



## (12)发明专利申请

(10)申请公布号 CN 108475255 A

(43)申请公布日 2018.08.31

(21)申请号 201680078164.3

(74)专利代理机构 永新专利商标代理有限公司  
72002

(22)申请日 2016.12.07

代理人 李光颖 王英

(30)优先权数据

2015911 2015.12.07 NL

(51)Int.Cl.

G06F 17/10(2006.01)

(85)PCT国际申请进入国家阶段日

G06F 21/14(2006.01)

2018.07.06

H04L 9/06(2006.01)

(86)PCT国际申请的申请数据

PCT/EP2016/079971 2016.12.07

(87)PCT国际申请的公布数据

W02017/097791 EN 2017.06.15

(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

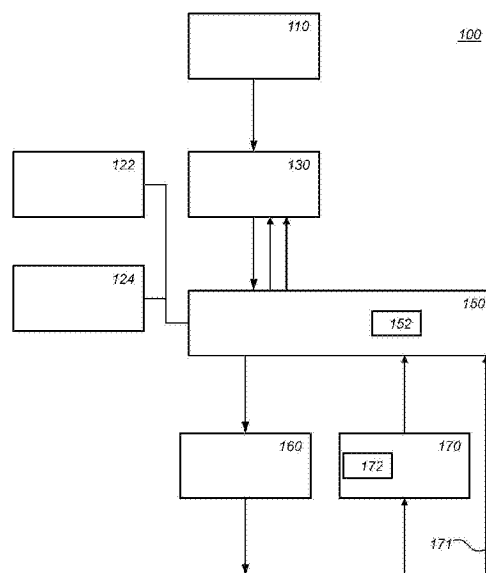
权利要求书5页 说明书16页 附图6页

## (54)发明名称

计算设备和方法

## (57)摘要

一种被布置为将主群 $((M,+))$ 的两个元素相加的电子计算设备,所述主群是有限阿贝尔群公式(I),所述计算设备包括:-加法表存储设备(110),其用于为第二子集 $(M_0)$ 的每个元素 $(m_i)$ 存储查找表 $(P_i)$ ;-加法单元,其被布置为:接收第一加法输入 $(\alpha_0 x_0)$ 和第二加法输入 $(\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots)$ ,所述第一加法输入和所述第二加法输入是所述主群 $(M)$ 的元素,其中,所述第一加法输入以归一化表示被接收,并且所述第二加法输入以广义化表示被接收;并且计算所述主群 $(M)$ 中的所述第一加法输入与所述第二加法输入的和。



1. 一种被布置为将主群  $(M, +)$  的两个元素相加的电子计算设备, 所述主群是有限阿贝尔群  $(\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{k_t}})$ ,

- 为所述主群定义了:

- 第一作用群  $(N)$  和第二作用群  $(H)$ , 所述第一作用群  $(N)$  和所述第二作用群  $(H)$  作用于所述主群  $(M)$ , 所述第二作用群  $(H)$  是由生成元素  $(h)$  生成的循环群  $(H = \langle h \rangle)$ ,

- 所述主群  $(M)$  的第一子集  $(\Delta)$ , 使得所述主群  $(M)$  的任何元素  $(m)$  能够被表示为所述第一作用群  $(N)$  的元素  $(n)$  和所述第一子集  $(\Delta)$  的元素  $(X)$  的乘积  $(m = nX)$ , 所述第一作用群  $(N)$  的所述元素  $(n)$  和所述第一子集  $(\Delta)$  的所述元素  $(X)$  被称为所述主群  $(M)$  的所述元素  $(m)$  的归一化表示,

- 所述主群  $(M)$  的第二子集  $(M_0 = \{m_0, \dots, m_{r-1}\})$ , 使得所述主群  $(M)$  的任何元素  $(m)$  能够被表示为多个被加数的和, 每个被加数是所述第一作用群  $(N)$  的元素  $(\gamma_t)$ 、所述第二子集  $(M_0)$  的元素  $(m_{i_t})$  和所述生成元素的幂  $(h^t)$  的乘积  $(m = \sum_t \gamma_t m_{i_t} h^t)$ , 所述多个被加数中的所述第一作用群的所述多个元素被称为所述主群  $(M)$  的所述元素  $(m)$  的广义化表示,

所述计算设备包括:

- 加法表存储设备 (110), 其为所述第二子集  $(M_0)$  的每个元素  $(m_i)$  存储查找表  $(P_i)$ , 所述查找表将所述主群  $(M)$  的归一化元素  $((\gamma, X))$  作为输入并将所述输入映射到所述第一作用群  $(N)$  的元素  $(\lambda)$  和所述第一子集  $(\Delta)$  的元素  $(Y)$ , 所述第一作用群  $(N)$  的所述元素  $(\lambda)$  和所述第一子集  $(\Delta)$  的所述元素  $(Y)$  的乘积是所述归一化元素  $(\gamma X)$  与所述第二子集  $(M_0)$  的所述元素  $(m_i)$  的和  $(\lambda Y h = \gamma X + m_i)$ ,

- 加法单元, 其被布置为: 接收第一加法输入  $(\alpha_0 X_0)$  和第二加法输入  $(\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots)$ , 所述第一加法输入和所述第二加法输入是所述主群  $(M)$  的元素, 其中, 所述第一加法输入以归一化表示被接收, 并且所述第二加法输入以广义化表示被接收; 并且计算所述主群  $(M)$  中的所述第一加法输入与所述第二加法输入的和, 其中, 所述加法单元被布置为:

- 通过将所述第二加法输入的被加数顺序地加到所述第一加法输入来计算部分和, 其中,

- 将所述第二加法输入的被加数  $(\gamma_t m_{i_t} h^t)$  加到所述部分和包括: 将针对所述第二子集  $(M_0)$  的所述元素  $(m_{i_t})$  存储于所述加法表存储设备 (110) 中的所述查找表  $(P_{i_t})$  应用于所述被加数中。

2. 根据权利要求1所述的电子计算设备, 其中,

- 以归一化表示的所述主群  $(M)$  的元素  $(m)$  在所述计算设备中被表示为两个数字的对, 所述两个数字中的第一个数字指示所述第一作用群  $(N)$  的所述元素  $(n)$ , 所述两个数字中的第二个数字指示所述第一子集  $(\Delta)$  的所述元素  $(X)$ , 并且

- 以广义化表示的所述主群  $(M)$  的元素  $(m)$  在所述计算设备中被表示为数字的至少第一序列, 所述第一序列指示所述被加数中的所述第一作用群  $(N)$  的所述元素  $(\gamma_t)$ 。

3. 根据前述权利要求中的任一项所述的电子计算设备, 其中,

- 由所述加法单元计算的所述和以归一化形式来表示。

4. 根据前述权利要求中的任一项所述的电子计算设备,包括:

- 网络接口,其被布置为从在所述电子计算设备外部的计算机接收一个或多个加法输入,所述一个或多个加法输入是以广义化表示的,以及
- 常数存储设备,其被布置为存储以归一化表示的一个或多个常数加法输入,
- 计算设备,其被布置为使用所述加法单元来将通过所述网络接口接收到的选定加法输入与来自所述常数存储设备的选定常数加法输入相加。

5. 根据前述权利要求中的任一项所述的电子计算设备,包括:

- 转换单元,其被布置为接收转换输入,其中,
- 所述转换输入是以广义化形式的,所述转换单元被布置为通过加上以归一化形式的所述主群的元素来将所述转换输入转换为归一化形式,并且/或者
- 所述转换输入是以归一化输入的,所述转换单元存储将所述第一子集的元素映射到广义化形式的转换表。

6. 根据前述权利要求中的任一项所述的电子计算设备,包括:

- 函数单元,其被布置为将线性函数(f)应用于以广义化形式的函数输入,以及
- 线性函数表存储设备,其存储表,所述表将所述第一作用群(N)的元素( $\gamma_t$ )、所述第二子集( $M_0$ )的元素( $m_{i_t}$ )和所述生成元素的幂( $h^t$ )的乘积( $m = \sum_t \gamma_t m_{i_t} h^t$ )作为输入并将所述乘积映射到将所述线性函数应用于所述乘积的结果,其中,
- 所述函数单元被布置为将所述线性函数表存储设备的所述表应用于所述函数输入的所述被加数。

7. 根据前述权利要求中的任一项所述的电子计算设备,其中,

- 所述第二作用群(H)具有3个或更多个元素,或者
- 所述第二作用群(H)具有2个元素,或者
- 所述第二子集( $M_0$ )具有2个或更多个元素,或者
- 所述第二子集( $M_0$ )具有不是单位元素的1个元素,或者
- 所述主群(M)是所述阿贝尔群 $\mathbb{Z}_2^l$ ,例如,其中, $l \geq 4$ ,或者
- 所述第一作用群(N)是具有3个或更多个元素的循环群。

8. 根据前述权利要求中的任一项所述的电子计算设备,其中,所述生成元素(h)具有阶数k,以广义化表示的所述生成元素(h)的指数(t)至多是所述阶数(k)的特定倍数减1( $t \leq \lambda k - 1$ ),所述特定倍数对于所述主群的所有元素是相同的。

9. 根据权利要求8所述的电子计算设备,其中,

- 所述主群具有特征2,并且所述第二作用群具有阶数2,并且以广义化表示的所述生成元素(h)的所述幂( $h^t$ )至多是所述阶数的两倍减1( $t \leq 2k - 1$ ),或者
- 所述主群具有大于2的特征或者所述第二作用群的所述阶数大于2,并且以广义化表示的所述生成元素(h)的所述幂( $h^t$ )至多是所述阶数减1( $t \leq k - 1$ )。

10. 根据前述权利要求中的任一项所述的电子计算设备,其中,

- 所述加法单元被布置为:
- 将所述部分和初始设置为所述第一加法输入( $\alpha_0 X_0$ ),并且
- 在所述第一加法输入的所述被加数上进行循环,在每个循环中通过加上所述第一加

法输入的所述被加数 $(\gamma_t m_{i_t} h^t)$ 来更新所述部分和。

11. 根据权利要求10所述的电子计算设备, 其中,

-所述第一加法输入是所述主群的所述元素 $\alpha_0 X_0$ , 其中,  $\alpha_0 \in N$  且  $X_0 \in \Delta$ , 并且所述第二加法输入是所述主群的所述元素 $\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots + \gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1}$ , 其中,  $k$  是所述生成元素的所述阶数,  $\gamma_i \in N$  且  $m_i \in M_0$ , 并且  $h$  是所述生成元素,

-所述加法单元被布置为:

-将所述部分和初始设置为所述第一加法输入 $\alpha_0 X_0$ ,

-对于所述生成元素 $(h^t)$ 的从0到 $\lambda k-1$ 的每个指数 $(t)$ ,

-通过加上对应于所述指数的所述被加数 $(\gamma_t m_{i_t} h^t)$ , 通过将针对 $m_{i_t}$ 的查找表 $(P_{i_t})$ 应用于 $\gamma_t^{-1} \gamma_{t-1} \alpha_t X_t$ , 来从当前部分和 $(\alpha_t X_t)$ 获得下一部分和 $(\alpha_{t+1} X_{t+1})$ , 其中,  $\gamma^{-1}$ 是所述主群 $(M)$ 中的单位元素, 并且其中,  $\alpha_t X_t$ 是所述当前部分和,

-所述部分和等于 $\gamma_{t-1} \alpha_t X_t h^t$ 。

12. 根据前述权利要求中的任一项所述的电子计算设备, 其中, 所述第一子集 $(\Delta)$ 仅包括通过对所述第一作用群 $(N)$ 的元素、所述第二子集的元素和所述第二作用群 $(H)$ 的元素加所述生成元素的所述生成元素的所述阶数减1的幂的乘积求和形成的元素 $(\beta_0 m_{i_0} h^0 + \dots + \beta_{k-2} m_{i_{k-2}} h^{k-2} + m_{i_{k-2}} h^{k-1})$ , 其中, 所述第二作用群的所述元素是所述生成元素 $(h)$ 的为至多所述生成元素的所述阶数减2的幂的幂。

13. 根据权利要求12所述的电子计算设备, 其中, 所述主群 $(M, +)$ 具有使所述主群成为环 $(R, +, \cdot)$ 的加法运算 $(\cdot)$ , 所述电子计算设备包括:

-乘法单元, 其被布置为: 接收第一乘法输入和第二乘法输入, 所述第一乘法输入和所述第二乘法输入是所述主环 $(R)$ 的元素, 其中, 所述第一乘法输入以归一化表示 $(\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha = X \alpha$ 被接收, 并且所述第二乘法输入以广义化表示 $(\gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots)$ 被接收; 并且计算所述环 $(R)$ 中的所述第一乘法输入和所述第二乘法输入的乘积, 其中, 所述乘法单元被布置为:

-根据所述第一乘法输入和所述第二乘法输入的第一被加数来计算第一加法输入, 所述第一加法输入是以归一化形式 $(X(\alpha \gamma_0))$ 的,

-根据所述第一乘法输入和所述第二乘法输入的除了所述第一被加数之外的多个被加数来计算一个或多个第二加法输入, 所述一个或多个第二加法输入是以广义化形式 $(X(\alpha \gamma_i) h^i = (X h^i) n')$ 的,

-通过所述加法单元将所述第一加法输入与所述一个或多个第二加法输入相加。

14. 根据前述权利要求中的任一项所述的电子计算设备, 其中,

$$(\#N \cdot \#M_0)^{\#H} \geq 3/2 (\#N \cdot \#\Delta)$$

更特别地, 其中,

$$(\#N \cdot \#M_0)^{\#H} \geq 5/2 (\#N \cdot \#\Delta)$$

其中,

$\#N$ 是所述第一作用群 $(N)$ 的大小,

$\#H$ 是所述第二作用群 $(H)$ 的大小,

$\#\Delta$ 是所述第一子集 $(\Delta)$ 的大小,

# $M_0$ 是所述第二子集( $M_0$ )的大小,

# $M$ 是所述主群( $M$ )的大小。

15.一种用于计算在被布置为将主群( $(M,+)$ )的两个元素相加的电子计算设备中使用的查找表的表计算设备(200),所述主群是有限阿贝尔群( $\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$ ),所述表计算设备包括:

-表创建单元(210),其被布置为构建针对所述第二子集( $M_0$ )的元素( $m_i$ )的所述查找表,所述表创建单元被布置为:

-重复地选择所述主群( $M$ )的输入归一化元素( $(\gamma, X)$ ),

-确定所述输入归一化元素( $\gamma X$ )与所述第二子集( $M_0$ )的所述元素( $m_i$ )的和( $\lambda Yh = \gamma X + m_i$ ),

-确定所述第一作用群( $N$ )的元素( $\lambda$ )和所述第一子集( $\Delta$ )的元素( $Y$ ),使得所述第一作用群( $N$ )的所述元素( $\lambda$ )和所述第一子集( $\Delta$ )的所述元素( $Y$ )的乘积是所述和,

-将条目添加到所述查找表中,所述查找表将输入环元素映射到所述第一作用群( $N$ )的所述元素( $\lambda$ )和所述第一子集( $\Delta$ )的所述元素( $Y$ )。

16.一种用于将主群( $(M,+)$ )的两个元素相加的电子计算方法,所述主群是有限阿贝尔群( $\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$ ),

-为所述主群定义了:

-第一作用群( $N$ )和第二作用群( $H$ ),所述第一作用群( $N$ )和所述第二作用群( $H$ )作用于所述主群( $M$ ),所述第二作用群( $H$ )是由生成元素( $h$ )生成的循环群( $H = \langle h \rangle$ ),

-所述主群( $M$ )的第一子集( $\Delta$ ),使得所述主群( $M$ )的任何元素( $m$ )能够被表示为所述第一作用群( $N$ )的元素( $n$ )和所述第一子集( $\Delta$ )的元素( $X$ )的乘积( $m = nX$ ),所述第一作用群( $N$ )的所述元素( $n$ )和所述第一子集( $\Delta$ )的所述元素( $X$ )被称为所述主群( $M$ )的所述元素( $m$ )的归一化表示,

-所述主群( $M$ )的第二子集( $M_0 = \{m_0, \dots, m_{r-1}\}$ ),使得所述主群( $M$ )的任何元素( $m$ )能够被表示为多个被加数的和,每个被加数是所述第一作用群( $N$ )的元素( $\gamma_i$ )、所述第二子集( $M_0$ )的元素( $m_{i_t}$ )和所述生成元素的幂( $h^t$ )的乘积( $m = \sum_t \gamma_t m_{i_t} h^t$ ),所述多个被加数中的所述第一作用群的所述多个元素被称为所述主群( $M$ )的所述元素( $m$ )的广义化表示,

所述计算方法包括:

-为所述第二子集( $M_0$ )的每个元素( $m_i$ )存储查找表( $P_i$ ),所述查找表将所述主群( $M$ )的归一化元素( $(\gamma, X)$ )作为输入并将所述输入映射到所述第一作用群( $N$ )的元素( $\lambda$ )和所述第一子集( $\Delta$ )的元素( $Y$ ),所述第一作用群( $N$ )的所述元素( $\lambda$ )和所述第一子集( $\Delta$ )的所述元素( $Y$ )的乘积是所述归一化元素( $\gamma X$ )与所述第二子集( $M_0$ )的所述元素( $m_i$ )的和( $\lambda Yh = \gamma X + m_i$ ),

-接收第一加法输入( $\alpha_0 X_0$ )和第二加法输入( $\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots$ ),所述第一加法输入和所述第二加法输入是所述主群( $M$ )的元素,其中,所述第一加法输入以归一化表示被接收,并且所述第二加法输入以广义化表示被接收;并且计算所述主群( $M$ )中的所述第一加法输入与所述第二加法输入的和,其中,所述计算包括:

-通过将所述第二加法输入的被加数顺序地加到所述第一加法输入来计算部分和,其

中,

-将所述第二加法输入的被加数 $(\gamma_t m_{i_t} h^t)$ 加到所述部分和包括将针对所述第二子集 $(M_0)$ 的所述元素 $(m_{i_t})$ 存储的查找表 $(P_{i_t})$ 应用于所述被加数中。

17.一种用于计算在被布置为将主群 $(M, +)$ 的两个元素相加的电子计算设备中使用的查找表的表计算方法(400),所述主群是有限阿贝尔群 $(\mathbb{Z}_{p_1 k_1} \oplus \dots \oplus \mathbb{Z}_{p_t k_t})$ ,所述表计算方法包括:

- 重复地选择(410)所述主群 $(M)$ 的输入归一化元素 $((\gamma, X))$ ,
- 确定所述输入归一化元素 $(\gamma X)$ 与所述第二子集 $(M_0)$ 的所述元素 $(m_i)$ 的和 $(\lambda Y_h = \gamma X + m_i)$ ,
- 确定(420)所述第一作用群 $(N)$ 的元素 $(\lambda)$ 和所述第一子集 $(\Delta)$ 的元素 $(Y)$ ,使得所述第一作用群 $(N)$ 的所述元素 $(\lambda)$ 和所述第一子集 $(\Delta)$ 的所述元素 $(Y)$ 的乘积是所述和,
- 将条目添加(430)到所述查找表中,所述查找表将输入环元素映射到所述第一作用群 $(N)$ 的所述元素 $(\lambda)$ 和所述第一子集 $(\Delta)$ 的所述元素 $(Y)$ 。

18.一种包括计算机程序指令的计算机程序(1020),所述计算机程序指令被布置为当所述计算机程序在计算机上运行时执行权利要求16或17所述的方法。

19.一种计算机可读介质(1000),包括如权利要求18所述的计算机程序(1020)。

## 计算设备和方法

### 技术领域

[0001] 本发明涉及电子计算设备、电子计算方法、表计算设备、表计算方法和计算机程序以及计算机可读介质。

### 背景技术

[0002] 在白盒密码术和更一般的软件混淆术中,计算通常是在编码值上而不是明语值上执行的。如果计算是在编码值上而不是在明语值本身上执行的,则混淆的软件的逆向工程将变得更难。

[0003] 在编码之后,常规运算(如加法或乘法)不能再使用计算机的内置原语来执行。编码值的直接相加通常不会得到对值的相加的编码。这同样适用于乘法。对于大多数 $x$ 和 $y$ ,以公式 $E(x) + E(y) \neq E(x+y)$ 表示; $E$ 表示编码函数。

[0004] 该问题的解决方案是引入加法表( $A$ )和乘法表( $M$ )。这些表将两个编码值作为输入,并产生编码值作为与加法或乘法运算的编码相对应的输出。这些表可以被定义为: $A(E(x), E(y)) = E(x+y)$ ;  $M(E(x), E(y)) = E(xy)$ 。这些表允许直接对编码值执行算术运算。

[0005] 使用表的混淆的加法和乘法遭受至少两个缺点。第一,表能够变得相当大。如果 $x$ 和 $y$ 被表示为 $l$ 位,则每个表需要 $2^{2l}$ 位。此外,编码可以是固定的,这打开了使攻击者做出可能的编码的列表的可能性。

### 发明内容

[0006] 具有解决这些和其他忧虑的计算设备将是有利的。

[0007] 发明人设计了一种方式,其中可以使用比背景中讨论的表小得多的表在编码值上执行加法:每个表需要大约 $2^l$ 位。此外,该系统适用于所有阿贝尔群,使其广泛适用。此外,除了具有小表和大应用范围之外,潜在编码的数量仍然很大,因此提高了安全性。

[0008] 事实上,该系统允许针对相同元素的不同表示,而不需要依靠冗余变量。这意味着多种不同的编码不容易被瓦解。此外,该系统允许与内部使用的编码相比不同的编码(广义表示)用于外部数据。此外,可能的表示的数量可以被增加到不需要多于一次使用外部表示的点,进一步减少使攻击者有效地使用可能的编码的列表的可能性。

[0009] 本发明适用于许多不同的交换群 $M$ 。也称为阿贝尔群的交换群是包括许多不同的类似数学结构(例如,整数模一数( $\mathbb{Z}_n$ )或多项式模一数和多项式( $\mathbb{Z}_n[x]/f(x)$ ))的数学概念。在实施例中,该系统被扩展到交换环。

[0010] 如将在本文中更完整地讨论的,存在许多可能性和变型。通常将不知道攻击者在任何给定实施方式中已经选择了许多变型中的哪一个。

[0011] 该计算设备是电子设备,并且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。

[0012] 如本文所描述的算术可以被应用于广泛的实际应用中。这种实际应用包括在专用硬件上运行的安全应用,例如,银行应用等,其中,逆向工程要被防止。其他应用包括其中数

据的无意泄露要被防止的应用。如果程序被诱骗以发布私有数据,则在泄露的数据被编码的情况下这就不那么让人忧虑了。该算法也可以被应用于运行应用的服务器。如果用户以编码的形式发送和接收数据,则会提高私密度。

[0013] 根据本发明的方法可以作为计算机实现的方法在计算机上实现,或者以专用硬件来实现,或者以两者的组合来实现。用于根据本发明的方法的可执行代码或其部分可以被存储在计算机程序产品上。计算机程序产品的范例包括存储器设备、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暂态程序代码单元,其用于在所述程序产品在计算机上运行时执行根据本发明的方法。

[0014] 在优选实施例中,所述计算机程序包括计算机程序代码单元,当所述计算机程序在计算机上运行时,所述计算机程序代码单元适于执行根据本发明的方法的所有步骤。优选地,所述计算机程序被体现在计算机可读介质上。

## 附图说明

[0015] 将参考附图仅通过举例的方式来描述本发明的进一步的细节、方面和实施例。为简单和清楚起见,示出了各图中的元件,并且各图中的元件不一定是按比例绘制的。在各图中,对应于已经描述的元件的元件可以具有相同的附图标记。在附图中,

[0016] 图1a示意性地示出了计算设备100的实施例的示例,

[0017] 图1b示意性地示出了加法单元130的实施例的示例,

[0018] 图1c示意性地示出了乘法单元140的实施例的示例,

[0019] 图1d示意性地示出了计算设备100'的实施例的示例,

[0020] 图2示意性地示出了计算设备101的实施例的示例,

[0021] 图3示意性地示出了用于计算用于在计算设备中使用的增量表的表计算设备200的实施例的示例,

[0022] 图4示意性地示出了计算方法300的实施例的示例,

[0023] 图5示意性地示出了表计算方法400的实施例的示例,

[0024] 图6a示意性地示出了根据实施例的具有包括计算机程序的可写部分的计算机可读介质,

[0025] 图6b示意性地示出了根据实施例的处理器系统的表示。

[0026] 图1a-1d中的附图标记列表:

[0027] 100 计算设备

[0028] 110 加法表存储设备

[0029] 122 转换单元

[0030] 124 函数单元

[0031] 130 加法单元

[0032] 131 第一加法输入

[0033] 132 第二加法输入

[0034] 133 部分和

[0035] 134 部分加法单元

[0036] 140 乘法单元

|        |     |                |
|--------|-----|----------------|
| [0037] | 141 | 第一乘法输入         |
| [0038] | 142 | 第二乘法输入         |
| [0039] | 144 | 中间乘法输入         |
| [0040] | 145 | 第一加法输入         |
| [0041] | 146 | 一个或多个第二加法输入    |
| [0042] | 150 | 操作数存储设备        |
| [0043] | 152 | 常数存储设备         |
| [0044] | 160 | 解码单元           |
| [0045] | 170 | 编码单元           |
| [0046] | 171 | 直接输入           |
| [0047] | 172 | 被布置为存储编码表的存储设备 |

### 具体实施方式

[0048] 虽然本发明容许许多不同形式的实施例,但是在附图中示出并将在本文中详细描述一个或多个具体实施例,应理解的是,本公开应被视为本发明的原理的示例,而不意图将本发明限制于所示出和描述的具体实施例。

[0049] 在下文中,为便于理解,在操作中描述了实施例的元件。然而,将显而易见的是,各个元件被布置为执行被描述为由它们执行的功能。

[0050] 此外,本发明不限于这些实施例,并且本发明在于以上描述的或在相互不同的从属权利要求中记载的每一个新颖特征或各特征的组合。

[0051] 图1以示意形式示出了电子计算设备100的实施例。计算设备100被布置为将主群 $(M, +)$ 的两个元素相加。主群由元素的集合 $M$ 和针对 $M$ 的每对元素定义的二元运算(用 $+$ 指示)表示。主群满足作为群的规范数学要求(加法是满足结合律的,存在双面的单位元素,并且每个群元素都具有倒数)。此外,群被限制为是有限的,并且是阿贝尔群。后者意味着对于一些素数 $p_i$ 和指数 $k_i$ ,该群可以被表示为 $\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$ 。对于主群,加法可以被表示为 $+$ 。注意,即使我们将群运算表示为 $+$ 或其单位元素为0,这也并不意味着计算设备必须被限制于传统算术意义上的加法。虽然假设模一模数的加法的群是可以应用于计算设备的阿贝尔群,但其不限于此,而是可以代替地被应用于任何阿贝尔群。所有的群和集合都是有限的而且是非空的。

[0052] 计算设备100被布置为计算群中的加法。通过对群元素进行编码来混淆它们。混淆群元素有益于安全性,因为尝试对计算设备进行逆向工程的攻击者不知道使用的编码。因此,即使攻击者能够观察计算设备的内部运作,他也不知道设备正在计算什么。

[0053] 有趣的是,计算设备100以两种不同的方式对群元素进行编码,为了专利的目的将这两种不同的方式命名为:归一化表示和广义化表示。发明人已经发现,可以为所有的有限阿贝尔群找到这样的表示。此外,群可以允许归一化表示和广义化表示的许多不同的选择。后者也提高了安全性,因为如果只有一个或几个编码可用,则具有一般编码系统的知识的攻击者可以尝试所有可能的编码,并找出哪个编码被使用。然而,如果用于编码的许多选择可用,则后一攻击路线变得不可行。

[0054] 此外,归一化表示和广义化表示两者都可以允许相同元素的多个不同表示。特别

地,广义化表示可以被容易地调整以允许相同群元素的许多不同表示。同样,这有益于安全;一个潜在的攻击路线可以是尝试并做出将群表示映射到更传统的表示的转换表。然而,如果存在针对相同元素的更多表示,则这将更难。

[0055] 归一化表示和广义化表示是关于下面讨论的许多集合来定义的。这些集合的选择确定表示以及还有它们如何被相加,特别地是在加法中使用的查找表(下面进一步讨论)。

[0056] 为主群定义了第一作用群N和第二作用群H。这两个群都作用于主群M上。注意:如果对于群A中的所有g和群B中的x,定义群B的元素 $g \cdot x$ ,则群A作用于群B。群A的单位元素不改变x,此外,对于A的任何 $g_1$ 和 $g_2$ ,  $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ 。

[0057] 第二作用群H是由生成元素(h)生成的循环群( $H = \langle h \rangle$ )。两个作用群都是有限的。存在被称为阶数的某个指数k,使得 $h^k$ 是单位元素。第一作用群和第二作用群两者都是数学意义上的群。作用群在主群上的作用被称为乘积。作用群的单位元素可以被称为1。使得,例如, $h^k \cdot x = 1 \cdot x = x$ 。注意,为方便符号表示,第二作用群已经被符号表示为右作用。

[0058] 第一作用群N和第二作用群H已经被选择为具有如下性质:对于所有 $n \in N, m \in M, h \in H$ ,  $(nm)h = n(mh)$ 。

[0059] 可以选择第一作用群和第二作用群作为M的自同构群的子群,例如,主群M对它自身的同构的集合。这表明总是可以选择第一群和第二群。可以通过选择M的自同构群的元素h并设置 $H = \langle h \rangle$ (即,由h生成的群)来选择第二作用群。例如,第一作用群和第二作用群可以被获得为矩阵群。

[0060] 虽然不是必须的,但是在实施例中,第一作用群是 $Aut_{\mathbb{Z}}(M)$ 的矩阵子群N,并且h是与第一作用群N的生成元交换的另一矩阵。在这种情况下,我们可以使用列向量用于M的元素并用标准矩阵乘法在左边写出所有矩阵。虽然分别用于作用群和M的矩阵和向量符号表示是方便的,并且可以例如用于在作用群中计算或者计算加法表,但是这种格式不需要被使用在计算设备本身(其中例如可以使用编码表示)中。

[0061] 计算设备100中的计算可以要求计算在作用群中被执行。如果作用群是循环的,例如如第二作用群那样,则这可以通过在去指数模上计算到群的阶数来完成。在任何情况下,可以使用表来表示在作用群中的群运算。

[0062] 还为主群定义了主群M的第一子集 $\Delta$ ,使得主群M的任何元素m可以被表示为 $m = nX$ ,例如被表示为第一作用群N的元素n与第一子集 $\Delta$ 的元素X的乘积。说明其的另一种方式是,在第一作用群N的作用下第一子集 $\Delta$ 的轨道等于主群。

[0063] 给定第一作用群N和主群M,使得保证第一子集 $\Delta$ 存在,因为 $N \cdot M = M$ 。例如,可以通过确定由N引起的M中的轨道并选择每个轨道的至少一个元素来找到第一子集。可以通过精确选择每个轨道的一个元素来找到最小大小的第一子集 $\Delta$ 。如果在N中存在n,则M的两个元素a和b在相同的轨道上,使得 $na = b$ 。从相同轨道选择更多元素会增加归一化表示的数量。

[0064] M的任何元素m可以被表示为第一作用群N的元素n和第一子集 $\Delta$ 的元素X的对,对此 $m = nX$ 。后一表示被称为归一化表示。通过选择不同的第一作用群和/或不同的第一子集,可以获得许多不同的归一化表示。

[0065] 在内部,对(n,X)可以由一对整数表示。例如,元素n可以由编码N的特定元素的整数表示。例如,元素X可以由编码第一子集 $\Delta$ 的特定元素的整数表示。这种编码不需要是规范化的。例如,可以通过在第一作用群和/或第一子集上施加随机顺序,并且将第一作用群

和/或第一子集中的元素表示为该顺序中的索引,来获得整数编码。或者,元素n和X可以以传统(例如规范化)表示来表示。后面的表示本身可以被编码,例如加密。

[0066] 还为主群定义了主群M的第二子集 $M_0 = \{m_0, \dots, m_{r-1}\}$ ,使得主群M的任何元素m可以被表示为多个被加数的和,每个被加数是第一作用群N的元素 $\gamma_t$ 、第二子集 $M_0$ 的元素 $m_{i_t}$ 以及生成元素的幂 $h^t$ 的乘积。例如, $m = \sum_t \gamma_t m_{i_t} h^t$ 。广义化元素可以例如被写为: $m = \gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \dots + \gamma_{k-1} m_{i_{k-1}} h^{k-1}$ 。在后一情况下,最高指数是第二作用群的阶数(即h的阶数)减1。更一般地,指数t可以被限制为 $\lambda k - 1$ ,即,h的阶数的倍数减1。最高指数 $k-1$ 通常是足够的,但是不是对于所有群都这样。下面我们将大体假设广义化表示使用至多为 $k-1$ 的h的幂,除非另有说明。尽管如此,下面给出的范例可以被扩展到更大的指数,例如在期望更多广义化表示的情况下。

[0067] 给定允许M的所有元素被表示的第二子集 $M_0$ ,集合 $nM_0h^j$ 也是有效的第二子集;其中n和 $h^j$ 分别在第一作用群和第二作用群中。

[0068] 可以将以广义化形式的元素表示为两个序列: $\{\gamma_0, \gamma_1, \dots, \gamma_{k-1}\}$ 和 $\{m_{i_0}, m_{i_1}, \dots, m_{i_{k-1}}\}$ 或 $\{i_0, i_1, \dots, i_{k-1}\}$ 。后一序列是由元素在列表中的指数表示元素的示例。另外,可以将元素 $\gamma_i$ 表示为整数,例如,作为N的列表表示中的指数。在实施例中,第二子集包含单个元素 $m_0$ ;在这种情况下,第二序列不需要是显式的,但可以是隐式的。在实施例中,对于M的所有元素,序列具有相同的长度。在实施例中,序列具有针对h的每个幂的从0到h上的边界的条目,例如对于 $\lambda > 1$ , $k-1$ 或 $\lambda k - 1$ 。

[0069] 这两个序列也可以被表示为单个序列,例如,被表示为 $\{\gamma_0, m_{i_0}, \gamma_1, m_{i_1}, \dots, \gamma_{k-1}, m_{i_{k-1}}\}$ 。

[0070] 我们具有以下边界 $\#N \cdot \# \Delta \geq \#M$ ,且 $(\#N \cdot \#M_0)^{\#H} \geq \#M$ ,其中

[0071]  $\#N$ 是第一作用群(N)的大小,

[0072]  $\#H$ 是第二作用群(H)的大小,

[0073]  $\# \Delta$ 是第一子集( $\Delta$ )的大小,

[0074]  $\#M_0$ 是第二子集( $M_0$ )的大小,

[0075]  $\#M$ 是主群(M)的大小。

[0076] 此外,第一作用群(N)、第二作用群(H)、第一子集( $\Delta$ )、第二子集( $M_0$ )、以及主群(M)的大小都不为空。在期望的情况下,归一化表示的数量可以相较于主群M的大小被设置上限;例如,在一些实施例中, $2\#M \geq \#N \cdot \# \Delta$ 。这可以具有优点,因为限制归一化元素的数量减小了加法表的大小。但是应注意,这不是必须的,特别是可以期望表示(特别是广义化表示)的数量与群的大小相比较。例如,可以通过选择较大的第一作用群或较大的第一子集来增加归一化表示的数量;可以通过允许针对h的较大指数或选择较大的作用群或较大的第二子集来增加广义化表示的数量。

[0077] 图1示出了操作数存储设备150。操作数存储设备150存储将进行相加的群M的元素。除了加法之外的其他运算(例如乘法等)也可以在操作数存储设备150中的元素上执行。操作数存储设备150包括以归一化表示和广义化表示的操作数。操作数存储设备150的一部分可以是常数存储设备152,其被布置为存储以归一化表示的一个或多个常数加法输入。操作数存储设备150还可以包括以广义化形式的常数。在M的元素已经被相加或以其他方式计

算之后,它们可以再次被存储在操作数存储设备150(例如作为工作存储器)中。

[0078] 计算设备100包括加法表存储设备110,其为第二子集 $M_0$ 的每个元素 $m_i$ 存储查找表 $P_i$ 。这样的查找表将主群 $M$ 的归一化元素 $(\gamma, X)$ 作为输入,并且将输入映射到第一作用群 $N$ 的元素 $\lambda$ 和第一子集 $\Delta$ 的元素 $Y$ ,使得第一作用群 $N$ 的元素 $\lambda$ 和第一子集 $\Delta$ 的元素 $Y$ 的乘积是归一化元素 $\gamma X$ 与第二子集 $M_0$ 的元素 $m_i$ 的和: $\lambda Yh = \gamma X + m_i$ 。例如,查找表 $P_i$ 映射 $P_i(\gamma, X) = (\lambda, Y)$ ,使得 $\lambda Yh = \gamma X + m_i$ 。在实施例中,元素 $m_i$ 的查找表将归一化输入映射到归一化输出元素,使得归一化输入加上(群 $M$ 中的)元素 $m_i$ 等于归一化输出乘以生成元素 $h$ (使用第二作用群的作用)。

[0079] 注意,查找表仅将以归一化形式的 $M$ 的单个元素作为输入。该表的大小与归一化元素的数量相当,其可以大约是 $M$ 本身的大小。然而,这样的表可以用于将 $M$ 的两个元素相加。注意,需要两个输入来计算和的表会随着 $M$ 平方的大小而增长。这意味着,即使群 $M$ 的大小被选择为较大(例如大于512个元素或大于1024个元素),表的大小也近似线性增长,而不是平方地增长。

[0080] 计算设备100包括加法单元130。加法单元130被布置为例如通过加法单元130的接口接收第一加法输入和第二加法输入,第一加法输入和第二加法输入是主群 $M$ 的元素。第一加法输入以归一化表示被接收,例如, $\alpha_0 X_0$ ,其中 $\alpha_0$ 在第一作用群 $N$ 中,且 $X_0$ 在第一子集中。第二加法输入以广义化表示被接收,例如, $\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots$ 。加法单元130被布置为计算主群 $M$ 中的第一加法输入与第二加法输入的和。

[0081] 加法单元130被布置为通过将第二加法输入的被加数顺序地加到第一加法输入来计算部分和。将第二加法输入的被加数 $\gamma_t m_{i_t} h^t$ 加到部分和包含将针对第二子集 $M_0$ 的元素 $m_{i_t}$ 存储于加法表存储设备110中的查找表 $P_{i_t}$ 应用于所述被加数中。

[0082] 图1b示出了加法单元130的实施例。加法单元130接收第一加法输入131和第二加法输入132。加法单元130包括部分加法单元134,其被布置为将从第二加法输入132获得的被加数迭代地加到第一加法输入元素。例如,部分加法单元134可以加到被初始化为第一加法输入131的部分和133。该加法包含应用来自存储设备110的查找表。下面进一步讨论实施例的数学细节。

[0083] 例如,加法单元可以被布置为将部分和131初始设置为第一加法输入 $\alpha_0 X_0$ ,并且在第一加法输入的被加数上进行循环,在每个循环中通过加上第一加法输入的被加数 $\gamma_t m_{i_t} h^t$ 来更新部分和。下文给出的示例性算法可以由加法单元130用于将第一加法输入与第二加法输入相加。

[0084] 第一加法输入131被初始化为群 $M$ 的元素 $(\alpha_0, X_0)$ ,其中, $\alpha_0 \in N$ 且 $X_0 \in \Delta$ ;例如第一加法输入131可以被表示为对 $\{\alpha_0, X_0\}$ 。第二加法输入是群 $M$ 的元素 $\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots + \gamma_{\lambda k - 1} m_{i_{\lambda k - 1}} h^{\lambda k - 1}$ ,其中 $k$ 是生成元素的阶数, $\gamma_i \in N$ 且 $m_i \in M_0$ ,并且 $h$ 是生成元素。我们将假设 $\lambda = 1$ ,但是注意下面的公式直接扩展到其中 $\lambda > 1$ 的情况。例如,第二加法输入132可以被表示为序列 $\{\gamma_0, m_{i_0}, \gamma_1, \dots, \gamma_{k-1}, m_{i_{k-1}}\}$ 。

[0085] 加法单元130可以被布置为计算作为应用加法表 $P$ 之一的结果而获得的部分结果的以下序列。下面查找表 $P_i$ 的归一化输入和输出已经被表示为第一作用群 $N$ 的元素和第一

子集  $\Delta$  的元素的对。

$$[0086] \quad (\alpha_1, X_1) \leftarrow P_{i_0}(\gamma_0^{-1}\alpha_0, X_0)$$

$$[0087] \quad (\alpha_2, X_2) \leftarrow P_{i_1}(\gamma_1^{-1}\gamma_0\alpha_1, X_1)$$

$$[0088] \quad (\alpha_3, X_3) \leftarrow P_{i_2}(\gamma_2^{-1}\gamma_1\alpha_2, X_2)$$

$$[0089] \quad \dots$$

$$[0090] \quad (\alpha_k, X_k) \leftarrow P_{i_{k-1}}(\gamma_{k-1}^{-1}\gamma_{k-2}\alpha_{k-1}, X_{k-1})$$

[0091] 例如,加法单元130可以被布置为将部分和初始设置为第一加法输入  $(\alpha_0, X_0)$ 。对于生成元素  $h$  的每个指数  $t$ ,例如从0到  $\lambda k-1$ ,部分加法单元134通过加上对应于幂  $\gamma_t m_{i_t} h^t$  的被加数而从当前部分和  $(\alpha_t, X_t)$  获得下一部分和  $(\alpha_{t+1}, X_{t+1})$ 。后者包含将针对  $m_{i_t}$  的查找表  $P_{i_t}$  应用于  $(\gamma_t^{-1} \gamma_{t-1} \alpha_t, X_t)$ , 其中,  $\gamma_{-1}$  是第一作用群中的单位元素,并且其中  $(\alpha_t, X_t)$  是存储于部分和133中的当前部分和。

[0092] 部分和133中的部分和  $(\alpha_i, X_i)$  表示第一加法输入与第二加法输入的部分和。虽然部分和  $(\alpha_i, X_i)$  与所述和不同,但是我们知道,值  $\gamma_{t-1} \alpha_t X_t h^t$  的确等于部分和,例如,第一加法输入与第二加法输入的前  $t$  个被加数的和。结果是表示部分和使得部分和等于值  $\gamma_{t-1} \alpha_t X_t h^t$  是高效的。这得到短的计算序列。然而,其他表示是可能的,特别是部分和可以由直接等于部分和(没有常数)的归一化元素来表示,但是这将不必要地使加法复杂化。注意,部分和是以归一化表示的。通过替代加法表和部分和的定义,可以证实上述算法确实产生了正确的结果。注意,该算法包括在第一作用群中的计算。这种计算可以以任何传统方式来执行,例如使用第一作用群的一些规范化表示,或通过存储指示第一作用群中的计算结果的表等。

[0093] 作为该算法的结果,我们得到了上述算法的最终部分和  $(\alpha_k, X_k)$ , 即  $(\gamma_{k-1} \alpha_k X_k)$  等于第一加法输入与第二加法输入的和。在期望的情况下,加法单元130可以被布置具有计算  $\gamma_{k-1} \alpha_k$  的另一步骤。对  $\{\gamma_{k-1} \alpha_k, X_k\}$  表示以归一化表示的和。下面我们将假设已经通过将第一作用群中的元素乘以  $\gamma_{k-1}$  来转换最终的归一化输出。然而,注意,该最后的步骤并非必要的。例如,最终的乘法可以与在相同元素上执行的下一操作合并。特别是在混淆的实施方式中,推迟纠正乘法是有益处的。例如,最终的部分和可以被认为是编码和。为了获得加法的最终归一化输出,还需要  $\gamma_{k-1}$ , 并且其对攻击者而言是不可获得的。

[0094] 在实施例中,加法单元130将两个元素作为输入,一个是归一化表示,另一个是广义化表示,并且产生以归一化表示的元素作为输出。在实施例中,加法单元130将多个元素(例如,多于两个)(一个以归一化表示,其余以广义化表示)作为输入,并且产生以归一化表示的和作为输出。例如,可以将归一化元素加到每个广义化元素,产生归一化元素作为部分和,直到已经加上了所有的广义化元素,多个元素的最终和是以归一化表示的。

[0095] 上述示例性算法将归一化元素与广义化(非归一化)元素相加。该加法使用归一化输入。归一化输入可以通过对广义化操作数进行归一化来获得,或者通过使用从先前加法或其他归一化函数得到的输出或归一化常数来获得。

[0096] 在实施例中,计算设备100的外部输入可以被选择为是非归一化的。这避免了值的重复,通常我们有比归一化元素更多的非归一化元素。例如,在实施例中,多个非归一化元素可以被使用并且之后不再被使用。

[0097] 例如,如果期望用输入值 $x$ 和常数 $c$ 来计算 $x+c$ ,则可以用以归一化形式给出的 $c$ 和以非归一化形式给出的 $x$ 来计算 $c+x$ 。用 $d+e=c$ 计算 $(d+x)+e$ 甚至更好,其中 $d$ 是以归一化形式的,而 $x$ 和 $e$ 是以非归一化形式的。在后一种形式中,计算不会披露 $c$ 的归一化值,这使得攻击者很难知道隐藏在过程中出现的值下面的真实值。值 $c$ 或值 $d$ 和 $e$ 可以存储在操作数存储设备150中,例如,在常数存储设备152中。可以随机选择值 $d$ ,并且选择值 $e$ 以使得 $d+e=c$ 。

[0098] 如果有必要计算两个非归一化值的相加,则可以包括能够开始运算链的归一化常数(或多个归一化常数)。例如,如果 $x$ 和 $y$ 都是非广义化的,则 $0+x+y$ 的归一化表示可以代替 $x+y$ 的计算。常数0被表示为归一化元素。如果有必要将两个归一化元素相加,则可以用广义化表示替换它们中的一个,如第二个。例如,这可以通过针对所有 $X \in \Delta$ 映射针对 $X$ 的广义化表示的映射(例如表)完成。在实施例中,映射包括针对 $X$ 的多个广义化表示,使得针对广义化表示 $X$ 的选择不是唯一的,并且为混淆选择提供了一定灵活性。

[0099] 在实施例中,计算设备100包括网络接口,该网络接口被布置为从电子计算设备外部的计算机接收一个或多个加法输入。一个或多个加法输入是广义化表示;除了一个或多个加法输入之外,还可以接收其他输入,其中的一些可以是以归一化表示的。在常数存储设备152中,一个或多个常数加法输入被存储在归一化表示中。计算设备100被布置为使用加法单元将通过网络接口接收到的以广义化形式的选定加法输入与来自常数存储设备152的以归一化形式的选定常数加法输入相加。一般而言,计算设备100可以包括计算控制器,该计算控制器被布置为控制在操作数存储设备150中的哪些操作数上执行哪些操作,例如加法。计算控制器未被单独示出。在实施例中,常数存储设备包括对 $(d,e)$ ,其中 $d$ 被归一化且 $e$ 被广义化,常数 $d$ 被首先加到选定加法输入,随后加上常数 $e$ 。得到的归一化元素可以存储在操作数存储设备150中。

[0100] 相对容易地布置计算系统使得存在比归一化表示更多的广义化表示。在设备外部有更多的选择可以提高外部通信中的安全性。例如,在实施例中,多个传感器(或其他设备)通信以广义化表示编码的传感器数据(或其他数据)。每个传感器都可以访问所有广义化表示的私有子集,例如,所述多个私有子集中没有两个重叠超过元素的阈值,例如小于所述两个私有子集中的任何一个的大小的10%。在实施例中,所述多个私有子集中没有两个重叠。这具有两个传感器使用不同表示来通信其数据的优点。可以访问传感器并以某种方式找到传感器数据与其广义化表示之间的关系的攻击者不能使用该映射来解码从不同传感器截获的通信。注意,即使创建多个广义化表示或甚至许多广义化表示更容易,但是任何给定的群元素也可以由多个归一化表示来表示。

[0101] 在实施例中,计算设备100包括被布置为接收转换输入的转换单元150。

[0102] 例如,转换输入可以是以广义化形式的,并且要被转换为归一化形式。在这种情况下,转换单元150可以被布置为通过加上以归一化形式的主群的元素来将转换输入转换为归一化形式。该元素可以是0。转换单元150还可以加上非零元素,在这种情况下,后续运算可以被调整使得输入已经被修改,例如修改为编码。转换单元150还可以加上总和为0的多个元素,其中的至少一个是以归一化形式的。

[0103] 例如,转换输入可以是以归一化形式的,并且要被转换为广义化形式。在这种情况下,转换单元150可以被布置为存储将至少第一子集的元素映射到广义化形式的转换表。例如,如果根据该映射,归一化形式 $n \times X$ 中的 $X$ 被映射到

$\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots + \gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1}$ , 则归一化形式  $n \times$  映射到  $n(\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots + \gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1}) = (n\gamma_0) m_{i_0} h^0 + \dots + (n\gamma_{\lambda k-1}) m_{i_{\lambda k-1}} h^{\lambda k-1}$ 。

表示X的序列到表示nX的序列的变换可以通过在第一作用群中进行计算来完成。

[0104] 转换单元允许将主群的两个元素相加, 而不管表示如何。例如, 如果两个元素都是以规范表示的, 则它们中的一个元素可以被转换为广义化表示。例如, 如果两个元素都是以广义化表示的, 则它们中的一个元素可以被转换为规范表示。

[0105] 计算设备100的实施例包括函数单元124。函数单元被布置为将线性函数f应用于以广义化形式的函数输入。例如, 可以从操作数存储设备150接收广义化形式。

[0106] 函数输入包括线性函数表存储设备, 在其中存储表, 表将第一作用群N的元素  $\gamma_t$ 、第二子集  $M_0$  的元素  $m_{i_t}$  以及生成元素的幂  $h^t$  的乘积  $m = \sum_t \gamma_t m_{i_t} h^t$  作为输入, 并将该乘积映射到将线性函数应用于乘积的结果。函数单元被布置为将线性函数表存储设备的表应用于函数输入的被加数。例如, 输入  $\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots + \gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1}$  被映射到输出  $f(\gamma_0 m_{i_0} h^0) + \dots + f(\gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1})$ 。注意, 广义化表示中的可能的被加数的数量远小于广义化表示的数量。因此, 计算线性函数f所需的表远小于将任何广义化元素作为输入的表所需的。非线性操作可以在主群M的元素上执行, 可以例如通过表执行。

[0107] 本文中阐述的原理适用于广泛的阿贝尔群并允许大量的表示。下面给出了这些大量可能性中的多个选择。发明人进行的大量实验已经表明, 对于所有这些选择, 许多可能的主群M是可能的。

[0108] 在实施例中, h的阶数受到限制。例如, 在实施例中, 第二作用群H具有3个元素, 或者第二作用群H具有2个元素。更一般地, 阶数小于4或8或16等。在组合时, 针对广义化表示中的指数的上限可以被取为k-1。在加法期间所采取的步骤的数量随着H的大小而增加。通过选择相对较小的H, 例如具有2或3个元素, 加法具有更少的步骤并且计算更快。

[0109] 在实施例中, 第二子集  $M_0$  具有至少2个元素。增加第二子集中的元素的数量会增加广义化表示的数量。特别地, 广义化表示的数量可以被增加到需要使用任何广义化表示仅仅一次的点。后者完全消除了基于从广义化表示直接构建转换表的攻击。

[0110] 在实施例中, 第二子集中的元素的数量受到限制。随着第二子集的大小增加, 加法存储设备110中的表的数量也增加。例如, 第二子集中的元素的数量小于4或8或16等。特别地, 第二子集中的元素的数量可以是1。在实施例中, 第二子集  $M_0$  具有不是单位元素的1个元素。

[0111] 上面给出的选项可以被组合。例如, 在实施例中, 第二子集可以仅具有单个元素, 并且第二作用群可以具有恰好2个元素。通过选择足够大的第一作用群, M的所有元素仍然可以被表示。

[0112] 方便实现的是如下选择: N是循环群, 例如具有至少3个元素的循环群。在这种情况下, N由一些元素生成, 并且N的元素可以被表示为生成元素的指数。指数可以以编码形式存储。有利地, 生成元素可以被保密。

[0113] 阿贝尔群M可以是整数模一模数n的群:  $\mathbb{Z}_n$ 。通过将这些群中的多个组合在余数系统中, 可以在任意大的数字上执行算术。有利地, 表示这些群中的指数的数字可以根据实施例中的一个或多个来表示, 从而创建递归定义。模数n可以大于例如8。

[0114] 阿贝尔群M也可以是阿贝尔群 $\mathbb{Z}_2^t$ ,例如,其中 $t \geq 4$ ,具有 $2^t$ 个元素(不要与群 $\mathbb{Z}_2^t$ 混淆),其特别适合于二元计算,特别是XOR运算。

[0115] 上面的群具有特征2。这可以与小的第二作用群H组合,特别是与具有两个元素的第二作用群H组合。例如,H可以由元素 $h=-1$ 生成。在这种情况下,为了获得足够的广义化元素,广义化表示中的生成元素h的幂 $h^t$ 需要被允许超过阶数减 $(k-1)$ 。在实施例中,广义化表示中的指数最多为阶数的两倍减1,例如 $t \leq 2k-1$ 。

[0116] 如果主群M具有大于2的特征或者第二作用群的阶数大于2,则广义化表示中的h的指数可以被限制为至多阶数减1,例如, $t \leq k-1$ 。有利的是,生成元素可以被保密并且这些表相对较小。广义化元素的数量可以与期望的一样大,例如通过选择较大的H、 $M_0$ 等等。

[0117] 对于一些实施例,期望存在比归一化元素更多的广义化元素;例如,在广义化元素被用于保护外部输入的情况下。这可以通过选择第二作用群、可允许的指数、第二子集以及甚至足够大的第一作用群来获得。在实施例中, $(\#N \cdot \#M_0)^{\#H} \geq 3/2 \#N \cdot \#\Delta$ ,即广义化表示的数量是归一化表示的数量的至少 $3/2$ ,更具体地,其中 $(\#N \cdot \#M_0)^{\#H} \geq 5/2 \#N \cdot \#\Delta$ 等。

[0118] 如上所讨论的,第一子集 $\Delta$ 的元素可以从第一作用群在主群M上引起的轨道中选择。在实施例中,第一子集 $\Delta$ 的元素从第一作用群和第二作用群以及第二子集获得,即通过将第一作用群N的元素、第二子集的元素和第二作用群H的元素加生成元素的生成元素的阶数减1的幂的乘积求和形成的元素。第二作用群的元素是生成元素h的为至多生成元素的阶数减2的幂的幂。第一子集 $\Delta$ 的元素被选择为 $\beta_0 m_{i_0} h^0 + \dots + \beta_{k-2} m_{i_{k-2}} h^{k-2} + m_{i_{k-2}} h^{k-1}$ ,其中 $\beta_i$ 取自第一作用群,而m取自第二子集。可以看出,这将产生如下的工作第一子集:因为任何元素都可以被写为 $m = \gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \dots + \gamma_{k-1} m_{i_{k-1}} h^{k-1}$ ,所以后者可以被写为 $\gamma_{k-1} (\gamma_{k-1}^{-1} \gamma_0 m_{i_0} h^0 + \dots + \gamma_{k-1}^{-1} \gamma_{k-1} m_{i_{k-1}} h^{k-1})$ ,其是来自第一作用群中的元素( $\gamma_{k-1}$ )和如上定义的第一子集的元素乘积。注意,通常对于第一子集存在许多其他可能的选择,其中的一些可以比本示例小。然而,这表明在给定第二子集的情况下,可以至少以这种方式来构建合适的第一子集。

[0119] 第一子集的上述构建也适合于其中第二子集 $M_0$ 由单个元素组成的情况。在这种情况下,我们得到元素 $\beta_0 m_0 h^0 + \dots + \beta_{k-2} m_0 h^{k-2} + m_0 h^{k-1}$ ,导致第一子集的大小显著减小。通常,具有小的第一子集减少了归一化表示的数量,这继而减小了加法表的大小。加法表表示代码大小的重要部分,特别是混淆的(例如编码的)实施方式的代码大小的重要部分。

[0120] 下面给出主群、作用群和子集的一些示例。

[0121] 在第一示例中:主群是 $M = \mathbb{Z}_3 \times \mathbb{Z}_3$ 。M的元素可以被表示为两个元素的列向量。第一作用群N由矩阵 $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ 生成,并且具有大小4。第二作用群由元素-1生成, $H = \langle -1 \rangle$ ,并且具有大小2。群H的元素可以被表示为+I和-I,其中I表示单位矩阵。第二子集被选择为具有单个元素 $m_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ 的集合。M的所有元素都可以用广义化表示写为 $\gamma_0 m_0 - \gamma_1 m_0$ ,其中 $\gamma_0$ 和 $\gamma_1$ 在N中。使用上述构建将第一子集选择为集合 $\{x m_0 - m_0\}$ ,其中,x的范围是N中的所有元素。虽然主群、第一作用群和第二作用群以及第一子集和第二子集的元素可以被表示为矩阵或向量,但是一般情况下将可能的是它们也可以以某种编码形式表示,例如作为对应群或集合的随机排序的索引。

[0122] 在第二示例中：主群是  $M = \mathbb{Z}_3^4$ 。第一作用群由矩阵  $\begin{bmatrix} 0 & 2 & 2 & 0 \\ 2 & 1 & 1 & 2 \\ 2 & 2 & 2 & 0 \\ 2 & 0 & 1 & 2 \end{bmatrix}$  生成，并且具有阶

数5。第二作用群由元素-1生成并且具有大小2。第一子集具有三个元素  $M_0 = \left\{ \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 2 \end{bmatrix} \right\}$ 。

第一子集是通过在群M中的N的轨道中选取任意元素进行选择。第一子集具有17个元素。

[0123] 在第三示例中，主群是  $M = \mathbb{Z}_2^6$ ，这是特征为二的群。第一作用群N具有14个元素，并通过以下项生成：

$$[0124] \quad g = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ 和 } s = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}。$$

[0125] 元素g具有阶数7，元素s具有阶数2，并彼此交换。由g和s生成的第一作用群N具有阶数14。N的所有元素都可以被写为  $g^i s^j$ ，整数对 (i, j) 可以用于表示第一作用群的元素。第二子集由单个元素组成：

$$[0126] \quad m_0 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

[0127] 第二作用群是仅有单位元素的大小为1的群。生成元素的阶数k为1。在这种情况下，关于广义化表示中的指数的上界从k-1增加到2k-1，因此具有两个被加数。第一子集是从M上的N的轨道选择的，并且在最小选择中具有9个元素。

[0128] 在第四示例中，主群是  $M = \mathbb{Z}_2^4$ 。第一作用群和第二作用群两者都与  $\mathbb{Z}_3$  同构。第一

作用群由  $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$  生成，第二作用群由  $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$  生成；两个生成元都具有阶数3。第二

子集具有单个元素：

$$[0129] \quad m_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

[0130] 第一子集可以利用来自在M上引起的N的轨道的6个元素来选择。

[0131] 在第五示例中，主群是  $M = \mathbb{Z}_4^2$ 。第一作用群具有6个元素，并且由  $\begin{bmatrix} 3 & 3 \\ 1 & 2 \end{bmatrix}$  生成，第二作用群具有2个元素，并且由  $\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$  生成。第二子集具有单个元素  $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$ 。第一子集可以从轨道中选择，并可以包含5个元素。

[0132] 在这些示例中，第二作用群的大小可以被增加，以创建更多广义化表示。类似地，第一子集和第二子集的大小可以被增加。加法表可以根据定义方程进行计算。

[0133] 通常，在给定阿贝尔群M的情况下，其他元素可以如下选择。群M可以被写为

$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$  的乘积, 其中  $d_1 | d_2 \cdots | d_t$ 。这意味着其足以找到元素  $M^+ = (\mathbb{Z}_{d_t})^t$ , 然后投影到  $M$ 。可以按照以下过程进行:

[0134] 1、获得针对  $M^+$  的自同构群的生成元, 例如矩阵群  $Mat_{t \times t}(\mathbb{Z}_{d_t})$  的可逆元素。

[0135] 2、在自同构群中选择元素  $h$ , 例如, 作为生成元的随机乘积。 $H$  被获得为由  $h$  生成的群。

[0136] 3、选择群  $N$  作为自同构群的子群。例如, 在自同构群中选择一个、两个或更多个生成元。生成元被选择为与群  $H$  交换。注意, 当生成元的元素被视为矩阵时, 可以通过求解关于生成元的元素的线性方程组来完成找到针对  $N$  的这样的生成元。

[0137] 4、最后, 选择第一集合  $M_0$  和第二集合  $\Delta$ 。后者可以通过计算  $N$  的轨道来获得。前者可以通过例如递增地放大空集合来选择。

[0138] 最后, 判定由此获得的算术是否满足约束 (例如关于  $H$  的大小, 关于广义化表示的数量等), 如果否, 则例如可以从步骤 2 重复该过程。注意, 不同的算法是可能的, 例如, 可以交换步骤 2 和 3。这些构建允许例如用于高效的存储器使用。

[0139] 图 1 示出了用于在计算设备 100 处接收输入的两个选项。计算设备 100 可以包括编码单元 170, 其被布置为接收未编码输入, 例如以任何传统格式的主群  $M$  的元素。编码单元 170 将输入变换为规范表示或广义化表示。在实施例中, 编码单元 170 包括用于将群  $M$  的元素映射到规范表示或广义化表示的编码表。在实施例中, 编码单元 170 产生广义化元素。编码单元 170 不需要是计算设备 100 的一部分; 例如, 计算设备可以直接以编码格式 (特别是以广义化表示) 接收输入。例如, 后者可以通过在从其接收到直接输入 171 的外部计算机处具有编码单元 170 来实现。

[0140] 在实施例中, 针对相同的计算设备 100 产生多个编码单元 170。多个编码单元 170 被布置为接收未编码的输入, 并将该输入变换为广义化表示。多个编码单元 170 使用不同的广义化表示。例如, 对于多个编码单元中的任何两个编码单元, 存在主群  $M$  的元素  $x$ , 使得  $x$  由两个编码单元不同地编码。例如, 在实施例中, 存在由多个编码单元上的每个编码单元不同地编码的主群  $M$  的元素  $x$ 。

[0141] 计算设备 100 的输出也可以由解码单元 160 解码。或者, 计算设备 100 的输出可以以编码格式 (例如, 归一化表示或广义化表示) 返回。在本地, 在外部计算机处, 可以通过例如解码单元 160 来去除编码。因此, 单元 160 和 170 都可以从设备 100 中省略。

[0142] 图 1d 以示意形式示出了包括乘法单元 140 的计算设备 100' 的细化。计算设备 100' 可以与计算设备 100 相同, 除了以下所指示的。

[0143] 在这种情况下, 主群  $(M, +)$  还是环  $(R, +, \cdot)$ ; 除了加法之外, 还定义了乘法。乘法是满足结合律的, 在阿贝尔群运算上是满足分配律的, 并且具有单位元素。针对乘法的单位元素通常被写为 1。

[0144] 为了方便符号表示, 在本节中, 右符号表示用于第一作用群的作用。这意味着归一化元素被写为  $X\alpha$ , 其中  $X$  在第一子集中, 而  $\alpha$  在第一作用群中。第一作用群和第二作用群是从作为环的  $M$  的自同构群 (例如主环  $M$  与其自身的环同构的集合) 获取的。

[0145] 乘法单元 140 被布置为接收第一乘法输入 141 和第二乘法输入 142。图 1c 以示意形式给出了乘法单元 140 的可能实施例。第一乘法输入 141 和第二乘法输入 142 是主群  $(R)$  的元素, 在这种情况下主群实际上是环。第一乘法输入 141 以归一化表示  $X\alpha$  被接收, 并且第二乘

法输入142以广义化表示被接收。乘法单元140被布置为计算环(R)中的第一乘法输入141和第二乘法输入142的乘积。

[0146] 乘法单元140被布置为:

[0147] -计算来自第一乘法输入141的第一加法输入145和第二乘法输入142的第一被加数,第一加法输入是以归一化形式的,并且

[0148] -计算来自第一乘法输入的一个或多个第二加法输入146和第二乘法输入142的除了用于计算第一加法输入145的第一被加数之外的多个被加数。一个或多个第二加法输入146是以广义化形式的。

[0149] 乘法单元140可以包括中间乘法单元144,其被布置为计算来自第一乘法输入141的第一加法输入145和来自第二乘法输入142的一个或多个第二加法输入146,如图1c所示。确定加法输入可以包含第一作用群和第二作用群中的运算,但不需要加法表。在从乘法输入转换到加法输入之后,例如通过加法单元130将第一加法输入145与一个或多个第二加法输入146相加。

[0150] 因为相同的表被用于加法和乘法,所以在逆向工程期间将很难看到是执行加法还是乘法。即使攻击者能够找到使用的表,并且即使他能够以某种方式发现其功能为加法表,他将仍然不知道是执行加法还是乘法运算。此外,由于乘法不需要加法表,所以代码大小被减小。

[0151] 在实施例中,第一作用群N和第二作用群H是环U(R)的单元的群子群,通过乘法作用于主群,第二子群 $M_0$ 仅包括主群的单位元素,例如,元素 $m_0=1$ 。在这种情况下,第一子集可以如上面所指示的那样被构建为元素 $\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}$ 。在这种情况下,第一乘法输入141具有形式 $(\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha = X\alpha$ ,并且第二乘法输入142具有形式 $(\gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots)$ 。

[0152] 下面给出将乘法输入转换为加法输入的转换算法的示例。假设第一乘法输入141为 $r = X\alpha = (\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha$ ,第二乘法输入142为 $r' = \gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots + \gamma_{k-1} h^{k-1}$ 。乘法 $r \cdot r'$ 用'的每个被加数来完成。第一个是 $r \gamma_0 h^0 = X(\alpha \gamma_0)$ ,该归一化元素是第一乘法输入145。以下是 $X\alpha \gamma_i h^i$ ,其中 $i > 0$ 。使用直接计算,使用分布性和 $h^k=1$ 的事实,我们获得一般表示 $X\alpha \gamma_i h^i$ 。该过程生成 $k-1$ 个以广义化表示的加法输入146,其与用于第一加法输入145(其为归一化元素)的加法公式相加。加法的数量随着k增加。使用 $k=2$ ,意味着乘法和加法具有相同的复杂性,这使得攻击者更难以区分代码中的加法和乘法运算。

[0153] 在实施例中,第一作用群N和第二作用群H是环U(R)的单元的群子群,通过乘法作用于主群,第二子集 $M_0$ 仅包括主群的单位元素。

[0154] 图2示意性地示出了计算设备101的实施例的示例。计算设备101是计算设备100'的细化。在实施例中,计算设备101包括多个加法单元和多个乘法单元。例如,图2示出了三个乘法单元1401.1、140.2和140.3以及两个加法单元130.1和130.2。这些单元可以分别具有与单元140和130相同的设计。乘法单元和加法单元占用相对少的空间,例如,当用软件实现时,这些单元不需要超过几百个低级计算机指令。特别地,加法单元和/或乘法单元的副本可以被用于在计算机程序中所需的每次乘法或加法。这允许传统的混淆技术使这些副本不同,使得攻击者不能看到使用相同的运算符。取决于例如所使用的混淆,乘法单元和/或加法单元可以被重复用于多次计算。作为范例,图2示出了如何使用混淆的算术来计算多项

式 $ax^2+bx+c$ 。

[0155] 多个算术单元的操作(例如,加法、乘法)可以按其数据依赖性所允许的任何顺序进行。例如,操作140.3可以在130.1之前的任何点处被插入到顺序140.1、140.2、130.1和130.2中。此外,后续乘法或加法的顺序可以颠倒。因此,像图2那样的图可以以许多方式以软件程序的线性顺序转换。不需要将单元严格分开;第一单元的指令可以与其他单元的指令散布在一起。

[0156] 图3示意性地示出了用于计算用于在计算设备中使用的加法表的表计算设备200的实施例的示例。加法表可以被使用在像计算设备100等的设备中。加法表可以存储在非暂态存储设备上,例如硬盘、非易失性存储器芯片等。

[0157] 表计算设备200被布置用于计算用于在被布置为将主群 $(M, +)$ 的两个元素相加的电子计算设备中使用的查找表,该主群是有限阿贝尔群 $(\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t})$ 。

[0158] 表计算设备包括表创建单元210,其被布置为构建针对第二子集 $M_0$ 的元素 $m_i$ 的查找表。表创建单元被布置为:

[0159] -重复地选择主群 $M$ 的输入归一化元素 $(\gamma, X)$ 。例如,设备200可以选择第一作用群的元素和第一子集的元素以选择归一化元素。

[0160] -确定输入归一化元素 $\gamma X$ 和第二子集 $M_0$ 的所述元素 $m_i$ 的和 $s = \gamma X + m_i$ 。这种加法可以在主群 $M$ 中完成。例如,输入归一化元素和 $m_i$ 两者都可以被转换为 $M$ 的规范化表示。并不反对设备200在主群 $M$ 中在没有混淆的情况下进行计算,因为设备200通常将不是计算设备100本身的一部分。

[0161] -确定第一作用群 $N$ 的元素 $\lambda$ 和第一子集 $\Delta$ 的元素 $Y$ ,使得第一作用群 $N$ 的元素 $\lambda$ 与第一子集 $\Delta$ 的元素 $Y$ 的乘积是所述和: $\lambda Y h = s = \gamma X + m_i$ 。例如,可以计算 $sh^{-1}$ 并例如使用转换表将其转换为归一化形式。或者,可以计算所有归一化元素的和,创建和的表,接着循环遍历所有归一化元素 $\lambda Y$ ,并确定哪个和等于 $\lambda Y h$ 。

[0162] -将条目添加到查找表,该查找表将输入环元素映射到第一作用群 $N$ 的元素 $\lambda$ 和第一子集 $\Delta$ 的元素 $Y$ 。

[0163] 结果是第二子集 $M_0$ 的元素 $m_i$ 的表。可以针对第二子集的所有其他元素重复表创建。

[0164] 操作数存储设备150、加法表存储设备110等可以被实现为电子存储器。存储器的一部分可以是易失性的或非易失性的。例如,它们可以包括SRAM、FLASH或ROM存储器。也可以使用其他存储技术,例如,磁存储、云存储等。有利地,所使用的存储设备允许快速随机访问,例如,紧密/牢固耦合的存储器。

[0165] 典型地,设备100、100'和200各自包括执行存储于设备处的适当软件的微处理器(未单独示出);例如,软件可以已经被下载和/或存储在对应的存储器中,例如,诸如RAM的易失性存储器或诸如闪存(未单独示出)的非易失性存储器。设备100、100'和200还可以配备有微处理器和存储器(未单独示出)。或者,这些设备可以全部或部分地以可编程逻辑实现,例如作为现场可编程门阵列(FPGA)。设备100、100'和200可以整体或部分地实现为所谓的专用集成电路(ASIC),即,为其特定用途定制的集成电路(IC)。例如,电路可以用CMOS来实现,例如使用诸如Verilog、VHDL等的硬件描述语言。

[0166] 计算的实施例可以包括加法电路、转换电路、函数电路和/或乘法电路等。这些电路实现本文中描述的对应单元。这些电路可以是处理器电路和存储电路,处理器电路执行

以电子方式在存储电路中表示的指令。这些电路也可以是FPGA、ASIC等。

[0167] 图3是以示意方式示出用于将主群  $(M, +)$  的两个元素相加的电子计算方法300的流程图,主群是有限阿贝尔群  $(\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{k_t}})$ 。

[0168] 方法300包括:

[0169] -为第二子集  $(M_0)$  的每个元素  $(m_i)$  存储310查找表  $(P_i)$ ,所述查找表将主群  $(M)$  的归一化元素  $((\gamma, X))$  作为输入,并将输入映射到第一作用群  $(N)$  的元素  $(\lambda)$  和第一子集  $(\Delta)$  的元素  $(Y)$ ,第一作用群  $(N)$  的元素  $(\lambda)$  和第一子集  $(\Delta)$  的元素  $(Y)$  的乘积为归一化元素  $(\gamma X)$  和第二子集  $(M_0)$  的所述元素  $(m_i)$  的和  $(\lambda Yh = \gamma X + m_i)$ 。例如,可以通过具有存储加法表的存储器来执行存储。

[0170] -接收320第一加法输入  $(\alpha_0 X_0)$  和第二加法输入  $(\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots)$ ,第一加法输入和第二加法输入是主群  $(M)$  的元素,其中,第一加法输入以归一化表示被接收,并且第二加法输入以广义化表示被接收,并且计算主群  $(M)$  中的第一加法输入和第二加法输入的和,其中,所述计算包括:

[0171] -通过将第二加法输入的被加数顺序地加到第一加法输入来计算330部分和,其中,

[0172] -将第二加法输入的被加数  $(\gamma_t m_{i_t} h^t)$  加到340部分和中包括将针对第二子集  $(M_0)$  的元素  $(m_{i_t})$  的查找表  $(P_{i_t})$  应用于被加数中。

[0173] 图5示出了以示意形式示出用于计算用于在被布置为将主群  $(M, +)$  的两个元素相加的电子计算设备中使用的查找表的表计算方法400,主群是有限阿贝尔群  $(\mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{k_t}})$ ,该表计算方法包括:

[0174] -重复地选择(410)主群  $(M)$  的输入归一化元素  $((\gamma, X))$ ,

[0175] -确定输入归一化元素  $(\gamma X)$  和第二子集  $(M_0)$  的所述元素  $(m_i)$  的和  $(\lambda Yh = \gamma X + m_i)$ ,

[0176] -确定(420)第一作用群  $(N)$  的元素  $(\lambda)$  和第一子集  $(\Delta)$  的元素  $(Y)$ ,使得第一作用群  $(N)$  的元素  $(\lambda)$  和第一子集  $(\Delta)$  的元素  $(Y)$  是所述和,

[0177] -将条目添加(430)到查找表,该查找表将输入环元素映射到第一作用群  $(N)$  的元素  $(\lambda)$  和第一子集  $(\Delta)$  的元素  $(Y)$ 。

[0178] 对于本领域技术人员来说将显而易见的是,执行该方法的许多不同方式是可能的。例如,可以改变步骤的顺序或者可以并行执行一些步骤。此外,在两个步骤之间可以插入其他方法步骤。插入的步骤可以表示诸如本文所述的方法的细化,或者可以与该方法无关。此外,在下一步骤开始之前,给定的步骤可以尚未完成。

[0179] 根据本发明的方法可以使用软件来执行,所述软件包括用于使处理器系统执行方法300和400的指令。软件可以仅包括由系统的特定子实体采取的那些步骤。该软件可以存储于诸如硬盘、软盘、存储器、光盘等的合适的存储介质中。该软件可以作为信号沿着有线或无线发送,或者使用数据网络(例如互联网)发送。该软件可以用于下载和/或在服务器上远程使用。根据本发明的方法可以使用被布置为配置可编程逻辑(例如,现场可编程门阵列(FPGA))的比特流来执行以执行该方法。

[0180] 将认识到,本发明还扩展到计算机程序,特别是在载体上或中适于将本发明付诸实践的计算机程序。该程序可以采用源代码、目标代码、代码中间源和目标代码(例如部分

编译的形式)的形式,或者以适合于使用在根据本发明的方法的实施方式中的任何其他形式。涉及计算机程序产品的实施例包括对应于所阐述的方法中的至少一个的处理步骤中的每个的计算机可执行指令。这些指令可以被细分为子例程和/或存储在可以被静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一实施例包括对应于所阐述的系统

和/或乘积中的至少一个的单元中的每个的计算机可执行指令。

[0181] 图6a示出了根据实施例的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,计算机程序1020包括用于使处理器系统执行用于将主群的两个元素相加的方法或用于计算用于在电子计算设备中使用的查找表的方法的指令。计算机程序1020可以作为物理标记被体现在计算机可读介质1000上或通过计算机可读介质1000的磁化来实现。然而,也可以想到任何其他合适的实施例。此外,将认识到,虽然计算机可读介质1000在这里被示出为光盘,但是计算机可读介质1000可以是任何合适的计算机可读介质,例如硬盘、固态存储器、闪存等,并且可以是不可记录的或可记录的。计算机程序1020包括用于使处理器系统执行用于将主群的两个元素相加的计算方法或用于计算用于在电子计算设备中使用的查找表的方法的所述方法的指令。

[0182] 图6b示出了根据实施例的处理器系统1140的示意图。处理器系统包括一个或多个集成电路1110。图6b示意性地示出了一个或多个集成电路1110的架构。电路1110包括处理单元1120(例如CPU),其用于运行计算机程序部件以执行根据实施例的方法和/或实现其模块或单元。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的一部分可以是只读的。电路1110可以包括通信元件1126,例如天线、连接器或两者,等等。电路1110可以包括用于执行该方法中定义的部分或全部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可以经由互连件1130(例如总线)彼此连接。处理器系统1110可以被布置用于分别使用天线和/或连接器进行接触式通信和/或无接触式通信。

[0183] 应当指出,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出许多备选实施例。

[0184] 在权利要求中,置于括号间的任何附图标记不应被解释为限制权利要求。对动词“包括”及其变形的使用不排除除了权利要求中陈述的元件或步骤以外的元件或步骤的存在。在元件前面的词语“一(a)”或“一个(an)”不排除多个这种元件的存在。本发明可以通过包括几个不同元件的硬件以及通过适当编程的计算机来实现。在枚举了若干单元的设备权利要求中,这些单元中的若干可以由同一项硬件来体现。在相互不同的从属权利要求中记载了某些措施的仅有事实并不指示不能有利地使用这些措施的组合。

[0185] 在权利要求中,括号内的引用是指实施例的附图中的附图标记或实施例的公式,因此增加了权利要求的可理解性。这些引用不应被解释为限制权利要求。

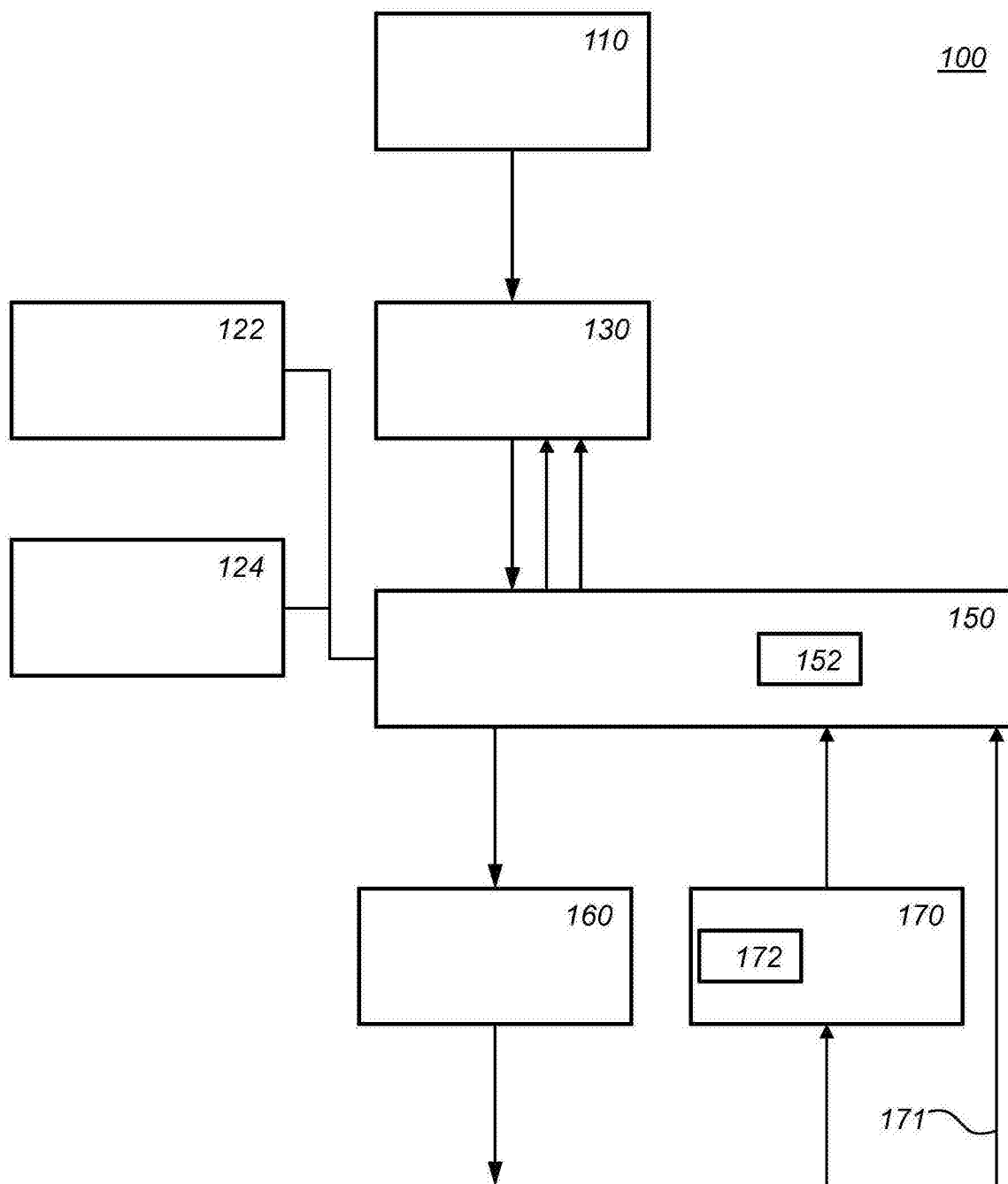


图1a

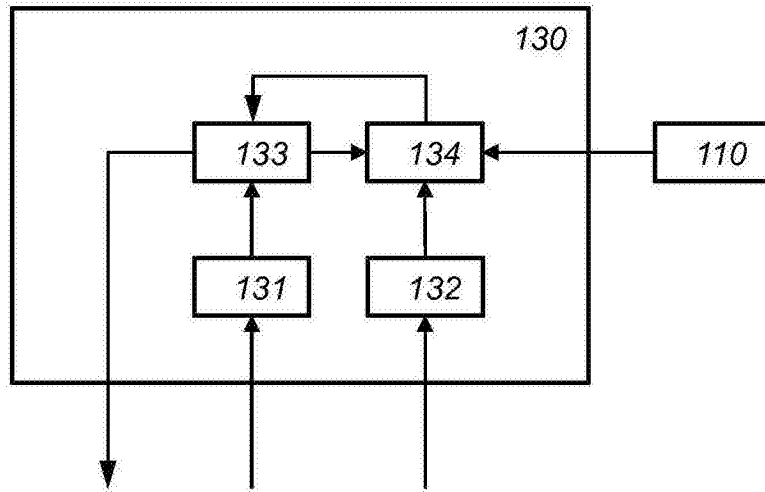


图1b

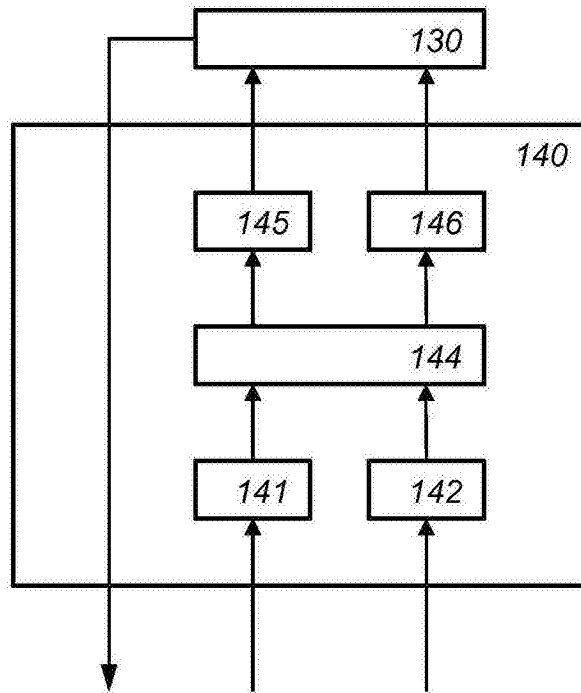


图1c

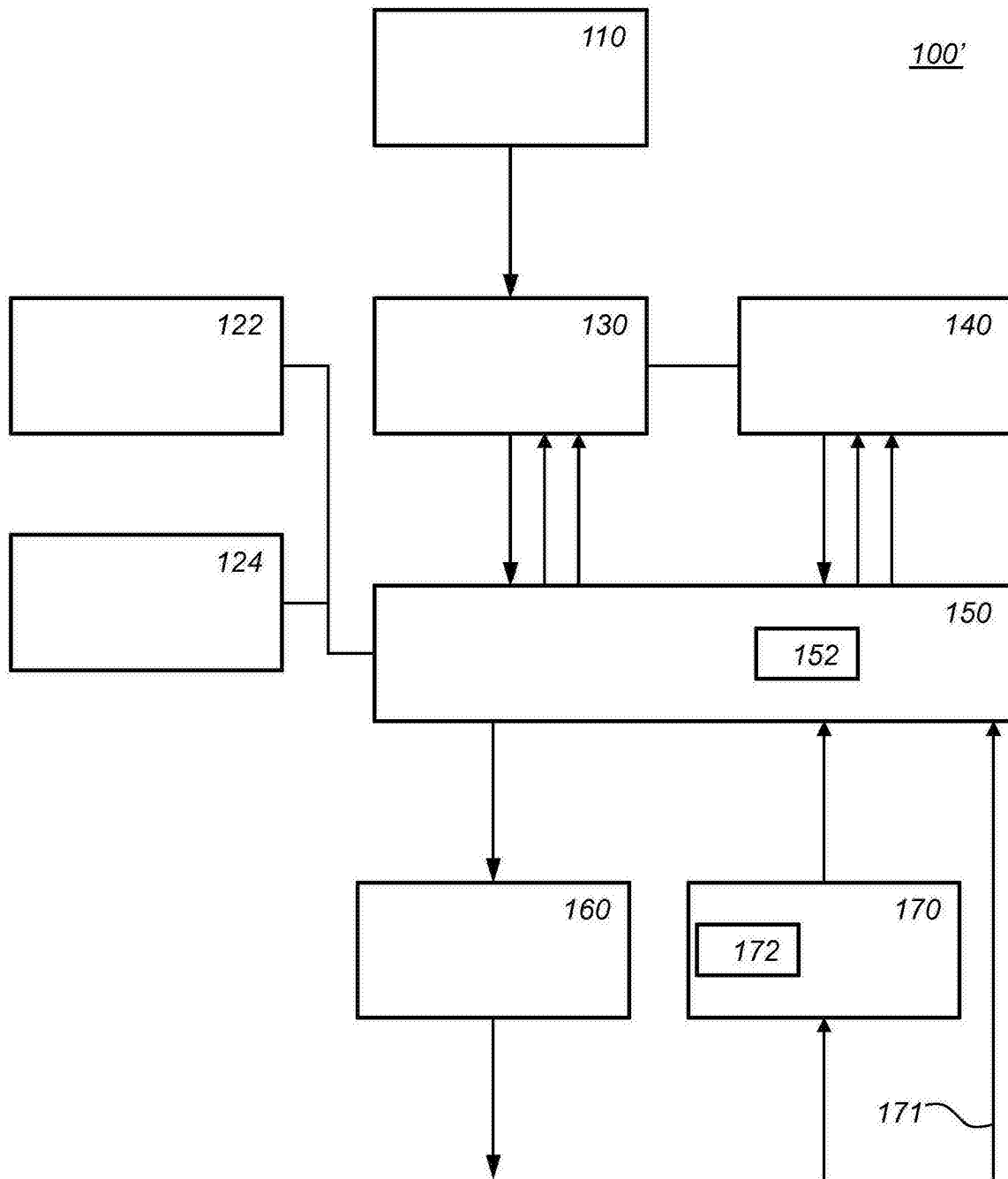


图1d

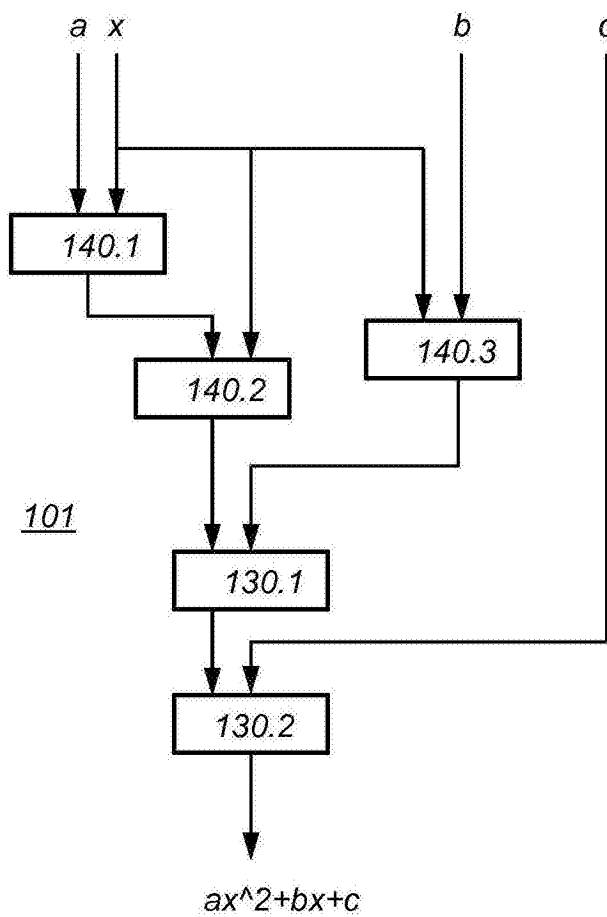


图2

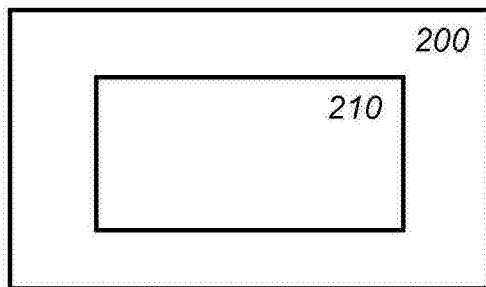


图3

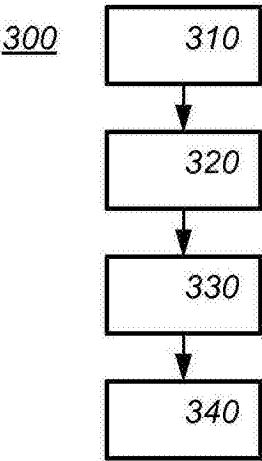


图4

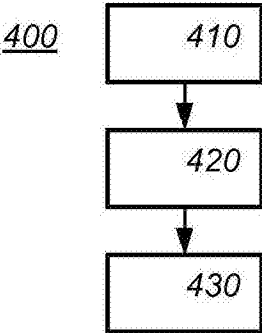


图5

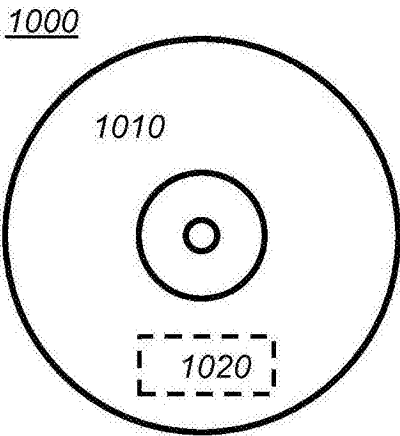


图6a

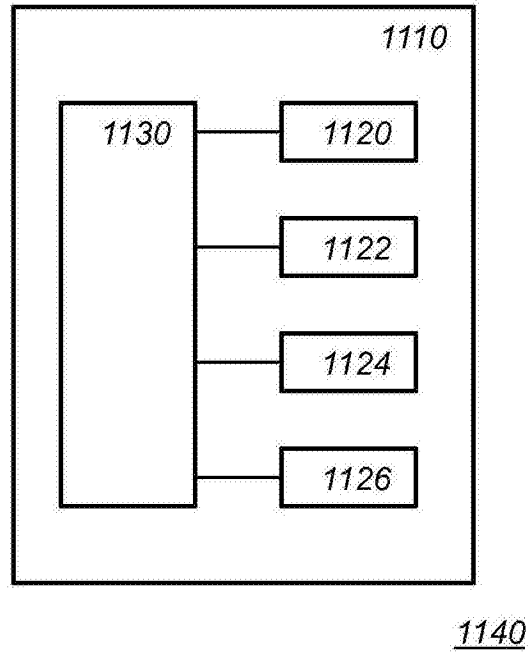


图6b