10所述的电子组件。

用于椭圆曲线上的点的通用计算方法

技术领域

本发明涉及用于椭圆曲线上的一些点的通用计算方法和包括实现这种方法的装置的电子组件。本发明特别适用于实现例如在芯片卡（chip card）内的公开密钥（public key）型的密码算法(cryptographic algorithm)。

背景技术

椭圆曲线上的公开密钥算法（Public key algorithm）允许实现保密、数字签名、认证等类型的密码应用。

特别是，这些公开密钥算法很多用于芯片卡型的应用，因为它们可以采用处理时间相当短的短密钥，从而可以不需要用密码处理器实现，这就降低了实现它们的电子器件的生产成本。

为了定义可用于密码技术，存在各种参数化。一种经常采用的参数化是所谓的Weierstrass参数化。然而，应该注意的是，Weierstrass参数化是非常通用的，任何椭圆曲线可以归为这种参数化。

对于记录在案的来说，如果IK为一个域，所有满足以下通用Weierstrass方程(式F1)的点(X，Y)∈1k×IK:

$$E/IK:\ Y^2+a1\times X\times Y+a3\times Y=X^3+a2\times X^2+a4\times X+a6$$

其中：ai∈1K

和无穷远点0形成一条椭圆曲线E。在一个域上的任何椭圆曲线可以用这个形式表示。

所有的点(X，Y)和无穷远点0形成一个交换群（Abelian group），无穷远点0为零元（neutral element），群运算为点的相加，标为+，由众所周知的割线和切线法则给出。在这个群内，数对(X，Y)（X为横坐标，Y为纵坐标轴）是域IK的元，形成椭圆曲线上的一个点P的仿射坐标（affine coordinate）。

用仿射坐标内的数对(X，Y)表示的点P也可以用一般形式的射影坐标（projective coordinate）(U，V，W)表示。

特别是，射影坐标在对椭圆曲线上的点的求幂运算中是令人感兴趣的，因为它们不包括任何在这个域内的逆运算。

点P可以用一般形式(U，V，W)的所谓Jacobi射影坐标表示，(X，Y)与(U，V，W)的关系由下式表示：

$$x=U/W^2;\quad Y=V/W^3 \qquad (式F2)$$

采用Jacobi坐标，椭圆曲线的Weierstrass方程就成为：

$$E/IK:\ V^2+a1UVW+a3VW^3=U^3+a2U^2W^2+a4UW^4+a6W^6$$

点P也可以用一般形式(U，V，W)的所谓齐次射影坐标表示，这样，(X，Y)和(U，V，W)的关系由以下式表示：

$$X=U/W;\quad Y=V/W \qquad (式F3)$$

采用齐次坐标，椭圆曲线的Weierstrass方程就成为：

$$E/IK:\ V^2W+a1UVW+a3VW^2=U^3+a2U^2W+a4UW^2+a6W^3 \qquad (式F4)$$

可以按照曲线定义的域的特征数将Weierstrass方程表达成简化形式。应该说，在一个有限域内，域的元的数目始终可以表示为p^n的形式，其中p为一个质数。p是域的特征数。如果域不是有限的，这个特征数按惯例定义为等于零。

在域的特征数不为2和3的情况下，在仿射坐标内Weierstrass方程简化为：

$$E/IK:\ Y^2=X^3+aX+b \qquad (式F5)$$

其中a和b为椭圆曲线的参数，IK的元。

在射影、Jacobi或者齐次坐标内Weierstrass参数化的情况下，当然从这个在仿射坐标内的简化方程可以得出一些等效的公式表示。

如果域的特征数等于2，非超奇异曲线的Weierstrass方程在仿射坐标内可以简化为：

$$E/IK: \quad V^2+XY=X^3+a\times X^2+b \qquad (式F6)$$

其中a和b为椭圆曲线的参数，IK的元。

在射影、Jacobi或者齐次坐标内Weierstrass参数化的情况下，当然从这个在仿射坐标内的简化方程可以得出一些如前面那样的等效的公式表示。

按照定义椭圆曲线的参数化和按照用以执行处理的坐标，可应用各种点的相加、相减和加倍的公式。在许多为熟悉该技术的人员所知的参考文献中都给出了这些公式。也应注意的是，在射影坐标的情况下，这些公式不是唯一的，因为如式F2和F3所示，仿射坐标内的一个点具有几个等效的射影表示。

在仿射坐标内的Weierstrass参数化给出的椭圆曲线E的例子中，这些公式如下。

这条曲线的点P1=(X1，Y1)的逆为具有坐标(X1，$\bar{Y}1$)的点-P1，其中

$$\bar{Y}1=-Y1-a1\times X1-a3 \qquad (式F11)$$

这条曲线的坐标(X1，Y1)的点P1和坐标(X2，Y2)的点P2的加法运算在P1≠-P2的情况下给出具有坐标(X3，Y3)的点P3=P1+P2，有

$$X3=\lambda^2+a1\times\lambda-a2-X1-X2 \qquad (式F12)$$

$$Y3=-(\lambda+a1)\times X3-\mu-a3 \qquad (式F13)$$

其中

$$\lambda=(Y1-Y2)/(X1-X2)，\text{如果 } X1\neq X2 \qquad (式F14)$$

$$\lambda=(3X1^2+2\times a2\times X1+a4-a1\times Y1)/(2Y1+a1\times X1+a3)，\text{如果 } X1=X2 \qquad (式F15)$$

以及

$$\mu=Y1-\lambda\times X1 \qquad (式F16)$$

式F14是两个相异点相加的公式：P3=P1+P2，而式F15是点加倍的公式：P3=2×P1。

从这些在仿射坐标内的方程当然可以得出在射影、Jacobi或齐次坐标内的等效公式表示。

在特征数不为2和3的域上Weierstrass参数化给出的椭圆曲线E的例子中，点的相加、相减和加倍的公式得到简化，因为这条曲线的方程本身简化为：a1=a2=a3=0，a4=a，而a5=b。

在仿射坐标内的Weierstrass参数化的情况下，简化后的点的加、减和倍增的公式于是如下。

这条曲线E的一个点P1=(X1，Y1)的逆为点-P1=(X1，$\bar{Y}1$)，其中

$$\bar{Y}1=-Y1 \qquad \text{(式F17)}$$

这条曲线的坐标(X1，Y1)的点P1与坐标(X2，Y2)的点P2的相加运算在P1≠-P2的情况下给出点P3=P1+P2，其坐标(X3，Y3)为：

$$X3=\lambda^{2}-X1-X2$$

$$Y3=\lambda\times(X1-X3)-Y1$$

其中：

$$\lambda=(Y1-Y2)/(X1-X2),\quad \text{如果}P1\neq P2 \qquad \text{(式18)}$$

$$\lambda=(3\times X1^{2}+a)/(2\times Y1),\quad \text{如果}P1=P2 \qquad \text{(式19)}$$

式18是两个相异点相加的公式：P3=P1+P2，而式19是点加倍的公式：P3=2xP1。

定义在特征数为2的域上的非超奇异椭圆曲线的点的相加和加倍的简化公式以类似方式从通式(式F12至F16)通过假设a1=1，a3=a4=0，a2=a，以及a6=b得出。

点的相加或相减和倍增的运算是椭圆曲线上的指数算法中所用的基本运算：给定一个属于椭圆曲线E的点P1和一个预定数(一个整数)d，点P1与数d的标量相乘的结果为曲线E上的点P2，P2=d×P1=P1+P1+... +P1（d个P1相加）。因此一条椭圆曲线上的公开密钥

（Public key）密码算法是基于在曲线上所选的一个点P1与一个预定数d（秘密密钥（secret key））的标量相乘。标量相乘d×P1的结果是一个在这个椭圆曲线上的点P2。在一个按照E1 Gamal方法加密的应用实例中，所得到的点P2是用来对消息加密的公开密钥。

标量相乘P2=d×P1的运算可以用各种算法实现。可以列举其中的一些，诸如基于指数d的二进制表示的加倍和相加算法，基于指数d的带符号二进制表示的相加-相减算法，滑窗算法（window algorithm）等。所有的这些算法都采用在椭圆曲线上定义的相加、相减和加倍公式。

然而，这些算法已证明是容易受到针对发现特别是秘密密钥的值的攻击。特别可以列举的是隐蔽性信道攻击，简单的或差分的。简单或差分的隐蔽性信道攻击意味着以设备外界可测量的物理量为基础的攻击，通过直接分析(简单攻击)或按照统计方法(差分攻击)有可能发现在设备内处理中所包含和处理的信息。这些攻击因此可以发现机密的信息。在Paul Kocher的“密码学进展”(“Advances in Cryptology”, CRYPTO' 99, Vol. 1666 of Lecture Notes in Computer Science, pp. 388 -397, Springer -Verlag, 1999))中特别揭示了这些攻击。在为了达到这些目的可以利用的物理量中有执行时间、电流消耗、用来执行运算的部分组件辐射的电磁场等。这些攻击基于对一个比特的操作（即用一个特定的指令对它的处理）按照这个比特的值和/或按照这个指令会对所述的物理量有特定的影响。

在基于椭圆曲线的密码系统中，这些攻击与标量相乘有关。

如果以在Weierstrass参数化的椭圆曲线上的标量相乘算法为例，这种算法可以是易受简单型隐蔽性信道攻击的，因为加倍和相加的基本运算本质上是不同的，如以上面F14和F15或者F18和F19中对λ的计算所示。

因此，需要提供防止各种攻击成功的对抗方法。也就是说，必须使标量相乘算法安全可靠。

发明内容

本发明的一个目的是实现一种对椭圆曲线的通用计算方法，广义地说一种密码方法，防止隐蔽性信道攻击。

就此而言，本发明的目的是提供一种对由Weierstrass方程定义的

椭圆曲线上的点的通用计算方法。按照本发明，用完全相同编程的计算装置执行点的相加运算和点的加倍运算。这种计算装置特别包括一个中央处理单元和一个存储器。

因此，采用本发明，一条椭圆曲线上的点的加倍和相加基本运算是完全相同的，由完全相同的计算装置执行，具有相同的公式表示。因此不再能区别它们，特别是在简单隐蔽性信道攻击的情况下。所以，按照本发明设计的通用计算方法防止了这样的攻击。

一般地说，对一条椭圆曲线上的点进行标量相乘的方法或采用按照本发明设计的通用计算方法的根据椭圆曲线的密码方法以同样的方式得到保护。

无论用仿射、射影、Jacobi还是齐次坐标来执行这些计算，这都是正确的。因此，用单个λ值来执行点的相加或加倍。

按照一个通用实施例，为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，将第一点P1的仿射坐标和第二点P2的仿射坐标分别存储在存储器的第一和第二寄存器内，第一点和第二点都属于由以下类型的Weierstrass方程定义的椭圆曲线：

$$Y^2+a1\times X\times Y+a3\times Y=X^3+a2\times X^2+a4\times X+a6$$

(X，Y)为曲线上的点的仿射坐标，而a1、a2、a3、a4、a5、a6为椭圆曲线的参数，

编程的计算装置用下式计算定义一个作为加法结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2+a1\times\lambda-a2-X1-X2 \qquad (式F12)$$

$$Y3=-(\lambda+a1)\times X3-\mu-a3 \qquad (式F13)$$

其中

$$\lambda=(X1^2+X1\times X2+X2^2+a2\times X1+a2\times X2+a4-a1\times Y1)/(Y1+Y2+a1\times X2+a3) \qquad (式F20)$$

$$\mu=Y1-\lambda\times X1 \qquad (式F16)$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于

第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器的第三寄存器内。

在X1≠X2的情况下，也就是说在P1≠P2(名符其实的两个不同的点的相加)的情况下，式F20定义的λ与式F14定义的现有技术的λ完全相同。同样，在X1=X2(一个点的加倍操作)的情况下，也就是说在P1=P2(一个点的加倍)的情况下，式F20定义的λ与式F15定义的现有技术的λ完全相同。这将在下面在一个例子中更为精确地示出。

因此，在一条由Weierstrass参数化定义的椭圆曲线的情况下可以用同一个λ值执行点的相加或加倍。

按照另一个实施例，为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，将第一点P1的仿射坐标和第二点P2的仿射坐标分别存储在存储器的第一和第二寄存器内，第一点和第二点都属于由以下类型的简化Weierstrass方程定义的在特征数不为2或3的域上的椭圆曲线：

$$Y^2=X^3+a\times X+b,$$

(X，Y)为曲线上的点的仿射坐标，而a、b为椭圆曲线的参数，

编程的计算装置用下式计算定义一个作为相加结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2-X1-X2$$

$$Y3=\lambda\times(X1-X3)-Y1$$

其中：

$$\lambda=(X1^2+X1\times X2+X2^2+a)/(Y1+Y2) \qquad \text{(式F21)}$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器的第三寄存器内。

在由简化的Weierstrass参数化定义的在特征数不为2和3的域上的椭圆曲线的情况下，在这里也是可以用同一个λ值执行点的相加或加倍。

按照另一个实施例，为了执行一个由第一仿射坐标(X1，Y1)定义的第一点P1与一个由第二仿射坐标(X2，Y2)定义的第二点P2的相加，将第一点P1的仿射坐标和第二点P2的仿射坐标分别存储在存储器(6，8)的第一和第二寄存器内，第一点和第二点都属于由以下类型的简化Weierstrass方程定义的在特征数为2的域上的非超奇异椭圆曲线：

$$Y^2+XY=X^3+a\times X2+b,$$

(X，Y)为曲线上的点的仿射坐标，而a、b为椭圆曲线的参数，

编程的计算装置用下式计算定义一个作为加法结果的第三点P3的第三仿射坐标(X3，Y3)：

$$X3=\lambda^2+\lambda+a+X1+X2$$

$$Y3=\lambda\times(X1+X3)+X3+Y1$$

其中：

$$\lambda=(X1^2+X1\times X2+X2^2+aX1+aX2+Y1)/(Y1+Y2+X2) \qquad (式F22)$$

第二点不同于第一点P1的逆(-P1)，第二点等于第一点或者不同于第一点，

然后，将第三仿射坐标(X3，Y3)存储在存储器的第三寄存器内。

在特征数等于2的域上的非超奇异椭圆曲线情况下，在这里也是可以用同一个λ值执行点的相加或加倍。

如刚才所看到的那样，按照本发明设计的计算方法可以用同一个公式表示执行对属于椭圆曲线的点的相加或加倍运算。

一般地说，按照本发明设计的方法可用于对一条椭圆曲线上的点的全局标量相乘计算方法和/或用于密码方法。

本发明的另一个目的是提供一种包括编程的计算装置的电子组件，计算装置特别是包括一个中央处理单元和一个存储器，用来实现一种如上面所说明的执行在一条椭圆曲线上的点的相加或加倍的通用计算方法。所述电子组件可以包括对用如上面所说明的通用计算方法的密码算法的全局使用。

最后，本发明的另一个目的是提供一种包括一个如上所述的电子组

件的芯片卡。

从以下结合一个附图对本发明的纯粹用来说明一些具体实施例的说明中可以更清楚地理解本发明和本发明的优点。这个附图以方框图形式示出了能执行密码计算的电子设备1。

附图说明

图1为一个结合入一个芯片卡的编程的计算装置。

具体实施方式

在下面的这些例子中，如图1所示，设备1是一个用来执行密码程序的芯片卡。为此，设备1组合在一个芯片卡编程的计算装置内，这个计算装置由一个中央处理单元2和与之连接的一系列存储器组成，这些存储器包括：

一个只以读出模式可接入的存储器4，例如掩模只读存储器(掩模ROM)，

电子可重编程的存储器6，例如EEPROM（电可擦可编程序只读存储器），以及

一个以读、写模式可接入的工作存储器8，例如RAM(随机存取存储器)。这个存储器特别是包括由设备1使用的一些计算寄存器。

与指数算法相应的可执行码包含在程序存储器内。这个码实际上可以包含在只以读模式可接入的存储器4内和/或包含在可重写的存储器6内。

中央处理单元2与一个提供与外界信号交换和为芯片供电的通信接口10连接。这个接口可以包括一些用来与一个读出器“接触”连接和/或在所谓“不接触”卡的情况下与天线连接的卡上引线。

设备1的功能之一是对发送给外界或从外界接收到的机密消息M加密或解密。这个消息可以涉及例如个人代码、医学信息、对银行或商业事务的兼容性、接入某些限制业务的授权等。另一个功能是计算或校验数字信号。

为了完成这些功能，中央处理单元2根据存储在掩模ROM 4和/或EEPROM 6一些部分内的编程数据执行密码算法。

在这里所用的算法是一种在Weierstrass参数化椭圆曲线上的公开密钥算法。确切地说，在这里所涉及的是这种算法的使在仿射坐标内的基本运算（即点的相加或者加倍运算）得以执行的部分。

在第一个例子中，椭圆曲线是在特征数严格大于3的域上的曲线，其方程用a、b？IK表示为：

$$E/IK: \quad Y^2=X^3+a \times X+b$$

在求幂计算设备1进行相加操作的计算时，中央处理单元2首先存储椭圆曲线的两个需相加的点P1、P2的坐标(X1，Y1)、(X2，Y2)。在这里可以认为点P2不同于作为点P1的逆的点(-P1)。

中央处理单元2然后按照下式计算出一个中间变量x：

$$\lambda=(X1^2+X1 \times X2+X2^2+a)/(Y1+Y2) \qquad (式F21)$$

中央处理单元将这个变量λ存储在工作存储器8的一个寄存器内，然后计算作为点P1与点P2相加的结果的点P3的坐标(X3，Y3)：

$$X3=\lambda^2-X1-X2$$
$$Y3=\lambda \times (X1-X3)-Y1$$

坐标(X3，Y3)最终存储在工作存储器8的其他寄存器内，以便在别处使用，例如用于加密算法的其余部分。

也是在这个例子中，在X1≠X2的情况下，也就是说在P1≠P2(名符其实的两个不同的点的相加)的情况下，式F21定义的λ与式F18定义的现有技术的λ完全相同。

这是因为，根据式F18，$\lambda=(Y1-Y2)/(X1-X2)$，如果X1≠X2，即有：

$$\lambda=(Y1-Y2)/(X1-X2)=[(Y1-Y2)(Y1-Y2)]/[(X1-X2)(Y1-Y2)]$$
$$=(Y1^2-Y2^2)/[(X1-X2)(Y1+Y2)]$$

由于在这个例子中$\bar{Y}2=-Y2$(式F17)，因此得出：

$$\lambda=(X1^3+a \times X1-X2^3-a \times X2)/[(X1-X2)\ (Y1+Y2)]$$

由于对于在这个例子中所考虑的椭圆曲线上的具有坐标(Xi，Yi)的点Pi，有$Yi^2=Xi^3+a\times Xi+b$，因此给出：

$$\lambda=(X1^2+X1\times X2+X2^2+a)/(Y1+Y2),$$

即为式F21。

同样，在X1=X2(一个点的加倍操作)的情况下，也就是说在P1=P2的情况下，式F21定义的λ与式F19定义的现有技术的λ完全相同。这是因为根据式F21，取X1=X2和Y1=Y2，就可得出：

$$\lambda=(3\times X1^2+a)/(2\times Y1) \qquad \text{(式F16)}$$

因此，在特征严格大于3和由一个简化Weierstrass参数化定义的椭圆曲线的情况下，可以用同一个λ值执行点的相加或加倍。

在第二个例子中，椭圆曲线是一条在特征数为2的域上的非超奇异曲线，其方程用a、b? IK表示为：

$$E/IK:\ Y^2+XY=X^3+a\times X^2+b$$

正象在上个例子中那样，在求幂计算设备1进行相加运算的计算时，中央处理单元2首先存储椭圆曲线的两个需相加的点P1、P2的坐标(X1，Y1)、(X2，Y2)。在那里也可以认为点P2不同于作为点P1的逆的点(-P1)。

中央处理单元2然后按照下式计算出一个中间变量λ：

$$\lambda=(X1^2+X1\times X2+X2^2+aX1+aX2+Y1)/(Y1+Y2+X2) \qquad \text{(式F22)}$$

中央处理单元将这个变量λ存储在工作存储器8的一个寄存器内，然后计算作为点P1与点P2相加的结果的点P3的坐标(X3，Y3)：

$$X3=\lambda^2+\lambda+a+X1+X2$$

$$Y3=\lambda\times(X1+X3)+X3+Y1$$

坐标(X3，Y3)最终存储在工作存储器8的其他寄存器内，以便在别处使用。

也是在这个例子中，在X1≠X2的情况下，也就是说在P1≠P2(名符其实的两个不同的点的相加)的情况下，式F21定义的λ与式F18定义的现有技术的λ完全相同。

在特征数等于2和由Weierstrass参数化定义的椭圆曲线的情况下，也可以用同一个λ值执行点的相加或加倍。

应指出的是，在所有上面所说明的这些例子中，都使用仿射坐标。然而，使用射影、齐次或Jacobi坐标也完全是可行的。只是要确保在使用时将这些公式改写成射影形式。

为此，作为一个例子在X3和Y3的λ中，仿射坐标Xi、Yi将作如下替换:

*在Jacobi射影坐标内:

$Xi=Ui/Wi^2$, $Yi=Vi/Wi^3$;

*在齐次射影坐标内:

Xi=Ui/Wi, Yi=Vi/Wi。