(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106716345 A
(43)申请公布日 2017.05.24

(21)申请号 201580053184.0

(22)申请日 2015.09.30

(30)优先权数据
14186951.1 2014.09.30 EP

(85)PCT国际申请进入国家阶段日
2017.03.30

(86)PCT国际申请的申请数据
PCT/EP2015/072635 2015.09.30

(87)PCT国际申请的公布数据
WO2016/050884 EN 2016.04.07

(71)申请人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬

(72)发明人 L.马林 A.A.M.L.布鲁克斯
P.M.H.M.A.戈里斯森

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张同庆 陈岚

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

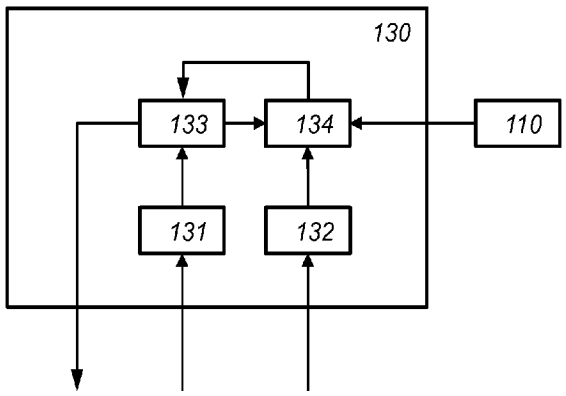
权利要求书4页 说明书16页 附图4页

(54)发明名称

用于执行混淆算术的电子计算设备

(57)摘要

提出了一种用于在有限交换环($\mathbb{Z}_n$; $\mathbb{Z}_n[x]/f(x)$)中执行算术的电子计算设备(100)。该计算设备包括被布置成存储针对增量环元素(1;u^t)定义的增量表(T)的存储库(110),该增量表将输入环元素($k = u^{k_1} - u^{k_2}$)映射到对输出环元素($I=u^{I1}-u^{I2}$)编码的输出整数列表($(T(k_1,k_2)) = (l_1,l_2)$),使得输出环元素等于增量环元素环加到输入环元素($I=k+1$)。使用增量表,环加法单元(130)将对第一加法输入环元素编码的第一加法输入整数列表((a_1,a_2))和对第二加法输入环元素编码的第二加法输入整数列表((b_1,b_2))相加。该设备可以包括也使用增量表的环乘法单元(140)。



CN 106716345 A

1.一种用于在交换环($\mathbb{Z}_n$; $\mathbb{Z}_n[x]/f(x)$)中执行算术的电子计算设备(100),该环具有有限数量的环元素,在环元素上定义了环加法和环乘法,该计算设备在对环元素($u^{a_1}-u^{a_2}$)编码的整数列表((a_1,a_2))上运算,所述整数列表包括至少两个元素,其中整数列表((a_1,a_2))对环元素(a)进行编码以使得环元素等于一个或多个基础环元素($u;u,v$)的幂的线性组合($a=u^{a_1}-u^{a_2}$; $a=u^{a_1}-v^{a_2}$),其中所述幂具有由整数列表确定的指数,该计算设备包括:

- 存储库(110),其被布置成存储针对增量环元素($1;u^t$)定义的增量表(T),

- 增量表将输入环元素($k=u^{k_1}-u^{k_2}$)映射到对输出环元素($l=u^{l_1}-u^{l_2}$)编码的输出整数列表($(T(k_1,k_2))=(l_1,l_2)$),使得输出环元素等于增量环元素环加到输入环元素(l=k+1),

- 环加法单元(130),其被布置成:

- 接收对第一加法输入环元素编码的第一加法输入整数列表((a_1,a_2))和对第二加法输入环元素编码的第二加法输入整数列表((b_1,b_2)),增量环元素独立于第一和第二加法输入环元素,

- 通过将增量表应用到从第一和第二加法输入整数列表确定的环元素来确定对加法输出环元素编码的加法输出整数列表,该加法输出环元素等于第一加法输入环元素与第二加法输入环元素的环加。

2.如权利要求1所述的计算设备,包括,

- 环乘法单元(140),其被布置成:

- 接收对第一乘法输入环元素编码的第一乘法输入整数列表((r_1,r_2))和对第二乘法输入环元素编码的第二乘法输入整数列表((s_1,s_2)),

- 通过将增量表应用到从第一和第二乘法输入整数列表确定的环元素来确定对乘法输出环元素编码的乘法输出整数列表,该乘法输出环元素等于第一乘法输入环元素和第二乘法输入环元素的环乘。

3.如权利要求1或2所述的计算设备,其中整数列表((a_1,a_2))对环元素(a)进行编码,使得:

- 环元素等于基础元素提升至由整数列表的第一整数确定的幂减去该基础元素提升至由该整数列表的第二整数确定的幂($a=u^{a_1}-u^{a_2}$),可选地乘以常数($a=t\,(u^{a_1}-u^{a_2})$),或者

- 环元素等于基础元素提升至由整数列表的第一整数确定的幂加上该基础元素提升至由该整数列表的第二整数确定的幂($a=u^{a_1}+u^{a_2}$),可选地乘以常数,或者

- 环元素等于基础元素提升至由整数列表的第一整数确定的幂与基础元素提升至由该整数列表的第二整数确定的幂减去基础元素提升至由整数列表的负的第二整数确定的幂相乘($a=u^{a_1}\,(u^{a_2}-u^{-a_2})$),可选地乘以常数,($a=u^{a_1}\left(\frac{u^{a_2}-u^{-a_2}}{2}\right)$),或者

- 环元素等于基础元素提升至指数为整数列表的第一整数和第二整数的第一线性组合的幂加上或减去基础元素提升至指数为整数列表的第一整数和第二整数的第二线性组

合的幂，($x = u^{b_1} + u^{b_2}$或者$x = u^{b_1} - u^{b_2}$，给定矩阵M，使得$M\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$)，可选地乘以常数。

4.如权利要求1和3中任一项所述的计算设备，其中确定加法输出整数列表包括：

- 通过增量表针对为一个或多个基础元素的幂的线性组合的环元素($u^{a_1-b_1} - u^{a_2-b_1}$)的第一应用确定对中间加法环元素编码的中间加法整数列表((c_1, c_2))，其中所述幂从第一和第二加法输入整数列表确定，($u^{c_1} - u^{c_2} = u^{a_1} - u^{a_2} + u^{b_1}$)，

- 确定加法输出整数列表包括增量表针对从中间加法整数列表确定的和从第二加法输入整数列表确定的环元素的第二应用。

5.如权利要求4所述的计算设备，其中

- 确定中间加法整数列表((c_1, c_2))进一步包括将从第一和第二加法输入整数列表确定的整数加到源自第一应用的整数列表中的整数。

6.如权利要求4和5中任一项所述的计算设备，其中

- 增量表被应用到通过所述一个或多个基础环元素(u)提升至以第一整数列表的第一整数(a_1)减去第二整数列表的第一整数(b_1)为指数的幂加上或减去基础环元素(u)提升至以第一整数列表的第二整数(a_2)减去第二整数列表的第一整数(b_1)为指数的幂形成的环元素($u^{a_1-b_1} - u^{a_2-b_1}$；$u^{a_1-b_1} + u^{a_2-b_1}$)；并且/或者

- 增量表被应用到通过所述一个或多个基础环元素(u)提升至以第一整数列表的第一整数(a_1)减去第一整数列表的第二整数(a_2)为指数的幂加上或减去基础环元素(u)提升至以第二整数列表的第一整数(b_1)减去第一整数列表的第二整数(a_2)为指数的幂形成的环元素($u^{a_1-a_2} + u^{b_1-a_2}$；$u^{a_1-a_2} + u^{b_1-a_2}$)；并且/或者

- 增量表被应用到通过所述一个或多个基础环元素(u)提升至以第一整数列表的第二整数(a_2)减去第一整数列表的第一整数(a_1)为指数的幂加上或减去基础环元素(u)提升至以第二整数列表的第一整数(b_1)减去第一整数列表的第一整数(a_1)为指数的幂形成的环元素($u^{b_1-a_1} - u^{a_2-a_1}$；$u^{a_2-a_1} + u^{b_1-a_1}$)。

7.如权利要求4、5和6中任一项所述的计算设备，其中

- 在增量表的第二应用之前，对由中间加法整数列表表示的中间加法环元素取反。

8.如前述权利要求中任一项所述的计算设备，其中

- 通过置换整数列表来对由整数列表表示的环元素取反，并且/或者

- 通过将常数加到整数列表的每一个整数来对由整数列表表示的环元素取反，并且/或者

- 通过置换整数列表并且使整数列表的一个或多个整数与常数相乘来对由整数列表((a_1, a_2))表示的环元素取反((sa_2, sa_1))。

9.如前述权利要求中任一项所述的计算设备，其中增量表把表示输入环元素($k = u^{k_1} - u^{k_2}$)的输入整数列表((k_1, k_2))当作输入。

10.如权利要求2所述的和如前述权利要求中任一项所述的计算设备，其中确定乘法输出整数列表包括：

- 从第一和第二乘法输入整数列表确定第一中间乘法整数列表((t_1, t_2))和第二中间乘法整数列表((u_1, u_2))，其分别对第一和第二中间乘法环元素进行编码，

- 通过环加法单元将第一和第二中间乘法整数列表相加。

11.如权利要求10所述的计算设备,其中

- 第一中间乘法整数列表的第一整数(t_1)包括第一乘法输入整数列表的第一整数(r_1)加上第二乘法输入整数列表的第一整数(s_1),并且

- 第一中间乘法整数列表的第二整数(t_2)包括第一乘法输入整数列表的第一整数(r_1)加上第二乘法输入整数列表的第二整数(s_2),($t_1 = r_1 + s_1, t_2 = r_1 + s_2$),并且

- 第二中间乘法整数列表的第一整数(u_1)包括第一乘法输入整数列表的第二整数(r_2)加上第二乘法输入整数列表的第二整数(s_2),并且

- 第二中间乘法整数列表的第二整数(u_2)包括第一乘法输入整数列表的第二整数(r_2)加上第二乘法输入整数列表的第一整数(s_1),($u_1 = r_2 + s_2, u_2 = r_2 + s_1$)。

12.如前述权利要求中任一项所述的计算设备,其中

交换环是通过整数对一整数模数取模形成的环($\mathbb{Z}_n$),或者

交换环是通过整数多项式对一整数多项式模数取模形成的环($\mathbb{Z}_n[x]/f(x)$)。

13.一种用于将交换环($\mathbb{Z}_n$; $\mathbb{Z}_n[x]/f(x)$)的环元素编码成整数列表的环编码设备(170),其与如权利要求1所述的计算设备一起使用,该环编码设备包括:

- 存储库(172),其被布置成存储针对一个或多个基础环元素(u)定义的编码表,该编码表将环元素(x)映射到整数列表((a,b)),使得环元素等于所述一个或多个基础环元素的幂的线性组合($x = u^a - u^b$),其中所述幂具有由整数列表确定的指数。

14.一种用于将整数列表((a,b))解码成交换环($\mathbb{Z}_n$; $\mathbb{Z}_n[x]/f(x)$)的环元素(x)的环解码设备(160),其与如权利要求1所述的计算设备一起使用,该环解码设备被布置成针对一个或多个基础环元素(u)确定环元素(x),使得该环元素等于一个或多个基础环元素的幂的线性组合($x = u^a - u^b$),其中所述幂具有由整数列表确定的指数。

15.一种用于演算与用于在交换环($\mathbb{Z}_n$; $\mathbb{Z}_n[x]/f(x)$)中执行算术的计算设备一起使用的增量表的表演算设备(200),该环具有有限数量的环元素,在环元素上定义了环加法和环乘法,该计算设备在对环元素($u^{a_1} - u^{a_2}$)编码的整数列表((a_1,a_2))上运算,所述整数列表包括至少两个元素,该表演算设备包括,

- 表创建单元(210),其被布置成构造增量表,该表创建单元被布置成:

- 反复地选择输入环元素,

- 确定等于增量环元素环加到输入环元素的输出环元素,

- 确定针对输出环元素编码的输出整数列表,

- 向将输入环元素映射到输出整数列表的增量表添加条目。

16.一种用于在交换环($\mathbb{Z}_n$;$\mathbb{Z}_n[x]/f(x)$)中执行算术的电子计算方法,该环具有有限数量的环元素,在环元素上定义了环加法和环乘法,该计算方法在对环元素($u^{a_1} - u^{a_2}$)编码的整数列表((a_1,a_2))上运算,所述整数列表包括至少两个整数,其中整数列表((a_1,a_2))对环元素(a)进行编码以使得环元素等于一个或多个基础环元素(u;u,v)的幂的线性组合($a = u^{a_1} - u^{a_2}$; $a = u^{a_1} - v^{a_2}$),其中所述幂具有由整数列表确定的指数,该计算方法包括:

- 存储针对增量环元素(1;u^t)定义的增量表(*T*),该增量表将输入环元素($k=u^{k_1}-u^{k_2}$)映射到对输出环元素($l=u^{l_1}-u^{l_2}$)编码的输出整数列表($T((k_1,k_2))=(l_1,l_2)$),使得输出环元素等于增量环元素环加到输入环元素(*l*=*k*+1),

- 环加,该环加包括:

- 接收对第一加法输入环元素编码的第一加法输入整数列表((a_1,a_2))和对第二加法输入环元素编码的第二加法输入整数列表((b_1,b_2)),

- 通过将增量表应用到从第一和第二加法输入整数列表确定的环元素来确定对加法输出环元素编码的加法输出整数列表,该加法输出环元素等于第一加法输入环元素与第二加法输入环元素的环加。

17.如权利要求16所述的电子计算方法,包括:

- 环乘,该环乘包括

- 接收对第一乘法输入环元素编码的第一乘法输入整数列表((r_1,r_2))和对第二乘法输入环元素编码的第二乘法输入整数列表((s_1,s_2)),

- 通过将增量表应用到从第一和第二乘法输入整数列表确定的环元素来确定对乘法输出环元素编码的乘法输出整数列表,该乘法输出环元素等于第一乘法输入环元素与第二乘法输入环元素的环乘。

18.一种包括计算机程序指令的计算机程序,该计算机程序指令被布置成当计算机程序在可编程装置上运行时执行权利要求16或17的方法。

19.一种计算机可读介质,包括:

- 依照权利要求18的计算机程序,和/或

- 由依照权利要求1的电子计算设备使用的增量表。

用于执行混淆算术的电子计算设备

技术领域

[0001] 本发明涉及电子计算设备、环编码设备、环解码设备、表演算方法、电子计算方法、计算机程序以及计算机可读介质。

背景技术

[0002] 在白箱密码术中以及更一般地在软件混淆(obfuscation)中，通常在编码值而非明文值上执行演算。如果在编码的值而非在明文值自身上执行演算，混淆的软件的逆向工程更加困难。

[0003] 在编码之后，像加法或乘法那样的常规运算可能不再使用计算机内置本原执行。编码值的简单相加在正常情况下并不导致这些值的相加的编码。这同样适用于乘法。在公式中，对于大多数x和y，$E(x)+E(y)\neq E(x+y)$；E表示编码函数。

[0004] 此问题的解决方案是引入加法(A)和乘法(M)表。所述表把两个编码值当作输入，并且产生一个编码值作为对应于加法或乘法运算的编码的输出。所述表可以被定义为：$A\big(E(x),E(y)\big)=E(x+y)$；$M\big(E(x),E(y)\big)=E(xy)$。这些表允许直接在编码值上执行算术。

[0005] 使用表的混淆加法和乘法遭受至少两个缺陷。首先，所述表可能变得相当大。如果x和y被表示为l位，每个表需要$2^{2l}l$ 位。

[0006] 其次，这样的大表可能在软件中容易被发现。更坏的是，这些表可能仍然被标识为加法或乘法运算，即使它们被编码了；例如凭借在编码中保留的这些函数的属性。例如，乘法表满足$M(E(0),E(x))=E(0)$。攻击者可以使用此属性和类似属性来猜测所述表表示哪种运算。

发明内容

[0007] 将会有利的是，具有一种执行混淆算术的改进的方式。提供了如权利要求1中限定的一种计算设备。

[0008] 发明人发现，在某些情况下，在编码值上的乘法和加法可以使用单个表执行，而不必将多个值编码成单个编码值。因为相同的表被用于加法和乘法，所以在逆向工程期间将难以领会是加法还是乘法被执行。因为从外部观看时加法和乘法表现为相同的运算，所以发明人把这个方法叫做“同质(homogeneous)混淆”。即使攻击者能够发现使用的表，并且即使他能够以某种方式算出其作为增量表的功能，他仍然不会知晓是加法还是乘法运算被执行。该表作用于整数列表的元素的方式对加法和乘法而言是不同的，然而这可以容易使用诸如代码混淆、白箱实现方式等之类的传统混淆来隐藏。

[0009] 此外，使用的单个表也小于在背景技术中所讨论的表：需要大约$2^{l}l$位。即使只使用加法，混淆加法所需的表小于背景技术中所建议的表。

[0010] 本发明适用于许多不同的交换环R，尽管不是每个和每一个环都允许作为整数列

表编码。交换环是一种数学概念，其包括许多不同的常见数学结构，例如整数模某数字（$\mathbb{Z}_n$）或者多项式模某数字和某多项式（$\mathbb{Z}_n[x]/f(x)$）。域是交换环的特殊情况。如本文将会描述，技术人员可以验证给定的环是否允许混淆。

[0011] 例如，环元素可以被编码为两个整数(*a*，*b*)。可以使用增量表在该编码上直接执行算术，该增量表将编码的环元素映射到该编码的环元素加增量值。例如，该表将(*a*，*b*)映射到(*c*，*d*)，如果$u^c - u^d = u^a - u^b + 1$。加法和乘法二者都通过增量表的反复应用而执行。

[0012] 如本文将会更充分地讨论的，存在许多其他可能性和变形。典型地对攻击者而言将未知的是，在任意给定的实现方式中选择了许多个变形中的哪一种。

[0013] 所述计算设备是电子设备并可以是移动电子设备，例如移动电话、机顶盒、计算机、智能卡等。

[0014] 如本文所描述的混淆算术可以应用于范围广泛的实际应用中。这样的实际应用包括运行在私有硬件上的安全应用，例如银行业应用等，在所述安全应用中逆向工程将被防止。其他应用包括其中将要防止数据的无意泄露的应用。如果程序被诱骗释放私有数据，那么若泄露的数据被编码的话，这不用太过担忧。混淆算术也可以应用于运行应用的服务器。如果用户以编码形式发送和接收数据，则私密性增强。

[0015] 一种依照本发明的方法可以作为计算机实现的方法在计算机上或在专用硬件中或在二者的组合中实现。用于依照本发明的方法的可执行代码或其部分可以存储在计算机程序产品上。计算机程序产品的示例包括存储器设备、光学存储设备、集成电路、服务器、在线软件等。优选地，计算机程序产品包括存储在计算机可读介质上的非临时性程序代码构件，以用于在所述程序产品在计算机上执行时执行依照本发明的方法。

[0016] 在一个优选实施例中，计算机程序包括适于当该计算机程序在计算机上运行时执行依照本发明的方法的所有步骤的计算机程序代码构件。优选地，计算机程序体现在计算机可读介质上。

附图说明

[0017] 本发明的这些和其他方面根据下文描述的实施例而是清楚明白的并且将参照这些实施例进行阐述。在附图中：

图1a示意性示出计算设备100的实施例的一个示例，

图1b示意性示出环加法单元130的实施例的一个示例，

图1c示意性示出环乘法单元140的实施例的一个示例，

图2示意性示出计算设备101的实施例的一个示例，

图3示意性示出用于演算用在计算设备中的增量表的表演算设备200的实施例的一个示例，

图4示意性示出用于执行混淆算术的计算方法30的实施例的一个示例，

图5示意性示出加法方法400的实施例的一个示例，

图6示意性示出乘法方法500的实施例的一个示例，

图7a示出具有包括依照一个实施例的计算机程序的可写部分的计算机可读介质，

图7b示出依照一个实施例的处理器系统的示意性表示。

[0018] 不同图中具有相同参考数字的项目具有相同的结构特征或相同的功能，或者是相同的信号。在这样的项目的功能和/或结构已被解释的情况下，在详细描述中没有必要其进行重复解释。

具体实施方式

[0019] 尽管本发明可受许多不同形式的实施例的影响，但是在附图中示出了一个或更多具体实施例并且将在本文中对其进行详细描述，应当理解的是，本公开内容应被视为例示本发明的原理，而不旨在将本发明限于所示出和描述的具体实施例。

[0020] 在下文中，为了理解，在操作中描述了实施例的元件。然而，将会显然的是，相应的元件被布置成执行被描述为它们所执行的功能。

[0021] 所述电子计算设备使用出奇小的表执行高效的算术。而且，在混淆算术的领域中，如果通过表执行运算，被认为是有利的，因为这样的运算容易进一步进行混淆，例如使用传统的白箱技术(参见，例如Chow等人的“White-box cryptography and an AES implementation”)。因而，有必要使用表来表达算术运算。实施例使用比现有技术中所用的表更小的表实现加法。即使没有诸如白箱密码术之类的附加混淆，电子计算设备也有助于混淆。如本文所示出，存在可以实现编码和增量表的许多方式。在任意特定实施例中使用哪一种编码是攻击者未知的，并且因而使得观察到的计算更难解释。

[0022] 实施例允许使用相同的表执行乘法和加法运算。这进一步添加到混淆，因为根据使用增量表的事实，可以不再确定执行了什么操作。下面，首先讨论计算设备的实施例的若干可能的架构。接下来，讨论执行混淆算术的若干可替换方式。

[0023] 图1示意性示出计算设备100的实施例的一个示例。计算设备100是用于在有限交换环中执行混淆算术的电子设备。交换环的许多示例是已知的。下面给出了两种这样的环的示例：整数模某数字($\mathbb{Z}_n$) 或者多项式模某数字和某多项式($\mathbb{Z}_n[x]/f(x)$)。其他实施例可以使用其他交换环。

[0024] 环的元素被称为环元素。在环元素上，定义了加法和乘法，后者被称为环加法和环乘法。

[0025] 环元素可以以任何适当的形式表示，如果该形式是所需要的话。例如，$\mathbb{Z}_n$的元素可以表示为整数；$\mathbb{Z}_n[x]/f(x)$的元素可以表示为多项式。然而，在计算设备100中，环元素被表示为整数列表。例如，环元素a在计算设备100中可以由列表(a_1,a_2)表示。后者甚至适用于非整数环，比如多项式环。整数列表依照环元素与整数列表之间的某种映射对环元素进行编码；给定任一环元素，存在至少一个表示该环元素的整数列表，并且给定任一整数列表，存在恰好一个它表示的环元素。在实施例中，任何环元素都可以表示为整数列表。

[0026] 整数列表具有至少两个元素。事实证明，如果整数列表更短，则加法和乘法运算需要更少的步骤。相应地，在一个实施例中，整数列表总是具有两个元素。在主要描述中，我们将假设整数列表是整数对，然而提供了具有多于两个元素的整数列表的示例。作为一个示例，(a_1,a_2)可以映射到环元素($u^{a_1}-u^{a_2}$)，其中u是一种特殊的环元素，被称为基础环元素。下面讨论许多变形，包括使用多个基础元素。然而，在主要的讨论中，作为“示例编码”，

我们将假设给定的整数列表(a_1,a_2)映射到环元素$(u^{a_1}-u^{a_2})$。

[0027] 在一个实施例中，整数列表中的整数是非负的。这简化了演算，但不是必需的。而且，在一个实施例中，整数列表中的整数以对基础元素u的次数取模来取得。基础元素u的次数是使得$u^k=1$的最小整数k。方便的是，例如通过执行模k运算，使整理列表中的值保持在$[0,k-1]$的范围之中。

[0028] 计算设备100可以包括运算数存储装置150。运算数被作为整数列表存储在运算数存储装置150中。可以在存储在运算数存储装置150中的运算数上执行算术。所述算术的结果可以存储在运算数存储装置150中，其中它们可以用在新的运算中，或者可以被输出给不同的设备，等等。

[0029] 计算设备100包括布置成存储针对增量环元素定义的增量表T的存储库110。该增量表将输入环元素映射到对输出环元素编码的输出整数列表，使得输出环元素等于增量环元素环加(ring-added)到输入环元素。在一个实施例中，输入环元素被表示为整数列表。以此方式，表T将整数列表映射到整数列表；二者依照相同的编码，例如相同的映射。然而，存在其中输入环元素在可替换的编码中被表示为整数列表的实施例。在任何情况下，输入环元素以数字形式表示，允许表将输入环元素映射到输出环元素。

[0030] 表可以以某种格式列出输入环元素，连同关联的输出整数列表。该表在存储库中也可以通过省略输入环而仅列出输出整数列表来表示。例如，这可以在输入环以规范格式表示的情况下进行。

[0031] 例如，假设示例编码，输入环元素$k=u^{k_1}-u^{k_2}$可以通过表T映射到输出整数列表。在此情况下，输入环元素可以表示为整数列表，使得我们可以有$((k_1,k_2))=(l_1,l_2)$。后者对输出环元素进行编码$l=u^{l_1}-u^{l_2}$。输出环元素等于增量环元素环加到输入环元素。例如，如果增量环元素为1，那么$l=k+1$。在一个实施例中，增量元素可以是1，然而这不是必要的。例如，使用示例编码，增量元素可以被选择为u^t，对于t的某个值，例如0<=t<次数(u)的任何值。

[0032] 增量表比背景技术中描述的表小得多。后者表采取两个输入，例如两个编码数字以产生编码输出。然而，表T仅采取一个编码输入以产生一个编码输出；增量环元素是固定的。假设所述编码采取类似量的空间，T的输入空间被减小至平方根周围。这是显著的尺寸改进。

[0033] 计算设备100包括环加法单元130和环乘法单元140。计算设备100还可以包括环取反单元120。在一个实施例中，环乘法单元140可以使用加法单元130执行加法；加法单元130可以使用取反单元120。这在图1中已经通过单元120、130和140之间的线指示。然而，单元可以复制；例如，加法单元130可以进行它自己的取反，并且乘法140可以进行它自己的加法。取反也被称为“符号改变”。

[0034] 取反单元120可以接收对取反输入环元素a编码的取反输入整数列表(a_1,a_2)。取反单元120被布置成确定对取反输出环元素b编码的取反输出整数列表(b_1,b_2)。取反输出环元素是取反输入环元素的负值，例如，取反输出环元素等于用于加法的中性环元素(0)减去取反输入环元素。因而，$b=-a$。

[0035] 在一个实施例中，取反单元可以通过置换取反输入整数列表来演算输出整数列

表。使用示例编码，$a = u^{a_1} - u^{a_2}$，输出整数列表可以是(a_2, a_1)。通过置换取反可以通过改变元素被从中读取的地址而在代码中高效地实现，并且它不必改变存储器中的实际顺序。

[0036] 在一个实施例中，取反单元可以通过向整数列表的每一个整数加上常数来演算输出整数列表。例如，在使用使得$u^m=-1$的整数m的示例编码中；例如输出整数列表可以是(a_1+m, a_2+m)。

[0037] 环加法单元130被布置成接收对第一加法输入环元素编码的第一加法输入整数列表(a_1, a_2)和对第二加法输入环元素编码的第二加法输入整数列表(b_1, b_2)。例如，环加法单元130可以从运算数存储装置150接收两个运算数。环加法单元130被布置成通过将增量表应用到从第一和第二加法输入整数列表确定的环元素来确定对加法输出环元素编码的加法输出整数列表，该加法输出环元素等于第一加法输入环元素和第二加法输入环元素的环加。

[0038] 在一个实施例中，整数列表到特定环元素的映射包括多个子映射，每一个子映射与整数列表的整数关联，子映射将整数映射到环元素。所述映射是应用于关联的整数的子映射的线性组合，例如和。子映射可以将基础元素提升至由关联的整数确定的幂。例如，在示例编码中，(a_1, a_2)可以被说成子映射u^{a_1}和子映射$-u^{a_2}$的和。

[0039] 图1b图示了加法单元130的一个实施例。加法单元130接收第一加法输入整数列表131和第二加法输入整数列表132。加法单元130包括中间加法单元134，其被布置成将从第二加法输入整数列表132的整数获得的环元素迭代地加到第一加法输入环元素。例如，中间加法单元132可以增加中间和133，其被初始化为第一整数列表元素。该加法涉及来自存储库110的增量表的应用。

[0040] 环乘法单元140被布置成接收对第一乘法输入环元素编码的第一乘法输入整数列表(r_1, r_2)和对第二乘法输入环元素编码的第二乘法输入整数列表(s_1, s_2)。例如，乘法单元140可以从运算数存储装置150接收两个运算数。环乘法单元140被布置成通过将增量表应用到从第一和第二乘法输入整数列表确定的环元素来确定对乘法输出环元素编码的乘法输出整数列表，该乘法输出环元素等于第一乘法输入环元素和第二乘法输入环元素的环乘。

[0041] 图1c示出乘法单元140的一个可能的实施例。乘法单元140接收第一乘法输入整数列表141和第二乘法输入整数列表142。乘法单元140包括中间乘法单元144，其被布置成从第一和第二乘法输入整数列表141、142确定第一中间乘法整数列表145(t_1, t_2)和第二中间乘法整数列表146(u_1, u_2)，其分别对第一和第二中间乘法环元素编码。乘法单元140被布置成通过环加法单元130加上第一145和第二中间乘法整数列表146。确定中间整数列表可以涉及在整数列表中的整数上的算术运算，但不需要增量表。

[0042] 计算设备100可选地包括用于将交换环的环元素编码为整数列表的环编码单元170，以及用于将整数列表(a, b)解码为交换环的环元素(x)的环解码单元160。编码单元170和/或解码单元160可以缺席，例如当计算设备100接收编码的输入和/或在编码输出中报告时。编码单元170和/或解码单元160可以实现为单独单元，例如实现为编码设备和/或解码设备160。

[0043] 环编码单元170可以包括布置成存储针对一个或多个基础环元素(u)定义的编码

表的存储库172，该编码表将环元素(x)映射到整数列表((a,b))，使得环元素等于一个或多个基础环元素的幂的线性组合($x = u^a - u^b$)，其中所述幂具有由整数列表确定的指数。编码单元170可以在算子存储装置150中存储编码的环元素。编码单元170允许系统利用明文信息工作。

[0044] 环解码单元160被布置成针对一个或多个基础环元素(u)确定环元素(x)，使得该环元素等于一个或多个基础环元素的幂的线性组合($x = u^a - u^b$)，其中所述幂具有由整数列表确定的指数。例如，解码单元160可以包括存储将整数列表映射到环元素的解码表的存储装置。例如，解码单元160可以包括演算单元以用于演算所述幂及其线性组合。

[0045] 许多有趣的实施例省略了编码和解码单元160和170中的一个或二者。例如，计算设备100可以被配置成通过计算机网络(比如因特网)接收编码信息。混淆计算设备100在其上运行的系统(例如执行混淆计算软件的计算机)的所有者可能不知晓用于输入信息的编码，也不知道由系统100输出(例如通过计算机网络传输回来)的信息的编码。相应地，即使在云中执行计算，信息的所有人具有他的信息是安全的某种保证。使用密码术(比如加密)在编码形式的信息上操作典型地是不可能的。即使表系统如背景技术中概述的那样使用，这要求双重表。

[0046] 典型地，计算单元100包括微处理器(未示出)，其执行设备100处存储的适当的软件；例如，该软件可能已经被下载的和/或存储在对应的存储器中，例如诸如RAM之类的易失性存储器或诸如闪存之类的非易失性存储器(未示出)。可替换地，设备100 可以整体地或部分地在可编程逻辑中实现，例如实现为现场可编程门阵列(FPGA)。设备100可以整体地或部分地实现为所谓的专用集成电路(ASIC)，即针对其特定用途定制的集成电路(IC)。

[0047] 在一个实施例中，电子计算设备包括环加法电路和环乘法电路，其被布置成执行对应单元的功能。计算设备还可以包括取反电路。该电路可以是例如通过以硬件描述语言(比如混合语言(Verilog)和VHDL)描述功能而获得的集成电路，比如CMOS。这些电路可以是处理器电路和存储电路，该处理器电路执行存储电路中电子地表示的指令。这些电路也可以是FPGA、ASIC等等。

[0048] 表存储装置110和运算数存储装置150可以实现为电子存储库，例如存储器。两种存储装置可以是相同存储器的部分，但是它们可以是不同的存储器。表存储装置110可以非易失性、不可写的，比如ROM，或写一次读许多次(WORM)存储器。运算数存储装置150可以是易失性或非易失性可写存储器，比如闪存或RAM。

[0049] 图2示意性示出计算设备101的实施例的一个示例。计算设备101是计算设备100的改善。在一个实施例中，计算设备101包括多个环加法单元、多个乘法单元以及可选地多个取反单元。例如，图2示出三个乘法单元 1401.1、140.2和140.3以及两个加法单元130.1和130.2。这些单元可以具有分别与单元140和130相同的设计。乘法和加法单元采取相对较小的空间，例如当在软件中实现时，这些单元不需要超过数百个低水平计算机指令。特别地，加法和/或乘法单元的副本可以用于计算机程序中所需的每一个乘法或加法。这允许传统的混淆技术。作为一个示例，图2示出如何可以使用混淆算术演算多项式ax^2+bx+c。

[0050] 多个算术单元的运算(例如，加法、乘法、取反)可以以其数据相关性所允许的任何顺序来排序。例如，运算140.3可以插入在排序140.1、140.2、130.1和130.2中的130.1之前的任一点处。而且，后续的乘法或加法的排序可以颠倒。因而，像图2那样的图可以在用于软

件程序的线性排序中以许多方式来解释。不需要将各单元严格地分离;用于第一单元的指令可以穿插有用于另一单元的指令。

[0051] 图3示意性示出用于演算用在计算设备中的增量表的表演算设备200的实施例的一个示例。增量表可以用在像计算设备100那样的设备中。增量表可以存储在非暂时性存储设备上,例如硬盘、非易失性存储器芯片等。

[0052] 表演算设备200包括被布置成构造增量表的表创建单元210。例如,表创建单元可以被布置成:

- 反复地选择输入环元素,例如x,

- 确定等于增量环元素环加到输入环元素的输出环元素。例如,如果增量值为1,则$y=x+1$。

- 确定针对输出环元素编码的输出整数列表。例如,表演算设备200可以包括像编码单元170那样的编码单元。

- 向将输入环元素映射到输出整数列表的增量表添加条目。

[0053] 这些步骤可以被执行,直到所有环元素都被映射到整数列表。在一些实施例中,元素可以被跳过,构建部分增量表;例如,可能从上下文得知某些环元素将不会出现。

[0054] 给定环R、潜在的基础环元素u、编码(比如示例编码)和整数列表长度(比如2),可以生成如下给出的解码表。令k为u的次数。

- 生成所有整数列表,例如通过生成整数列表长度的所有整数列表且允许从0直到k(但不包括k)的所有整数用于列表中的每一个位置。例如,生成:(0,0),(0,1),(1,0),(1,1),(0,2),(1,2),(2,2)(2,0),(2,1),(0,3),...等等

- 对于每一个所生成的整数列表,演算通过整数列表编码的环元素,并且向与将整数列表关联到解码的解码表添加条目。

[0055] 尽管解码可能使用或可能不使用解码表,但是这样的表也是有用的,因为编码表可以从解码表生成,例如通过对用于环元素的表进行分类来生成。可能发生的是,环元素具有多个编码。例如,环元素0(用于加法的中性元素)可以在示例编码中针对任意a而表示为(a,a)。这样的多个编码可以从表中移除,例如通过删除用于给定环元素的多个条目中除了1之外的所有条目;或者通过在表中留下所述多个编码并且使用编码表来对多个条目中随机的一个条目进行编码。

[0056] 构造解码或编码表还可以用于找出环元素u是否是基础环元素。如果构造编码表失败,因为事实证明一些环元素不具有编码,那么u不是基础环元素。

[0057] 下面呈现编码、增量表、环加法方法以及环乘法方法的若干实施例。计算设备100的取反、加法和乘法单元可以被配置用于这些实施例中任意一个。所有示例适用于任何交换环,特别是$\mathbb{Z}_n$和$\mathbb{Z}_n[x]/f(x)$。本文中,n是正整数。而且,非常优选的是,交换环的任何元素可以在选择的编码中表示。不是所有交换环都允许所有元素在给定的编码中表示,例如表示为给定类型的整数列表表示。给定交换环R,我们将假定如果R中的任何元素可以使用给定的编码类型表示为整数列表,则它允许完全同质的混淆。本领域技术人员可以验证,在给定编码的情况下,给定的交换环是否允许完全同质的混淆,例如通过生成所有许可的编码并验证它们一起表示给定环的所有元素。对于某些应用,可能允许的是,所述编码具有一些间隙。这可能具有如下后果:算术无法在那些间隙上执行,至少不使用混淆整数列表编

码。下面进一步呈现允许特定类型的编码的交换环的特定示例。

[0058] 下面首先给出示例编码的描述。存在许多类型的编码，其共同之处在于环元素可以表示为整数的列表。这些整数不是环元素，例如即使环不是整数环(比如多项式环)，则尽管如此元素可以表示为整数列表。所使用的编码、给定的整数列表如何映射到环元素被称为编码。典型地，整数列表将总是具有相同的长度，然而这不是必需的。一般地，随着编码允许更多类型的整数列表(例如更长列表)，变得更有可能的是给定的环元素可以以不同方式被编码为整数列表。

[0059] 给定具有示例编码的交换环R，存在特殊元素u，使得对于某些整数a_1和a_2，R中任何元素a可以被写作$u^{a_1}-u^{a_2}$。我们将这样的特殊环元素称为基础环元素。不是所有交换环都可以以这种方式进行编码，而是它们中的足够多对于编码将是有用的。整数a_1和a_2自身不是环R的环元素；它们是基于对基础元素的次数取模而运算的整数。注意到，环元素a等于基础元素u的幂的线性组合，即u^{a_1}和u^{a_2}的线性组合；在此情况下，该线性组合通过将所述幂与+1或-1相乘并且将它们求和而获得，更特别地，通过从第一幂减去第二幂而获得。计算设备在以上述方式编码的环元素上运算。加法、取反和乘法单元可以在这个编码中的环元素上运算。

[0060] 增量表T在加法和乘法运算二者中发挥中心作用。增量表映射输入环元素，在此情况下输入环元素可以表示为整数列表。例如，给定表示输入环元素$k=u^{k_1}-u^{k_2}$的输入整数列表(k_1,k_2)，表T将此映射到输出整数列表，例如$T((k_1,k_2))=(l_1,l_2)$，其对输出环元素$l=u^{l_1}-u^{l_2}$进行编码。输出环元素等于增量环元素环加到输入环元素。在此示例中，增量元素可以被取为1，即，为用于环乘法的单位元素的环元素；在此情况下，$l=k+1$。方便的是，该表可以直接应用到使用相同编码的环元素，并且因而其可以应用于具有整数列表表示的环元素。尽管如此，存在其中表应用于在可替换的编码中的环元素的实施例。该可替换编码也可以是整数列表，但是具有可替换类型。再者，增量环元素不必是1。

[0061] 下面描述运算、取反、加法和乘法。

[0062] 取反。给定表示取反输入环元素$a=u^{a_1}-u^{a_2}$的取反输入整数列表(a_1,a_2)，可以通过置换整数列表、在此情况下通过颠倒顺序来获得取反输出整数列表。取反输出整数列表可以是(a_2,a_1)。假设存在m，使得$u^m=-1$(其在许多环R上发生)，取反可以可替换地通过将常数(例如m)加到整数列表的每一个整数而获得。在后者的情况下，取反输出整数列表可以是(a_1+m,a_2+m)。这是起作用的，因为$-a=u^{a_2}-u^{a_1}=u^{a_1+m}-u^{a_2+m}$。整数列表中的算术优选地以对基础元素的次数取模来进行。这里，整数列表的整数对应于基础元素的指数，因此以对基础元素的次数取模同余的整数对相同的环元素编码。

[0063] 加法。为了将接收的对第一加法输入环元素$a=u^{a_1}-u^{a_2}$编码的第一加法输入整数列表(a_1,a_2)与对第二加法输入环元素$b=u^{b_1}-u^{b_2}$编码的第二加法输入整数列表(b_1,b_2)相加，首先确定对中间加法环元素c编码的中间加法整数列表$((c_1,c_2))$。

[0064] 环元素c可以是第一加法输入环元素a加上基础元素u的从第二加法输入整数列表确定的幂，特别是第二加法输入整数列表的第一个整数。在此示例中，我们可以有$c=u^{a_1}-u^{a_2}+u^{b_1}$。为了演算后者，我们观察到$c=u^{a_1}-u^{a_2}+u^{b_1}=(u^{a_1-b_1}-u^{a_2-b_1}+1)u^{b_1}$。括号中的

项可以使用增量表在编码中重写。通过增量表针对环元素$u^{a_1-b_1}-u^{a_2-b_1}$的第一应用，获得了元素$u^{a_1}-u^{a_2}=u^{a_1-b_1}-u^{a_2-b_1}+1$。例如，通过$T((a_1-b_1,a_2-b_1))=(d_1,d_2)$。然后我们有，$c_1=d_1+b_1$和$c_2=d_2+b_1$，从而确定中间加法整数列表$((c_1,c_2))$可以进一步包括将从第二加法输入整数列表确定的整数加到源自第一应用的整数列表中的整数。将u^{b_1}加到整数列表表示中的环元素(在此情况下加到a)有时被称为正约简步骤。

[0065] 因而，加法单元已经获得中间加法环元素$c=u^{a_1}-u^{a_2}+u^{b_1}=u^{c_1}-u^{c_2}$，作为整数列表$(c_1,c_2)$。该中间加法环元素因而是一个或多个基础元素的幂的线性组合，其中所述幂从第一和第二加法输入整数列表确定。在此情况下，增量表被应用于环元素$u^{a_1-b_1}-u^{a_2-b_1}$，其通过一个或多个基础元素(u)提升至以第一整数列表的第一整数(a_1)减去第二整数列表的第一整数(b_1)为指数的幂减去基础环元素(u)提升至以第一整数列表的第二整数(a_2)减去第二整数列表的第一整数(b_1)为指数的幂而形成。

[0066] 在此示例中，加法输出整数列表可以通过增量表针对从中间加法整数列表和第二加法输入整数列表确定的环元素的第二应用来确定。这可以包括演算中间加法环元素c的和并减去基础元素提升至从第二加法输入整数列表确定的幂(例如第二加法输入整数列表的第二整数b_2)：$c-u^{b_2}=u^{c_1}-u^{c_2}-u^{b_2}$。这可以在增量表的第二应用之前通过对由中间加法整数列表表示的中间加法环元素取反而实现。c的取反可以如上文所指示的那样进行。作为示例，我们使用置换，但是相同的运算可以通过将常数加到指数来执行。在取反之后，所述和可以使用加(而非减)基础元素提升至从第二加法输入整数列表确定的幂：$-c+u^{b_2}=u^{c_2}-u^{c_1}+u^{b_2}$。后者运算具有与上文相同的类型，并且可以以与加上$u^{b_1}$相同的方式通过表应用来执行。在此之后，结果再次被取反。该完全加法可以使用相同增量表T的两次取反和两个表应用。

[0067] 从整数列表表示中的环元素(在此情况下从c)减去$-u^{b_2}$有时被称为取反约简步骤。取反约简步骤可以通过取反、执行正约简步骤以及再次取反来执行。

[0068] 乘法。为了使接收的对第一乘法输入环元素$r=u^{r_1}-u^{r_2}$编码的第一乘法输入整数列表(r_1,r_2)与对第二乘法输入环元素$s=u^{s_1}-u^{s_2}$编码的第二乘法输入整数列表$((s_1,s_2))$相乘，确定第一中间乘法整数列表(t_1,t_2)和第二中间乘法整数列表(u_1,u_2)。从第一和第二中间元素确定对乘法输出环元素编码的乘法输出整数列表。在其他实施例中，可能存在超过两个中间乘法整数列表。我们有，$r\cdot s=(u^{r_1}-u^{r_2})(u^{s_1}-u^{s_2})=u^{r_1+s_1}-u^{r_1+s_2}+u^{r_2+s_2}-u^{r_2+s_1}=(u^{r_1+s_1}-u^{r_1+s_2})+(u^{r_2+s_2}-u^{r_2+s_1})=t+u$。在展开乘积中的关于两项t和u分开各项可以以不同方式进行，例如，分开为$(u^{r_1+s_1}-u^{r_2+s_1})+(u^{r_2+s_2}-u^{r_1+s_2})$。

[0069] 因而，为了使表示为整数列表的两个环元素相乘，它们可以被变换成可以被相加的两个新的整数列表以获得该乘法的答案。该加法可以如上文所述那样进行。例如，乘法单元可以演算中间整数列表并且将它们发送至乘法单元。

[0070] 例如，第一中间乘法整数列表的第一整数t_1可以包括第一乘法输入整数列表的第一整数r_1加上第二乘法输入整数列表的第一整数s_1，并且第一中间乘法整数列表的第二整数t_2可以包括第一乘法输入整数列表的第一整数r_1加上第二乘法输入整数列表的第二整数

s_2,$t_1 = r_1 + s_1, t_2 = r_1 + s_2$;第二中间乘法整数列表的第一整数$u_1$可以包括第一乘法输入整数列表的第二整数$r_2$加上第二乘法输入整数列表的第二整数$s_2$,并且第二中间乘法整数列表的第二整数$u_2$可以包括第一乘法输入整数列表的第二整数$r_2$加上第二乘法输入整数列表的第一整数$s_1$,$u_1 = r_2 + s_2, u_2 = r_2 + s_1$。

[0071] 在一个实施例中,例如在刚刚公开的示例中,算术在整数列表上执行,环元素不需要作为某种自然表示的环元素被计算。现在,讨论若干变形。许多变形是独立的,例如变形的编码可以与执行加法的变形组合。

[0072] 通过在整数列表中执行计算(例如对应于$u^{a_1-b_1}$等)时的混淆算术,所述值可以以对u的次数取模进行约简。例如,如果u的次数为30,则所有演算可以以对30取模来执行。

[0073] 增量值。增量值不必是1。存在至少两种使用不同增量值的方式。首先,等式$c = u^{a_1} - u^{a_2} + u^{b_1} = (u^{a_1-b_1} - u^{a_2-b_1} + 1)u^{b_1}$可以被修改成$c = u^{a_1} - u^{a_2} + u^{b_1} = (u^{a_1-b_1+t} - u^{a_2-b_1+t} + u^t)u^{b_1-t}$。这意味着,可以构造加上值$u^t$的增量表。此增量表被应用于相同的整数列表,除了加上整数t之外。在增量表的第一应用之后,加上数字$b_1 - t$而非b_1。

[0074] 改变增量值的另一种方式是取R的两个元素g和p,使得环中的g的反复相加给出p。例如,存在整数h,使得$h \cdot g = g + \cdots + g = p$。假设存在具有增量值$p$的增量表$T_p$,例如,$p = 1$或$p = u^t$。增量表$T_g$可以针对作为增量值的$g$构造。表$T_g$可以被应用$h$次以获得与直接应用$T_p$相同的效果。使用具有不同增量值的不同增量表甚至可以在单个实施例中组合,例如以增强混淆。后者的构造具有以下优点:多个增量表可以组合,而不改变后面的加法演算。

[0075] 增量表的构造也可以变化。例如,返回到用于中间加法环元素的等式,但是取代因式分解为$c = u^{a_1} - u^{a_2} + u^{b_1} = (u^{a_1-b_1} - u^{a_2-b_1} + 1)u^{b_1}$的是,进行下面的观察:$c = u^{a_1} - u^{a_2} + u^{b_1} = (u^{a_1-a_2} + u^{b_1-a_2} - 1)u^{a_2}$。使用此公式,可以针对增量值-1构造增量表。此类型的增量表被应用于环元素$u^{a_1-a_2} + u^{b_1-a_2}$。此环元素没有示例编码。尽管如此,该环元素可以表示为整数列表,例如表示为(a_1-a_2, b_1-a_2),使得此增量表取整数列表作为输入并且产生作为输出的整数列表。然而,不同于先前的示例,该输入整数列表具有与输出编码不同的编码。而且,尽管非常优选的是到加法单元的输入中使用的编码没有间隙,即任何环元素可以在此编码中表示,但是并不需要此增量表的此可替换输入编码没有间隙;需要表示为表输入的所有元素可以通过构造表示。

[0076] 在将增量表应用到环元素$u^{a_1-a_2} + u^{b_1-a_2}$,例如表示为整数列表$(a_1-a_2, b_1-a_2)$,整数$a_2$被加到增量表的输出的两个元素。结果是如上文所定义的中间值c。为了执行第二表应用,可以使用与上文相同的构造:取反、使用此可替换增量表加u^{b_2}、再次取反。使用上文所指示的构造,增量值可以从-1变化到其他值。

[0077] 将增量表应用到环元素$u^{a_1-a_2} + u^{b_1-a_2}$具有明显优点,表达式是对称的,从而$T(a_1 - a_2, b_1 - a_2) = T(b_1 - a_2, a_1 - a_2)$,使用整数列表表达式为输入值。这进

而允许以压缩形式存储增量表，该表的大约一半不需要存储。例如可能仅在$x <= y$时存储$T(x,y)$。此方法的轻微的潜在缺点是中间整数列表使用不同的编码。

[0078] 作为另外的变形，增量表也可以适用于$u^{a_2-a_1} - u^{b_1-a_1}$。

[0079] 针对示例编码说明的原理可以应用于若干可替换编码。第一可替换编码是使用编码$a = u^{a_1} + u^{a_2}$将环元素a编码为整数列表(a_1,a_2)。具有基础环元素u以使得任何环元素可以以此方式编码的环被说成允许正混淆算术。示例编码将被称为负混淆算术。可以在数学上证明，对于允许正混淆算术的具有基础环元素u的任何环，存在整数m，使得$u^m = -1$。而且，当且仅当这样的值m存在时，允许负混淆算术的环允许正混淆算术。允许正混淆算术的任何环也允许负混淆算术，尽管反之不成立。

[0080] 正混淆算术很大程度上遵循与上文概述的针对负混淆算术相同的线(line)。简言之，整数列表的符号的改变可以通过将值m加到整数列表中的所有整数来完成。给定加法输入$a = u^{a_1} + u^{a_2}$和$b = u^{b_1} + u^{b_2}$，该加法可以通过演算中间者$c = u^{a_1} + u^{a_2} + u^{b_1}$来执行，例如通过$(u^{a_1-b_1} + u^{a_2-b_1} + 1)u^{b_1}$来执行。增量表适用于$u^{a_1-b_1} + u^{a_2-b_1}$，其中增量值为1。正约简可以应用两次，两次都针对$u^{b_1}$和$u^{b_2}$，没有负约简是必需的。这简化了加法。通过对u的不同幂进行因式分解，增量表的构造可以如上文所指示变化。增量表可以如上文所示变化。正混淆算术具有以下优点：增量表总是对称的，并且可以以压缩形式存储。正混淆的一个缺点是较少的环允许此类型的编码。

[0081] 迄今为止给定的编码可以可选地乘以恒定环元素$w=u^v$(对于某个v)。因而，整数列表(a_1,a_2)可以表示环元素$a = w(u^{a_1} - u^{a_2})$。取反步骤不变。正约简步骤变成$c = wu^{a_1} - wu^{a_2} + w u^{b_1} = (wu^{a_1-b_1} - wu^{a_2-b_1} + w)u^{b_1}$。增量表可以使用$w$作为增量值，并且应用到$wu^{a_1-b_1} - wu^{a_2-b_1}$，其具有相同的编码类型。负约简步骤可以从如上文所指示的正约简步骤导出。所述乘法可以使用$r \cdot s = (wu^{r_1} - wu^{r_2})(wu^{s_1} - wu^{s_2}) = (wu^{r_1+s_1+v} - wu^{r_1+s_2+v}) + (wu^{r_2+s_2+v} - wu^{r_2+s_1+v}) = t + u$使$r = wu^{r_1} - wu^{r_2}$和$s = wu^{s_1} - wu^{s_2}$（其被表示为整数列表$(r_1,r_2)$和整数列表$(s_1,s_2)$）相乘。

[0082] 一种另外的可替换编码通过$a = u^{a_1}(u^{a_2} - u^{-a_2})$给出或通过$u^{a_1}(\frac{u^{a_2} - u^{-a_2}}{2})$乘以常数½给出。可以证明，对于允许负混淆算术的具有含有奇数次数的基础元素u的环，任何环元素x可以被写作$u^{a_1}(\frac{u^{a_2} - u^{-a_2}}{2})$。这改变了编码，例如从整数列表到环元素的映射。如果环具有负混淆，则它也允许这种表示，假如基础环元素具有奇数次数。

[0083] 加法和乘法步骤可以相应地适应于不同的编码。例如，给定编码形式的数字$a = u^{a_1}(u^{a_2} - u^{-a_2})$，可以演算$a_1$和$a_2$中的$a'_1$和$a'_2$，使得$a = u^{a'_1} - u^{a'_2}$，例如通过以对$u$的次数取模演算$a_1 + a_2$和以对$u$的次数取模来演算$a_1 - a_2$。使用后者的整数，可以使用如上文那样的加法和乘法。

[0084] 我们为获得双曲线表示而做过的事情可以被概括为任何种类的线性变换，并且如果变换可能是可逆的，则新的表示等效于原始表示。

[0085] 假定我们有表示$a = u^{a_1} - u^{a_2}$，以及以矩阵形式写的关系：

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} m & n \\ o & p \end{pmatrix} \begin{pmatrix} a_3 \\ a_4 \end{pmatrix}$$

如果变换具有行列式$mp - no$，则a_3和a_4的表示等效于其他，其中$mp - no$为环$\mathbb{Z}_k$中的单元；k为环R中的u的次数。当且仅当$\gcd(mp - no, k) = 1$时，这是成立的。双曲线表示是一个示例(包括与½相乘)并且要求k为奇数，因为在此情况下，所述变换的行列式为2(或-2)。

[0086] 我们将利用另一个示例解释所述方法。考虑环$\mathbb{Z}_{79}$并取u=8。此元素具有次数k=13，并且我们知晓$\mathbb{Z}_{79}$中的所有元素对某些指数而言可以被写成差$u^{a_1} - u^{a_2}$。考虑变换$M = \begin{pmatrix} 10 & 8 \\ 6 & 4 \end{pmatrix}$。行列式为5模13，所以该矩阵具有逆；其为$M^{-1} = \begin{pmatrix} 6 & 1 \\ 4 & 2 \end{pmatrix}$。

[0087] 我们知道，对于$\mathbb{Z}_{79}$中的每一个x，我们可以找到α和β，使得$x = 8^{\alpha} - 8^{\beta}$，但是使用此变换，我们直接推断出对于所有$x$，我们可以找到$\gamma$和$\delta$，使得$x = 8^{10\gamma+8\delta} - 8^{6\gamma+4\delta}$。

[0088] 这表明表示的大类是等效的。线性变换可以推广到仿射变换，如果我们包括两个加法常数r、s，使得

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} m & n \\ o & p \end{pmatrix} \begin{pmatrix} a_3 \\ a_4 \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix}。$$

[0089] 如果线性编码M可以取逆，此变换可以取逆。

[0090] 整数列表中整数的数量。在迄今所讨论的示例中，整数列表中元素的数量总是2。此数量具有优势，即它减少了演算步骤的数量。另一方面，允许在整数列表中的更多元素扩大了允许混淆的环的数量。下面的示例考虑每列表三个整数，但是更多是可能的且工作类似。

[0091] 考虑分别对元素$u^{a_1} + u^{a_2} + u^{a_3}$和$u^{b_1} + u^{b_2} + u^{b_3}$编码的第一整数列表$(a_1, a_2, a_3)$和第二整数列表$(b_1, b_2, b_3)$。取反可以通过将常数m加到列表中的整数来进行。加法可以通过增量表针对第二整数列表中的每一个整数的应用来进行，在此情况下应用三次。第一中间加法整数列表可以从$u^{a_1} + u^{a_2} + u^{a_3} + u^{b_3} = (u^{a_1-b_3} + u^{a_2-b_3} + u^{a_3-b_3} + 1)u^{b_3}$演算。在此情况下，增量值为1并且增量表适用于$u^{a_1-b_3} + u^{a_2-b_3} + u^{a_3-b_3}$。为了相乘，形成与第二整数列表中相同数量的中间乘法整数列表，例如：$(a_1 + b_1, a_2 + b_1, a_3 + b_1)$，$(a_1 + b_2, a_2 + b_2, a_3 + b_2)$，$(a_1 + b_3, a_2 + b_3, a_3 + b_3)$。

[0092] 多个不同的基础环元素。考虑两个具有指数的基础元素u和v，使得$u^s = v$且$v^t = u$。整数列表(a_1, a_2)对环元素$\alpha = u^{a_1} - v^{a_2}$编码；对$(b_1, b_2)$类似。取反通过将$(a_1, a_2)$映射到$(sa_2, ta_1)$获得。正约简步骤$u^{a_1} - v^{a_2} + u^{b_1} = (u^{a_1-b_1} - v^{a_2-tb_1} + 1)u^{b_1}$。增量值为1，且该表适用于整数列表$(a_1 - b_1, a_2 - tb_1)$。负约简可以使用取反而被简化为正约简。乘法可以简化为加法。

[0093] 下面给出用于允许负和/或正混淆的环的示例。

[0094] 环R可以是整数环$\mathbb{Z}_n$，其中模数为n。

[0095] 例如，n可以是13，其中基础环元素u=4。此元素具有次数6。下面，使用示例编码将所有环元素0-6编码为整数列表。注意到，这里所有的元素具有多个编码。对于所列出的第一编码，给出了映射示例，该映射示例展示了在给定整数列表情况下如何可以找到对应的环元素。环元素7-12可以被发现是对环元素1-6取反。

环元素	整数列表	映射示例
0	(x，x)，对于任意 0<=x<6	4^x-4^x
1	(1，2)，(5，4)	4^1-4^2
2	(0，3)，(2，0)，(3，5)	4^0-4^3
3	(1，0)，(3，4)	4^1-4^0
4	(0，5)，(2，3)	4^0-4^5
5	(0,4)，(1,3)，(4,1)	4^0-4^4
6	(2,5)，(4,2)，(5,1)	4^2-4^5

[0096] 此示例也允许正混淆，在此环中为4^3=-1。

[0097] 允许负混淆的n和u的其他值为：n=151，u=2；n=87，u=20；n=79；u=8等等。

[0098] 发明人已经发现允许负和/或正编码的环的大量实例。注意到，许多变形是可从给定的负和/或正编码导出的，如本文所描述。

[0099] 环R可以是多项式环$\mathbb{Z}_n[x]/f(x)$，对于多项式f以及模数n。多项式不需要是不可约的。如果f不是不可约的，我们得到不是域的交换环。事实证明，任何交换多项式环R允许混淆。

[0100] 例如，给出若干域

域F(2^6)

此域与F2 [x]/(x^6 + x^4 + x^3 + x + 1)同构。基u = x^3具有次数21。

[0101] 域F(2^8)

此域与F2 [x]/(x^8 + x^4 + x^3 + x^2 + 1)同构。

[0102] 基u = x^3具有次数85。

[0103] 基u = x + 1具有次数51。

[0104] 域F(2^10)

此域与F2[x]/(x^10 + x^6 + x^5 + x^3 + x^2 + x + 1)同构。

[0105] 基u = x^3 具有次数341。

[0106] 基u = x^7 + x^6 + x^4 + x^3 + x^2 + x 具有次数93。

[0107] 域F(2^12)

此域与F2 [x]/(x^12 + x^7 + x^6 + x^5 + x^3 + x + 1)同构。

[0108] 基u = x^3 具有次数1365。

[0109] 基u = x^5 具有次数819。

[0110] 基u = x^7 具有次数585。

[0111] 基u = x^9 具有次数455。

[0112] 基u = x^8 + x^7 + x^6 + x^4 + x^2 + x具有次数315.

基u = x^10 + x^9 + x^8 + x^6 + x^4 + x^3具有次数273。

[0113] 基u = x^11 + x^10 + x^7 + x^5 + x^3 + x^2 + x + 1具有次数195。

[0114] 图4示意性示出用于在交换环（例如 $\mathbb{Z}_n; \mathbb{Z}_n[x]/f(x)$）中执行混淆算术的计算方法300的实施例的一个示例，该环具有有限数量的环元素，在环元素上定义了环加法和环乘法，该计算方法在对环元素（$u^{a_1} - u^{a_2}$）编码的整数列表（(a_1, a_2)）上操作，整数列表包括至少两个整数。该计算方法包括：

- 存储针对增量环元素（1；u^t）定义的增量表（T），该增量表将输入环元素（$k = u^{k_1} - u^{k_2}$）映射到对输出环元素（$l = u^{l_1} - u^{l_2}$）编码的输出整数列表（$T((k_1, k_2)) = (l_1, l_2)$），使得输出环元素等于增量元素环加到输入环元素（$l$=$k$+1），

- 环加，该环加包括：

- 接收310对第一加法输入环元素编码的第一加法输入整数列表（(a_1, a_2)）和对第二加法输入环元素编码的第二加法输入整数列表（(b_1, b_2)），

- 通过将增量表应用到从第一和第二加法输入整数列表确定的环元素来确定320对加法输出环元素编码的加法输出整数列表，该加法输出环元素等于第一加法输入环元素和第二加法输入环元素的环加，

- 环乘，该环乘包括：

- 接收330对第一乘法输入环元素编码的第一乘法输入整数列表（(r_1, r_2)）和对第二乘法输入环元素编码的第二乘法输入整数列表（(s_1, s_2)），

- 通过将增量表应用到从第一和第二乘法输入整数列表确定的环元素来确定340对乘法输出环元素编码的乘法输出整数列表，该乘法输出环元素等于第一乘法输入环元素和第二乘法输入环元素的环乘。

[0115] 图5示意性示出加法方法400的实施例的一个示例，该加法方法可以用在设备100或用在方法300中等等。此示例使用示例编码。该方法可以适应于其他编码。可以应用本文描述的所有变形；此示例使用增量值1并且增量表通过因式分解出u^{b_1}构造。

[0116] 方法400包括接收加法运算数410。这可以包括接收410第一加法输入整数列表，例如(a_1, a_2)，以及接收420第二加法输入整数列表，例如(b_1, b_2)。

[0117] 方法400进一步包括确定420中间加法整数列表，例如(c_1, c_2)。例如，这可以包括将增量表应用到从第一和第二加法输入整数列表确定的环元素。特别地，增量表可以被应用于整数列表，整数中的元素从输入整数列表中的元素导出。

[0118] 例如，确定420可以包括将增量表应用422到$(a_1 - b_1, a_2 - b_1)$，例如获得(d_1, d_2)；将从第二加法输入整数列表确定的整数b_1加424到源自第一应用的整数列表中的整数，例如，$(c_1, c_2) = (d_1 + b_1, d_2 + b_1)$。

[0119] 方法400进一步包括通过增量表针对从中间加法整数列表和第二加法输入整数列表确定的环元素的第二应用来确定430加法输出整数列表。对于更长的整数列表，这可以涉及附加的增量表应用。例如，这可以包括对中间加法整数列表取反431，例如，置换成(c_1, c_2)。应用432增量表以及相加434与应用422和相加424相同，除了加法输入整数列表(a_1, a_2)被中间整数列表(c_2, c_1)和b_1乘b_2替代。最后，434的结果被取反453以获得混淆加

法的结果。

[0120] 如果取代负混淆，如这里那样使用正混淆，那么可以省略取反431、435。

[0121] 图6示意性示出乘法方法500的实施例的一个示例，其可以用在设备100或方法300等等中。此示例使用与方法400相同的编码和增量表。

[0122] 方法500包括接收乘法运算数510。这可以包括接收510第一乘法输入整数列表，例如(r_1, r_2)，以及接收514第二乘法输入整数列表(s_1, s_2)。

[0123] 方法500进一步包括确定520第一和第二中间乘法整数列表。例如，520可以包括确定522第一中间乘法整数列表和确定524第二中间乘法整数列表。这些可以例如分别被选择为$(s_1 + r_1, s_1 + r_2)$和$(s_2 + r_2, s_2 + r_1)$，尽管存在其他选择。所述乘法通过在加法方法400中增加这些数字继续。

[0124] 注意到，所述表仅用在应用422和应用432中，而没有应用在方法400和500中的任何其他地方。加法和乘法二者使用相同的表，并且二者以相同次数(2)使用表。其他运算包括在整数列表中的整数上进行的小算术运算，例如对基础环元素的次数取模。

[0125] 执行方法的许多不同方式是可能的，如对本领域技术人员而言将是显然的。例如，可以改变步骤的次序并且可以并行执行一些步骤。而且，在各步骤之间可以插入其他方法步骤。所插入的步骤可以表示诸如本文所描述之类的方法的改进，或者可以与该方法无关。而且，给定的步骤可能没有在下一步骤开始之前完全结束。

[0126] 根据一个实施例的一种方法可以使用软件执行，该软件包括用于促使处理器系统执行方法300、400和500中任何一种的指令。软件可以只包括系统的特定子实体所采取的那些步骤。软件可以存储在适当的存储介质中，比如硬盘、软盘、存储器等。软件可以作为信号沿着线缆、或无线或使用数据网络(例如因特网)而被发送。可以使得软件可用于下载和/或在服务器上远程使用。一种方法可以使用位流执行，该位流被布置成配置可编程逻辑(例如现场可编程门阵列(FPGA))以执行该方法。

[0127] 应当领会，实施例也扩展到计算机程序，特别是载体上或载体中的计算机程序，其适于使实施例付诸实践。该程序可以是源代码、目标代码、代码中间源和目标代码形式(比如部分编译的形式)，或者是适合用于依照一个实施例的方法的实现方式中任何其他形式。一个涉及计算机程序产品的实施例包括对应于所阐述的方法的至少一个的每一个处理步骤的计算机可执行指令。这些指令被细分成子例程和/或存储在一个或多个可以静态或动态链接的文件中。另一个涉及计算机程序产品的实施例包括对应于所阐述的系统和/或产品的至少一个的每一个构件的计算机可执行指令。

[0128] 图7a示出具有包括计算机程序1020的可写部分1010的计算机可读介质1000，该计算机程序1020包括用于致使处理器系统执行依照一个实施例的用于执行混淆算术的计算方法的指令。该可写部分可以被布置用于多次写入或用于仅一次写入。计算机程序1020可以作为物理标记或借助于计算机可读介质1000的磁化而体现在计算机可读介质100上。然而，任何其他适当的实施例也是可想到的。而且，应当领会，尽管计算机可读介质1000在这里被作为光盘示出，但是计算机可读介质1000可以是任何适当的计算机可读介质，比如硬盘、固态存储器、闪存等，并且可以是非可记录或可记录的。计算机程序1020包括用于致使处理器系统执行用于执行混淆算术的所述计算方法的指令。

[0129] 计算机可读介质，例如计算机可读介质1000，可以包括增量表、和/或解码表、和/

或编码表。

[0130] 图7b示出依照一个实施例的处理器系统1100的示意性表示。该处理器系统包括一个或多个集成电路1110。图7b中示意性示出了一个或多个集成电路1110的架构。电路1110包括用于运行计算机程序组件以执行依照一个实施例的方法且/或实现起模块或单元的处理单元1120，例如CPU。电路1110包括用于存储编程代码、数据等的存储器1122。存储器1122的部分可以是只读的。电路1110可以包括通信元件1126，例如天线、连接器或二者等等。电路1110可以包括用于执行所述方法中限定的部分或所有处理的专用集成电路1124。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由互连1130(比如总线)连接到彼此。处理器系统1110可以被布置用于分别使用天线和/或连接器的接触式和/或非接触式通信。

[0131] 应当注意，上述实施例说明而非限制本发明，并且本领域技术人员将能够设计许多可替换实施例。

[0132] 在权利要求中，置于括号之间的任何附图标记不应当被解释为限制权利要求。动词“包括”及其词形变化的使用不排除存在权利要求中非陈述的其他元件或步骤。元件之前的冠词“一”并没有排除存在多个这样的元件。本发明可以借助于包括若干不同元件的硬件、且借助于适当编程的计算机实现。在列举了若干构件的设备权利要求中，这些构件中的若干个可以由同一硬件项体现。在相互不同的从属权利要求中记载了某些措施的起码事实并不指示这些措施的组合不可以用于获益。

[0133] 在权利要求中，括号中的参考是指实施例的附图中的附图标记或者指实施例的公式，从而增加权利要求的可理解性。这些参考不是详尽的并且不应当解释为限制权利要求。

[0134] 图1中参考数字的列表

100	计算设备
110	布置成存储增量表的存储库
120	环取反单元
130	环加法单元
140	环乘法单元
150	运行数存储装置
160	解码单元
170	编码单元
172	布置成存储编码表的存储库

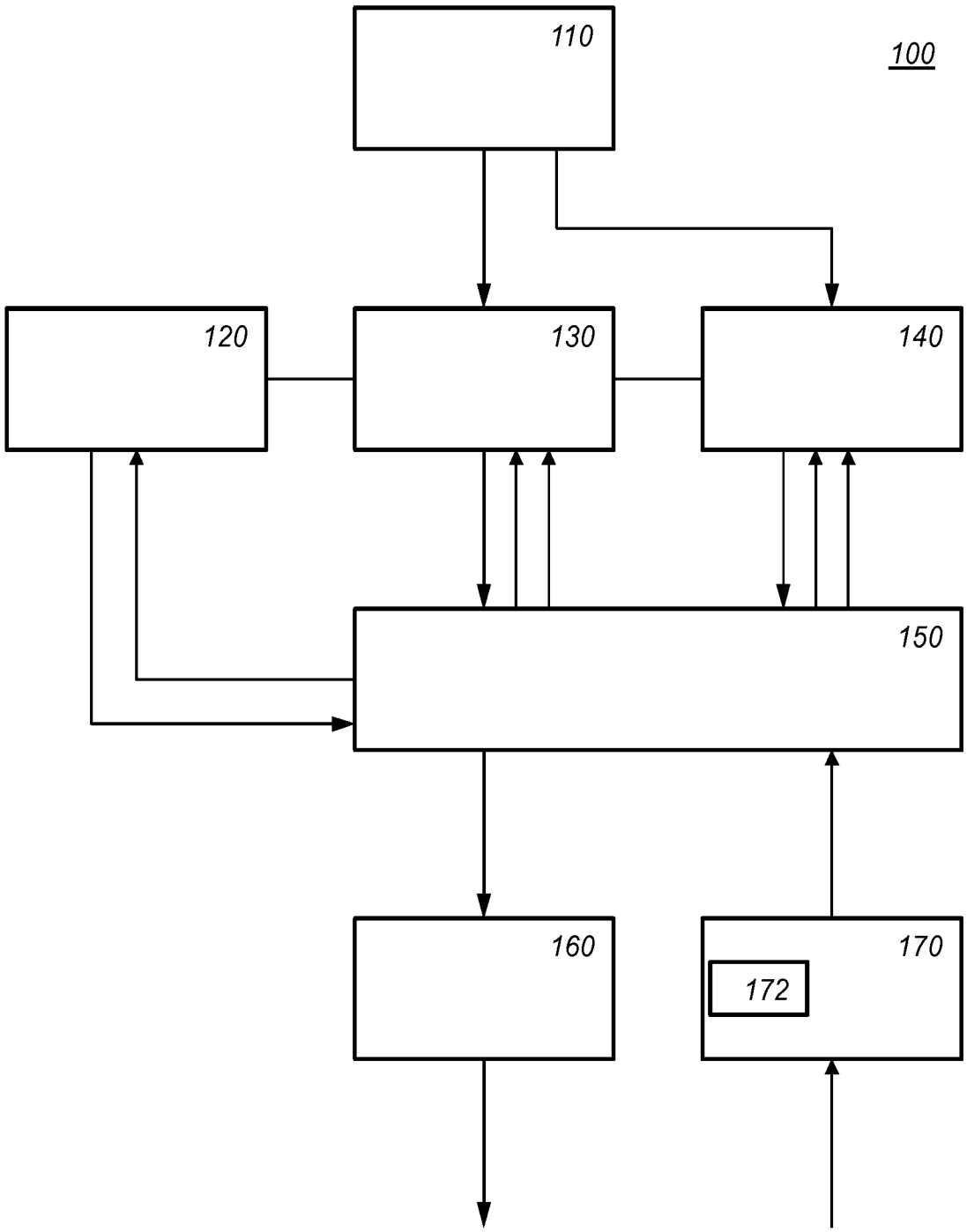


图 1a

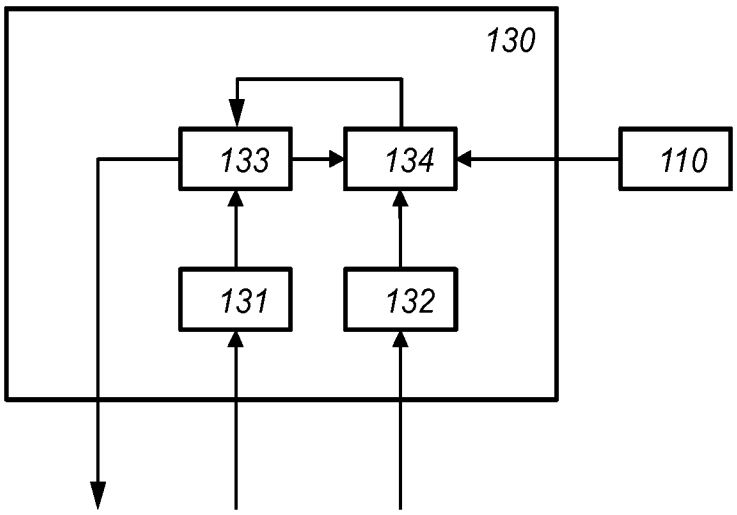

130
133
134
110
131
132

图 1b

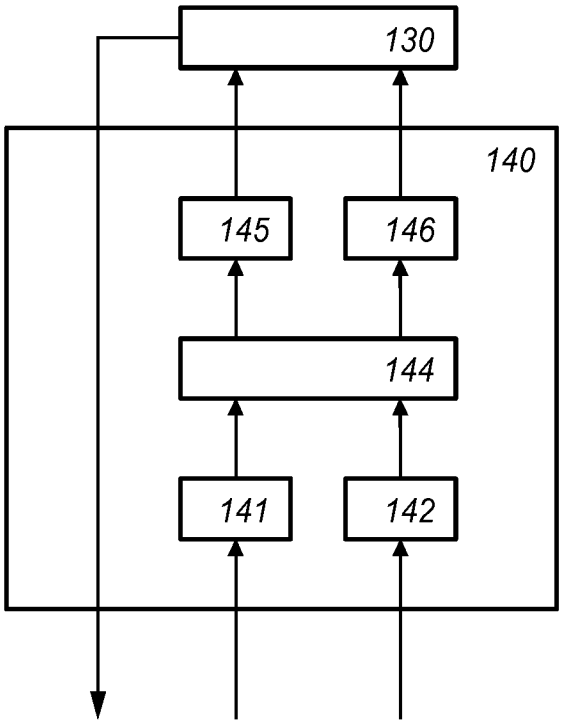

130
140
145
146
144
141
142

图 1c

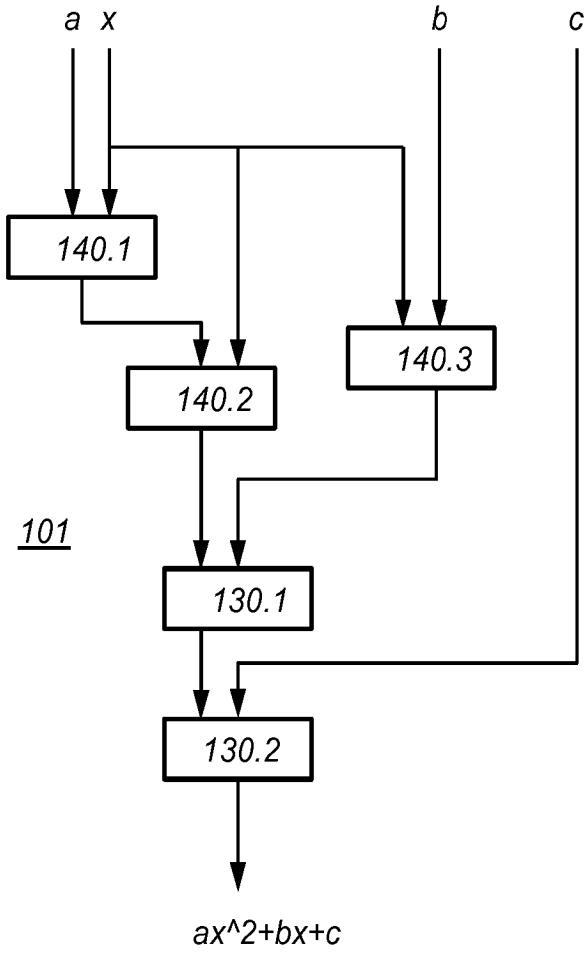

a x
b
c
140.1
140.2
140.3
101
130.1
130.2
ax^2+bx+c

图 2

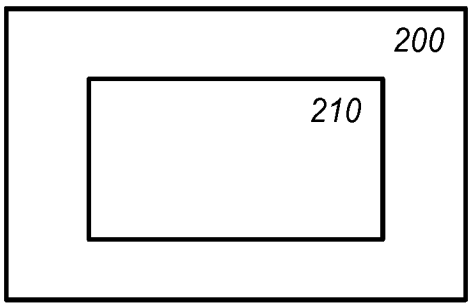

200
210

图 3

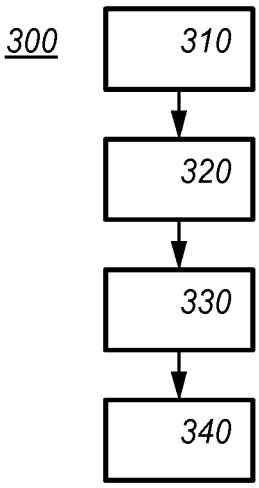

300
310
320
330
340

图 4

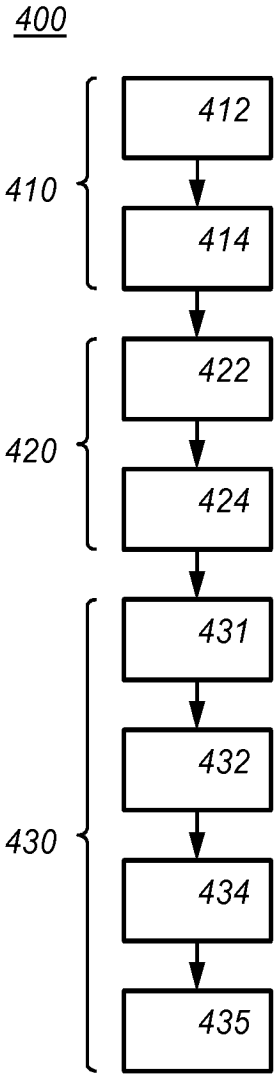

400
410
412
414
420
422
424
430
431
432
434
435

图 5

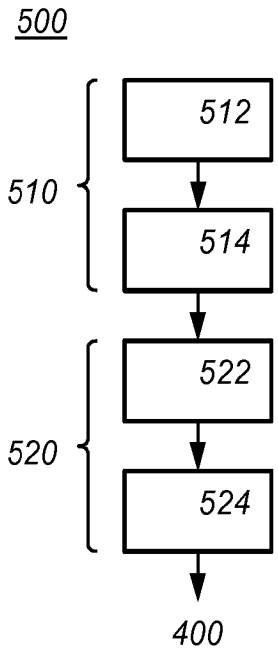

500
512
510
514
522
520
524
400

图 6

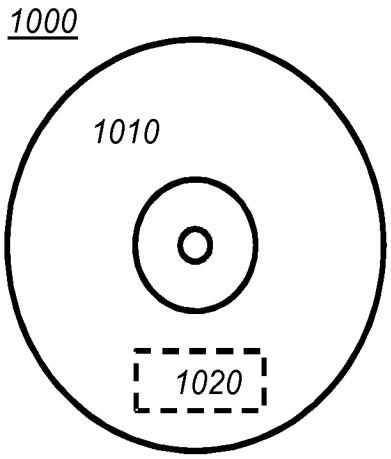

1000
1010
1020

图 7a

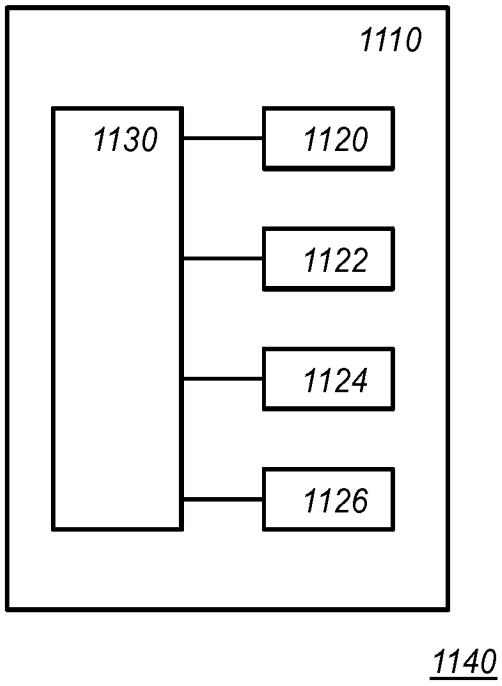

1110
1130
1120
1122
1124
1126
1140

图 7b