

(12) 发明专利

(10) 授权公告号 CN 101300569 B

(45) 授权公告日 2010. 06. 16

(21) 申请号 200680040456. 4

(22) 申请日 2006. 10. 16

(30) 优先权数据

11/263, 701 2005. 11. 01 US

(85) PCT申请进入国家阶段日

2008. 04. 28

(86) PCT申请的申请数据

PCT/US2006/040538 2006. 10. 16

(87) PCT申请的公布数据

W02007/053295 EN 2007. 05. 10

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 K·E·劳特 D·X·查尔斯

E·Z·戈伦

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

代理人 陈斌

(51) Int. Cl.

G06F 17/00 (2006. 01)

(56) 对比文件

US 6104811 A, 2000. 08. 15, 全文.

CN 1236454 A, 1999. 11. 24, 全文.

审查员 富瑶

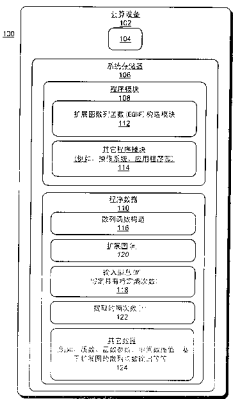
权利要求书 2 页 说明书 8 页 附图 4 页

(54) 发明名称

用于从扩展图构造散列函数的系统和方法

(57) 摘要

描述了从扩展图构造散列函数。在一方面，走查一扩展图以计算散列函数。该扩展图是使用输入消息的相应子集来走查的。所走查的最后一个顶点的标签是该散列函数的输出。



1. 一种从扩展图构造散列函数的方法,包括:

根据对一散列函数的输入走查一扩展图,所述扩展图是使用输入消息的相应子集来走查的;

确定所走查的最后一个顶点的标签;以及

输出所述标签作为所述散列函数的结果。

2. 如权利要求 1 所述的方法,其特征在于,所述扩展图是 Ramanujan 图。

3. 如权利要求 1 所述的方法,其特征在于,所述扩展图是 Lubotzky-Phillips-Sarnak 扩展图。

4. 如权利要求 1 所述的方法,其特征在于,所述扩展图是有限特征域 p 上的超奇异椭圆曲线的图。

5. 如权利要求 1 所述的方法,其特征在于,所述结果是密码散列。

6. 如权利要求 1 所述的方法,其特征在于,找出所述散列函数的冲突在计算上是困难的。

7. 如权利要求 1 所述的方法,其特征在于,所述输入消息具有特定的熵次数,并且其中,所述散列函数是抗冲突的。

8. 如权利要求 1 所述的方法,其特征在于,走查还包括:

将所述输入消息划分成段;以及

对这些段中的至少一个子集,基于一子集的特定一段的各方面来确定到所述扩展图中的下一相应顶点的路径。

9. 如权利要求 1 所述的方法,其特征在于,所述扩展图包括 n 个顶点,其中所述输入消息具有一熵次数,并且其中,所述方法还包括:

向所述图的各顶点分配相应的标签;

确定所述熵次数;

其中,走查还包括使用所述熵次数来走查所述 n 个顶点以标识完全随机的顶点输出;并且

所述输出是所走查的 n 个顶点中的最后一个顶点的相应的所分配的标签。

10. 如权利要求 9 所述的方法,其特征在于,确定所述熵次数包括使用一提取器函数来确定与所述输入消息相关联的随机性程度。

11. 一种用于从扩展图构造散列函数的方法,包括:

将消息划分成段;

根据对一散列函数的输入走查一扩展图,所述扩展图是使用所述各段中的相应段确定到所述扩展图中的 n 个顶点中的下一顶点的路径来走查的;

确定所走查的最后一个顶点的标签;以及

输出所述标签作为所述散列函数的结果。

12. 如权利要求 11 所述的方法,其特征在于,所述扩展图是 Ramanujan 图或 Lubotzky-Phillips-Sarnak 扩展图。

13. 如权利要求 11 所述的方法,其特征在于,所述结果是密码散列。

14. 如权利要求 11 所述的方法,其特征在于,找出所述散列函数的冲突在计算上是困难的。

15. 如权利要求 11 所述的方法,其特征在于,所述消息基于从所述消息中提取的熵次数被划分成所述段。

16. 如权利要求 11 所述的方法,其特征在于,所述扩展图包括 n 个顶点,其中所述消息具有一熵次数,并且其中,所述方法还包括:

向所述图的各顶点分配相应的标签;

确定所述熵次数;

其中,走查还包括使用所述熵次数来走查所述 n 个顶点以标识完全随机的顶点输出;并且

所述输出是所走查的 n 个顶点中的最后一个顶点的相应的所分配的标签。

17. 如权利要求 11 所述的方法,其特征在于,所述确定熵次数包括使用一提取器函数来确定与所述消息相关联的随机性程度。

18. 一种用于从扩展图构造散列函数的计算设备,包括:

用于根据对一散列函数的输入走查扩展图的装置,所述扩展图是使用输入消息的相应子集来走查的;

用于确定所走查的最后一个顶点的标签的装置;以及

用于输出所述标签作为所述散列函数的结果的装置。

19. 如权利要求 18 所述的计算设备,其特征在于,所述扩展图是 Ramanujan 图或 Lubotzky-Phillips-Sarnak 扩展图。

20. 如权利要求 18 所述的计算设备,其特征在于,所述结果是密码散列。

用于从扩展图构造散列函数的系统和方法

技术领域

[0001] 本申请涉及构造散列函数。

背景技术

[0002] 散列函数构造在许多算法和密码协议中使用。它们是将其像“均匀”分布的函数 $f:U \rightarrow S$, 其中 $|U| \geq |S|$ 。换言之, 对于大多数

[0003] $x \in U$, $|\{y \in U | f(x) = y\}|$ 接近于 $\frac{|U|}{|S|}$ 。

[0004] 使冲突对 (colliding pair), 即使得 $f(x) = f(y)$ 的对 (x, y) 的数量最小化的散列函数是非常有用的。对于散列函数的密码学应用, 通常希望工程设计冲突的问题是困难的。这意味着找到使得 $f(x) = f(y)$ 的不同元素 x 和 y 的任务在计算上是困难的。通常, 对于以下较弱的性质是感兴趣的: 给定 x , 找到另一 y , 使得 $f(x) = f(y)$ 是困难的。

发明内容

[0005] 提供本概述以使用简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述并不旨在确定所要求保护的主题的关键特征或必要特征, 也不旨在用于帮助确定所要求保护的主题的范围。

[0006] 鉴于上述内容, 描述了从扩展图 (expander graph) 构造散列函数。在一方面, 走查作为散列函数的输入的扩展图。使用输入消息的相应子集来走查该扩展图。散列函数的输出是所走查的最后一个顶点的标签。

附图说明

[0007] 在附图中, 组件参考标号最左边的数字标识该组件首次出现的特定图。

[0008] 图 1 示出了根据一个实施例的用于从扩展图构造散列函数的示例性系统。

[0009] 图 2 示出了根据一个实施例的用于从扩展图构造散列函数的示例性过程。

[0010] 图 3 示出了根据一个实施例的用于从扩展图构造散列函数的示例性过程。

[0011] 图 4 示出了其中可全部或部分地实现从扩展图的散列函数构造的合适的计算环境的一个示例。

具体实施方式

[0012] 综述

[0013] 以下参考图 1 到 4 描述用于从扩展图构造散列函数的系统 (例如, 系统、装置、计算机可读介质等) 和方法。散列函数通过在特定扩展图上走查来构造。对一扩展图的随机走查非常快速地混合, 因此散列函数输出在输入消息是均匀地随机的时候一般是均匀的。在一个实现中, 该系统和方法使用提取器 (extractor) 结合扩展图来产生散列函数。在此实现中, 输入消息对最小熵 (min-entropy) 具有特定下限。例如, 用密码签署一消息 (通过

散列来完成)是在向该消息添加“随机填充(random pad)”之后完成的。(该过程将熵注入到签名中)。假设输入消息具有某一少量的熵,则利用提取器来提取该随机性然后根据提取器的输出执行走查。

[0014] 现在更详细描述用于从扩展图构造散列函数的系统列和方法的这些和其它方面。

[0015] 示例性系统

[0016] 尽管并非必需,但是用于从扩展图构造散列函数的系统和方法将在由诸如个人计算机等计算设备执行的计算机可执行指令(程序模块)的一般上下文中描述。程序模块一般包括执行特定的任务或实现特定的抽象数据类型的例程、程序、对象、组件、数据结构等等。尽管该系统和方法是在上述上下文中描述的,但是以下所描述的动作和操作也可以用硬件来实现。

[0017] 图1示出了根据一个实施例的用于从扩展图构造散列函数的示例性系统100。系统100包括计算设备102,它包括耦合到系统存储器106的一个或多个处理单元104。处理器104从程序模块108中取出并执行计算机程序指令,并从系统存储器106存取程序数据110部分。程序模块108包括,例如扩展图散列函数构造模块(“EGHF构造模块”)112和其它程序模块114。其它程序模块114包括,例如操作系统和利用由模块112生成的基于扩展图的散列函数构造116的一个或多个应用程序。存在对其可用这一散列函数构造116的许多应用程序。例如,这一构造可用于实现密码术、散列表、纠错、音频标识、Rabin-Karp串搜索算法等的一个或多个应用程序。

[0018] EGHF构造模块112从输入消息118和 n 个顶点的扩展图120生成散列函数构造116。扩展图118是具有高顶点或边扩展,或者换言之是高度连接的稀疏图。在一个实现中,扩展图118是Ramanujan图。在一个实现中,输入消息118具有一随机性程度(或熵)。

[0019] 例如,在一个实现中,扩展图120如下确定。设 p 是质数,并设 $l(\neq p)$ 是另一质数。扩展图 $G(p, l)$ 具有 V 作为其顶点集, V 是有限域 F_q 上的超奇异(supersingular) j 不变式(j -invariant), $q = p^2$ 。如果在其 j 不变式是 j_1 和 j_2 的超奇异椭圆曲线之间有次数为1的同源,则在顶点 j_1 和 j_2 之间有一条边。图 $G(p, l)$ 被称为是 $l+1$ 正则Ramanujan图。 $G(p, l)$ 的顶点数是四元数代数 $B_{p,\infty}$ 的类数,这大约是 $p/12$ 。 $G(p, l)$ 是扩展图120。

[0020] 在另一实现中,扩展图120是Lubotzky-Phillips-Sarnak扩展图,如在以下“替换实施例”一节中所描述的。

[0021] 为了生成散列函数构造116,扩展图散列函数构造模块112标识消息118。在一个实现中消息具有熵次数。EGHF构造模块112向构成扩展图120的 n 个顶点中的每一顶点分配相应的名称或标签。当输入消息具有与其相关联的熵次数时,EGHF构造模块112用一提取器函数来提取(确定)随机性程度。从这一消息中提取随机性的示例性的这样的提取函数和技术在以下题为“从输入中提取随机性”一节中更详细描述。

[0022] 鉴于标识要随机地走查(访问)的扩展图120的顶点的可配置顶点边约定,构造模块112基于所提取的熵次数(当存在时)或其它客观准则(以下描述)来标识输入消息118的 k 长度比特段。走查扩展图120的示例性操作在以下题为“示例性过程”一节中更详细描述。与所走查的顶点中的最后一个顶点相关联的相应名称/标签表示散列函数构造114的输出。

[0023] 从输入中提取随机性

[0024] 最小熵: 设 X 是在 $\{0, 1\}^n$ 中取值的随机变量。 X 的最小熵被定义为以下量

$$[0025] \quad \min_{x \in \{0, 1\}^n} \left(-\log \left(\Pr[X = x] \right) \right)$$

[0026] 分布接近度 (closeness): 设 X 和 Y 是 $\{0, 1\}^d$ 上的两个分布。 如果

$$[0027] \quad \max_{x \in \{0, 1\}^d} |\Pr[X = x] - \Pr[Y = x]| \leq \varepsilon$$

[0028] 则它们被认为是 ε 接近 (ε -close) 的 (ε 是实数)。

[0029] 提取器: 如果对最小熵 $\{0, 1\}^n$ 上的任何随机变量 X , 至少 k 和 $U_d(\{0, 1\}^d)$ 上的均匀分布), 分布 $\text{Ext}(X, U_d)$ 对 U_m 是 ε 接近的, 则函数 $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ 被称为 (k, ε) 提取器 ((k, ε) -extractor)。

[0030] 定理: 如果 $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ 是 (k, ε) 提取器, 则对于随机种子 $\sigma \in \{0, 1\}^d$ 的大多数选择, 分布 $\text{Ext}(X, U_d)$ 对 U_m 是 ε 接近的。

[0031] 证明: 分布 $\text{Ext}(X, U_d)$ 可被描述为在由 $\sigma \in \{0, 1\}^d$ 索引的分布的簇 X_d 中均匀地随机选择一分布, 其中 $\sigma \in \{0, 1\}^d$ 由 $X_d = \text{Ext}(X, \sigma)$ 定义。 Ext 是提取器的事实意味着这些分布中的许多都对 U_m 是 ε 接近的 (证明结束)。

[0032] 如果 d 至少是 $\log^2 n$ 并且 $m = k^{1-\alpha}$, 其中 α 是任意实数, 则多项式时间提取器的构造对于任何 $k > n^\gamma$ ($\gamma < 1$) 和 $\varepsilon > 0$ 都是已知的。

[0033] 散列函数的构造

[0034] 表示对散列函数构造 116 的输入的随机变量 M (即, 输入消息 118) 具有至少为 $\log^{1+\beta} n$ 的最小熵, 其中 n 是 $G(p, 1)$ 的顶点数, 且 $\beta > 0$ 。 设 $\{0, 1\}^N$ 是输入空间。 为确定 M 的熵次数 122, 构造模块 112 实现提取器函数 Ext , 并用参数 $k = \log^{1+\beta} n$ 来修正函数 $\text{Ext}: \{0, 1\}^N \times \{0, 1\}^d \rightarrow \{0, 1\}^m$, ε 非常小并且 $m = \Theta(\log^{1+\alpha} n)$ 。 出于示例性说明的目的, 这些参数被示为“其它数据”124 的相应部分。 系统 100 假定 $N = k^{O(1)}$ 。 构造模块 112 从 $\{0, 1\}^d$ 中均匀地随机选取 a 。 给定输入 $x \in \{0, 1\}^N$, 构造模块 112 计算 $\varpi = \text{Ext}(x, a)$ (即, 熵次数 122)。 该构造的结果是大小为 m 的串。 构造模块 112 从某一固定顶点 v_0 开始沿着由 ϖ 给出的方向对 m 执行走查, 并且散列函数 116 的输出是走查中的最终顶点的标签。

[0035] 对于其节点是超奇异椭圆曲线对质数 p 的模, 并且边是椭圆曲线之间次数为 1 的同源的扩展图, 可如下在围绕该图执行走查步骤:

[0036] 在对应于椭圆曲线 E 的节点处开始, 首先找出 $E[1]$ 的 1 扭矩的生成元 P 和 Q 。 为此:

[0037] 1. 设 n 为使得 $F_q(E[\ell]) \subseteq F_{q^n}$ 。

[0038] 2. 设 $S = \#E(F_{q^n})$; E 上的有理点 F_{q^n} 的个数 (原始)。

[0039] 3. 设 $s = S/1^k$, 其中 1^k 是整除 S 的 1 的最大幂 (注意 $k \geq 2$)。

[0040] 4. 从 $E[1]$ 中随机地选取两个点 P 和 Q :

[0041] (a) 从 $E(F_{q^n})$ 中随机地选取两个点 U, V 。

[0042] (b) 设 $P' = sU$ 且 $Q' = sV$, 如果 P' 或 Q' 等于 0, 则重复步骤 (i)。

[0043] (c) 找出最小的 i_1, i_2 , 使得 $\ell^{i_1} P' \neq O$ 且 $\ell^{i_2} Q' \neq O$, 但是 $\ell^{i_1+1} P' = O$ 且

[0044] $\ell^{i_2+1} Q' = O$ 。

[0045] (d) 设 $P = \ell^{i_1} P'$ 且 $Q = \ell^{i_2} Q'$ 。

[0046] 5. 使用公知的 Shank 的小步-大步 (Baby-steps-Giant-steps) 算法, 确定 Q 是否属于由 P 生成的群。如果是, 则重复步骤 (d)。

[0047] $1+1$ 条椭圆曲线上的 F_p^2 中与 E 同源的 j 不变式是 $j_1, \dots, j_{1+1}$ 。为找到它们:

[0048] (a) 对于 $1 \leq i \leq 1$, 设 $G_1 = \langle Q \rangle$ 且 $G_{i+1} = \langle P+(i-1)*Q \rangle$ 。

[0049] (b) 对于每一 $i, 1 \leq i \leq 1+1$, 使用 Vélu 公式计算椭圆曲线 E/G 的 j 不变式。

[0050] 如果使用例如具有 2 同源的超奇异椭圆曲线的图, 则可用以下显式方式进行随机走查: 在每一步, 在找到 E 的三个非平凡 2 扭矩点之后, 按照其 x 坐标以预先指定的方式对它们进行排序。然后, 对散列函数使用输入比特来确定要选择哪一点来对椭圆曲线求商以到达走查中的下一节点。

[0051] 散列函数几乎是均匀的证明

[0052] 按照定理, 由扩展图散列函数构造模块 112 实现的提取器函数的输出接近均匀, 并且在扩展图 120 上进行的走查非常接近随机走查。(走查是随机的仅仅意味着在图上的某一顶点 v 处, 在下一步在其任一相邻点处的可能性是相等的。) 现在, 由于图 $G(p, 1)$ 具有 n 个顶点, 并且 $m = \Omega(\log^{1+\alpha} n)$, 因此走查迅速混合并且输出顶点非常接近均匀。接着, 使得以上陈述更精确。在 n 个顶点的 d 正则图 G (例如) 上的 $O(\log n)$ 步的随机走查迅速混合的一种表述方式是

$$[0053] \quad \left\| \left(\frac{1}{d} A \right)^{O(\log n)} \cdot v - \frac{1}{n} \vec{1} \right\| \leq \varepsilon$$

[0054] 其中 ε 很小, A 是 G 的邻接矩阵, v 可被取作为任一标准单位向量, $\vec{1}$ 是向量 $(1, 1, \dots, 1)$ 。矩阵

$$[0055] \quad \frac{1}{d} A$$

[0056] 可被认为是图 120 上的均匀随机 Markov 链的转移矩阵。在此实现中, 系统 100 在图 120 上实现几乎随机的走查。这可被认为是使用矩阵 B 作为转移矩阵, 使得

$$[0057] \quad \left\| \frac{1}{d} A - B \right\| \leq \delta$$

[0058] 并且 δ 是很小的实数 (其中符号 $|||$ 表示矩阵模)。换言之, 构造模块 112 将随机走查摄动一较小的量。以下定理示出该新的随机走查在 δ 可取得足够小的时候快速混合。

[0059] 定理: 设 A 和 B 是两个子随机矩阵, 则 $||A^k - B^k|| \leq k ||A - B||$ 。

[0060] 证明: 可将差 $A^k - B^k$ 写为

$$[0061] \quad \sum_{0 \leq i \leq k-1} A^{k-i-1} (A - B) B^i$$

[0062] 对两边取模并使用 $||A|| = ||B|| = 1$ 的事实 (因为它们是子随机矩阵), 得到结果。(证明结束)。

[0063] 由于所进行的随机走查的长度是 $O(\log n)$ 。如果可将参数 δ 安排如下:

$$[0064] \quad O\left(\frac{1}{\log^2 n}\right),$$

[0065] 则所得的近似随机走查也将快速混合。这可通过将提取器的参数 ε 设为等于以

下来安排：

$$[0066] \quad O\left(\frac{1}{\log^2 n}\right).$$

[0067] 抗冲突

[0068] 在这一散列函数 116 下明确地找到冲突等效于找到相同 1 次方的一对超奇异椭圆曲线之间的两个同源。如果图 $G(p, 1)$ 没有小环, 则这一问题是非常困难的, 因为在曲线之间构造高次同源公知地是计算上的难题。

[0069] 替换实施例

[0070] 作为对上述使用图 $G(p, 1)$ 的一种替换, 系统 100 利用了 Lubotzky-Phillips-Sarnak 扩展图 120。设 l 和 p 是两个不同的质数, 其中 l 是小质数, 而 p 相当大。还假设 p 和 $l \equiv 1 \pmod{4}$ 并且 l 是 $\pmod{p}$ 的二次剩余 (这是 $l^{(p-1)/2} \equiv 1 \pmod{p}$ 的情况)。用 $X_{l,p}$ 来表示具有参数 l 和 p 的 LPS 图。接着定义构成图 $X_{l,p}$ 的顶点和边。 $X_{l,p}$ 的顶点是 $\text{PSL}(2, F_p)$ 中的矩阵, 即不可逆 2×2 矩阵, 其项 F_p 中, 行列式为 1, 以及对任何矩阵 A 的等价关系 $A = -A$ 。给定一行列式为 1 的 2×2 矩阵 A , 顶点的名称将是 A 的项或 $-A$ 的项的 4 元组, 取决于在集合 $\{0, \dots, p-1\}^4$ 的普通排序中哪一个在字典顺序上更小。接着描述构成图的边。矩阵 A 连接到矩阵 $g_i A$, 其中 g_i 是以下显式定义的矩阵。设 i 是满足 $i^2 \equiv -1 \pmod{p}$ 的整数。对等式 $g_0^2 + g_1^2 + g_2^2 + g_3^2 = 1$ 恰好有 $8(1+l)$ 个解 $g = (g_0, g_1, g_2, g_3)$ 。在这些解中只有 $1+l$ 个的 $g_0 > 0$ 且为奇数, 并且对 $j = 1, 2, 3$, g_j 是偶数。对于每一这样的 g , 关联矩阵

$$[0071] \quad \begin{pmatrix} g_0 + ig_1 & g_2 + ig_3 \\ -g_2 + ig_3 & g_0 - ig_1 \end{pmatrix}.$$

[0072] 这给出了 $\text{PSL}(2, F_p)$ 中 $1+l$ 个矩阵的集合 S 。 g_i 是此集合中的矩阵。事实是, 如果 g 在 S 中, 则 g^{-1} 也在 S 中。此外, 由于 l 很小, 因此, 该矩阵集合 S 可通过穷尽搜索非常快地找到。

[0073] 示例性过程

[0074] 图 2 示出了根据一个实施例的用于从扩展图构造散列函数的示例性过程 200。出于示例性描述的目的, 过程 200 的操作相对于图 1 的系统 100 的组件来描述。组件参考标号最左边的数字指示了该组件首次被描述的特定图。

[0075] 在框 202 处, EG HF 构造模块 112 (图 1) 将输入消息 118 划分成段。例如, 输入消息的长度为 N 。假设在 k 正则扩展图 120 中有 n 个顶点 (每一顶点具有名称 / 标签), 则从任一顶点出发的每一条边的名称将具有 $\log k$ 比特。输入消息 118 被分解成长度为 $\log k$ 的块。在框 204 处, EG HF 构造模块 112 走查作为对散列函数的输入的扩展图 120。走查如下确定: 假定在某一顶点 v 处, 走查中的下一顶点通过从输入中读取下一 $\log k$ 的块以确定从顶点 v 出发的将遍历的边来确定, 该边的另一端点将是走查的下一顶点。例如, EG HF 构造模块 112 从由输入消息 118 的前 k 个比特 (段 / 块) 指定的第一顶点开始对扩展图 120 中的边的随机走查。在扩展图 120 中走查的下一顶点由下一 $\log k$ 比特的块来指定。考虑到指定边的名称如何对应于扩展图 120 中的顶点的约定, 迭代地执行这些运算。一个示例性的这样的约定是对于每一顶点 v , 存在函数 $f_v: \{1, \dots, k\} \rightarrow E_v$ 。由此, $f_v(1)$ 是从 v 出发的第一条边, $f_v(2)$ 是从 v 出发的第二条边, 依此类推。

[0076] 在框 206 处, EG HF 构造模块 112 确定所走查的最后一个顶点的标签。在框 208

处,EG HF 构造模块 112 输出标签作为散列函数的结果。

[0077] 图 3 示出了根据一个实施例用于从扩展图构造散列函数的示例性过程。出于示例性描述的目的,过程 300 的操作相对于图 1 的系统 100 的组件来描述。在框 302 处,扩展图散列函数构造模块 (“EGHF 构造模块”)112(图 1)标识具有熵次数的消息 118。在框 304 处,EGHF 构造模块 112 向扩展图 120 中的每一顶点分配相应的标签。在框 306 处,EGHF 构造模块 112 使用提取器函数来确定输入消息 118 中的熵次数。所确定的次数被示为所提取的熵次数 122。在框 308 处,EGHF 构造模块基于所提取的熵次数 122 走查扩展图 120。在框 310 处,EGHF 构造模块 112 输出与所走查的最后一个顶点的标签以及扩展图 120 作为散列函数构造 116 的结果。即,框 302 到 310 的操作对应于散列函数构造 116 的操作。

[0078] 示例性操作环境

[0079] 图 4 示出了其中可全部或部分实现从扩展图构造散列函数的合适的计算环境的一个示例。计算性计算环境 400 仅为适用于图 1 的示例性系统以及图 2 和 3 的示例性操作的计算环境的一个示例,并非对此处所描述的系统和方法的使用范围或功能提出任何局限。也不应将计算环境 400 解释为对计算环境 400 中示出的任一组件或其组合具有任何依赖性要求。

[0080] 此处所描述的方法和系统可以使用众多其它通用或专用计算系统环境或配置来操作。适合使用的众所周知的计算系统、环境和 / 或配置的示例包括但不限于,个人计算机、服务器计算机、多处理器系统、基于微处理器的系统、网络 PC、小型机、大型机、包括任一上述系统或设备的分布式计算环境等等。该框架的紧凑或子集形式也可以在诸如手持式计算机或其它计算设备等有限资源的客户机中实现。本发明在其中任务由通过通信网络链接的远程处理设备来执行的分布式计算环境中实践。在分布式计算环境中,程序模块可以位于本地和远程存储器存储设备中。

[0081] 参考图 4,用于从扩展图构造散列函数的示例性系统包括实现例如图 1 的系统 100 的计算机 410 形式的通用计算设备。以下描述的计算机 410 的各方面是图 1 的计算设备 102 的示例性实现。计算机 410 的组件可包括但不限于,处理单元 420、系统存储器 430 以及将包括系统存储器的各类系统组件耦合至处理单元 420 的系统总线 421。系统总线 421 可以是若干种总线结构的任一种,包括存储器总线或存储器控制器、外围总线以及使用各类总线体系结构的任一种的局部总线。作为示例而非局限,这类体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强型 ISA (EISA) 总线、视频电子技术标准协会 (VESA) 局部总线、外围部件互连 (PCI) 总线 (也称为小背板 (Mezzanine) 总线)。

[0082] 计算机 410 通常包括各种计算机可读介质。计算机可读介质可以是可由计算机 410 访问的任一可用介质,包括易失性和非易失性介质、可移动和不可移动介质。作为示例而非局限,计算机可读介质包括计算机存储介质和通信介质。计算机存储介质包括以用于储存诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任一方法或技术实现的易失性和非易失性,可移动和不可移动介质。计算机存储介质包括但不限于, RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘 (DVD) 或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存所期望的信息并可由计算机 410 访问的任一其它介质。

[0083] 通信介质通常以诸如载波或其它传输机制等已调制数据信号来体现计算机可读

指令、数据结构、程序模块或其它数据,并包括任一信息传送介质。术语“已调制数据信号”指以对信号中的信息进行编码的方式设置或改变其一个或多个特征的信号。作为示例而非局限,通信介质包括有线介质,如有线网络或直接连线连接,以及无线介质,如声学、RF、红外和其它无线介质。上述任一的组合也应当包括在计算机可读介质的范围之内。

[0084] 系统存储器 430 包括易失性和 / 或非易失性存储器形式的计算机存储介质,如只读存储器 (ROM) 431 和随机存取存储器 (RAM) 432。基本输入 / 输出系统 433 (BIOS) 包括如在启动时帮助在计算机 410 内的元件之间传输信息的基本例程,它通常储存在 ROM 431 中。RAM 432 通常包含处理单元 420 立即可访问和 / 或当前正在操作的数据和 / 或程序模块。作为示例而非局限,图 4 示出了操作系统 434、应用程序 435、其它程序模块 436 和程序数据 437。

[0085] 计算机 410 也可包括其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质。仅作为示例,图 4 示出了对不可移动、非易失性磁介质进行读写的硬盘驱动器 441,对可移动、非易失性磁盘 432 进行读写的磁盘驱动器 431,以及对可移动、非易失性光盘 436,如 CD ROM 或其它光介质进行读写的光盘驱动器 433。可以在示例性操作环境中使用的其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质包括但不限于,磁带盒、闪存卡、数字多功能盘、数字录像带、固态 RAM、固态 ROM 等等。硬盘驱动器 441 通常通过不可移动存储器接口,如接口 440 连接到系统总线 421,磁盘驱动器 431 和光盘驱动器 433 通常通过可移动存储器接口,如接口 430 连接到系统总线 421。

[0086] 上文讨论并在图 4 示出的驱动器及其关联的计算机存储介质为计算机 410 提供了计算机可读指令、数据结构、程序模块和其它数据的存储。例如,在图 4 中,示出硬盘驱动器 441 储存操作系统 444、应用程序 443、其它程序模块 446 和程序数据 447。注意,这些组件可以与操作系统 434、应用程序 433、其它程序模块 436 和程序数据 437 相同,也可以与它们不同。应用程序 433 包括例如图 1 的计算设备 102 的程序模块 108。程序数据 437 包括例如图 1 的计算设备 102 的程序数据 110。这里对操作系统 444、应用程序 443、其它程序模块 446 和程序数据 447 给予不同的标号来说明至少它们是不同的副本。

[0087] 用户可以通过输入设备,如键盘 462 和定位设备 461 (通常指鼠标、跟踪球或触摸垫) 向计算机 410 输入命令和信息。其它输入设备 (未示出) 可包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通常通过耦合至系统总线 421 的用户输入接口 460 连接至处理单元 420,但是也可以通过其它接口和总线结构连接,如并行端口、游戏端口或通用串行总线 (USB)。

[0088] 监视器 491 或其它类型的显示设备也通过接口,如视频接口 490 连接至系统总线 421。除监视器之外,计算机也可包括其它外围输出设备,如打印机 496 和音频设备 497,它们通过输出外围接口 493 连接。

[0089] 计算机 410 可以使用到一个或多个远程计算机,如远程计算机 480 的逻辑连接在网络化环境中操作。在一个实现中,远程计算机 480 表示图 1 的计算设备 102 或联网计算机 104。远程计算机 480 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它常见的网络节点,并根据其具体实现,可以包括许多或所有相对于计算机 410 所描述的元件,尽管在图 4 中仅示出了存储器存储设备 481。图 4 描述的逻辑连接包括局域网 (LAN) 471 和广域网 (WAN) 473,但也可包括其它网络。这类网络环境常见于办公室、企业范围计算机网络、

内联网以及因特网。

[0090] 当在 LAN 网络环境中使用时,计算机 410 通过网络接口或适配器 470 连接至 LAN 471。当在 WAN 网络环境中使用时,计算机 410 通常包括调制解调器 472 或用于通过 WAN 473,如因特网建立通信的其它装置。调制解调器 472 可以是内置或外置的,它通过用户输入接口 460 或其它适当的机制连接至系统总线 421。在网络化环境中,相对于计算机 410 所描述的程序模块或其部分可储存在远程存储器存储设备中。作为示例而非局限,图 4 示出远程应用程序 483 驻留在存储器设备 481 上。可以理解,示出的网络连接是示例性的,也可以使用在计算机之间建立通信链路的其它手段。

[0091] 结论

[0092] 尽管以对结构特征和 / 或方法操作或动作专用的语言描述了用于从扩展图构造散列函数的系统和方法,但是可以理解,所附权利要求书中定义的实现不一定限于所描述的具体特征或动作。相反,系统 100 的具体特征和操作是作为实现所要求保护的主题的示例性形式而公开的。

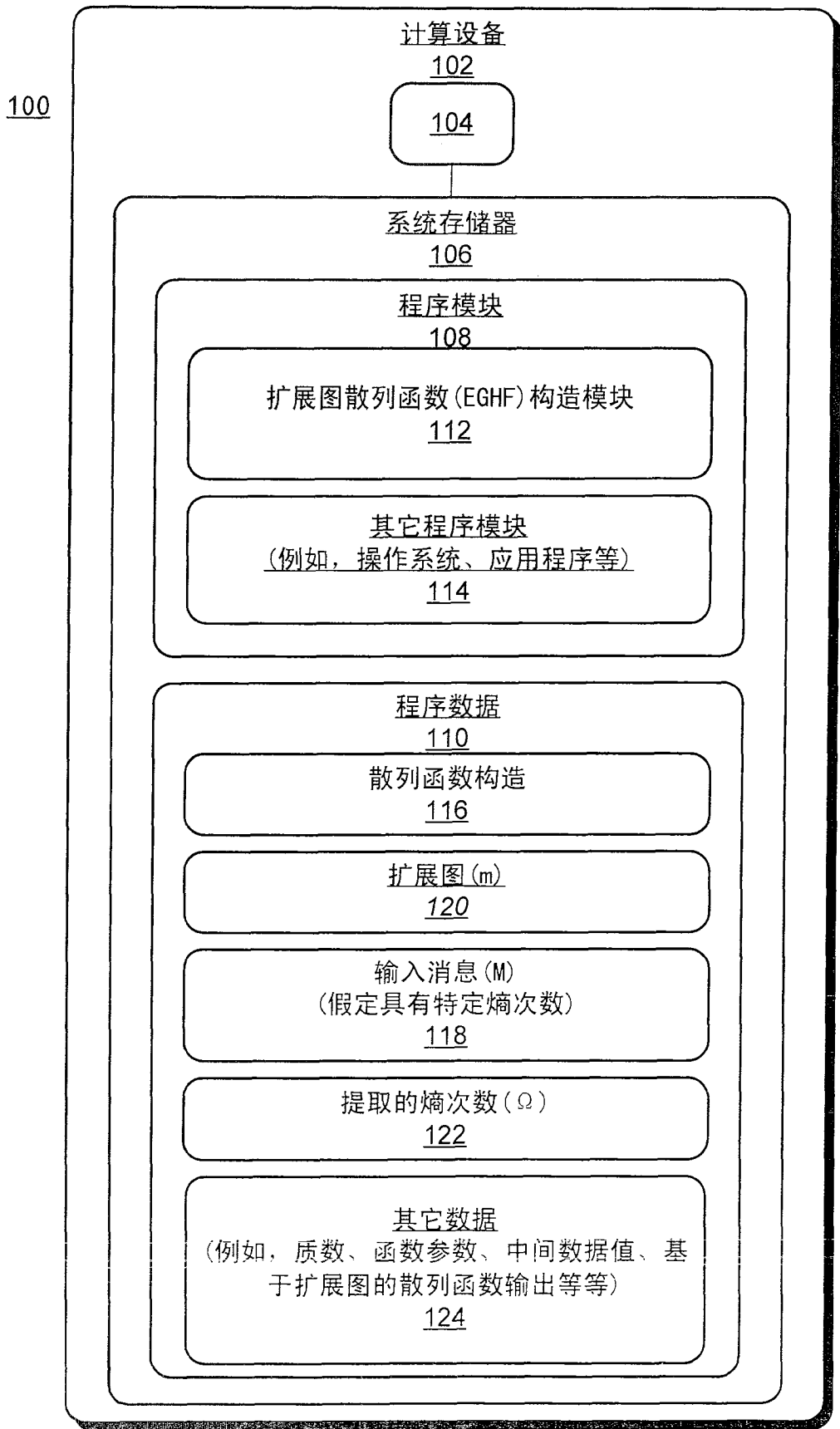


图 1

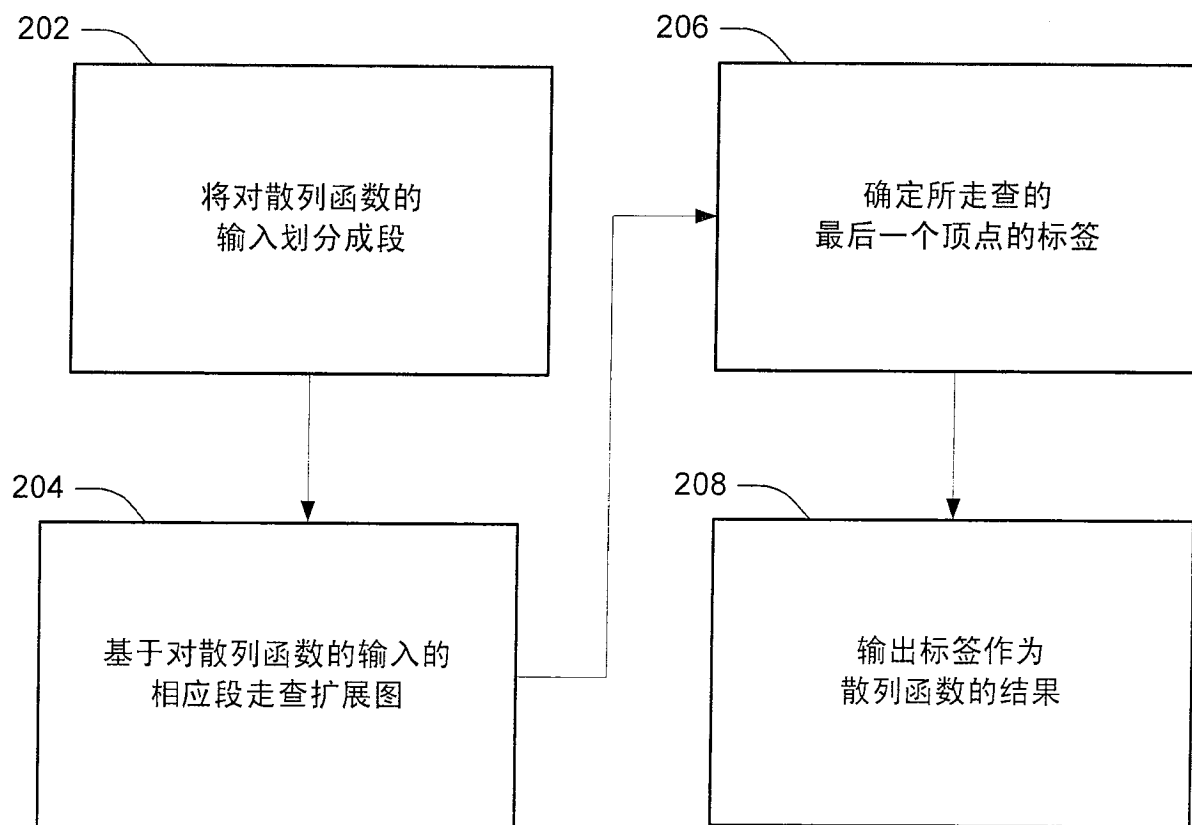
200

图 2

300

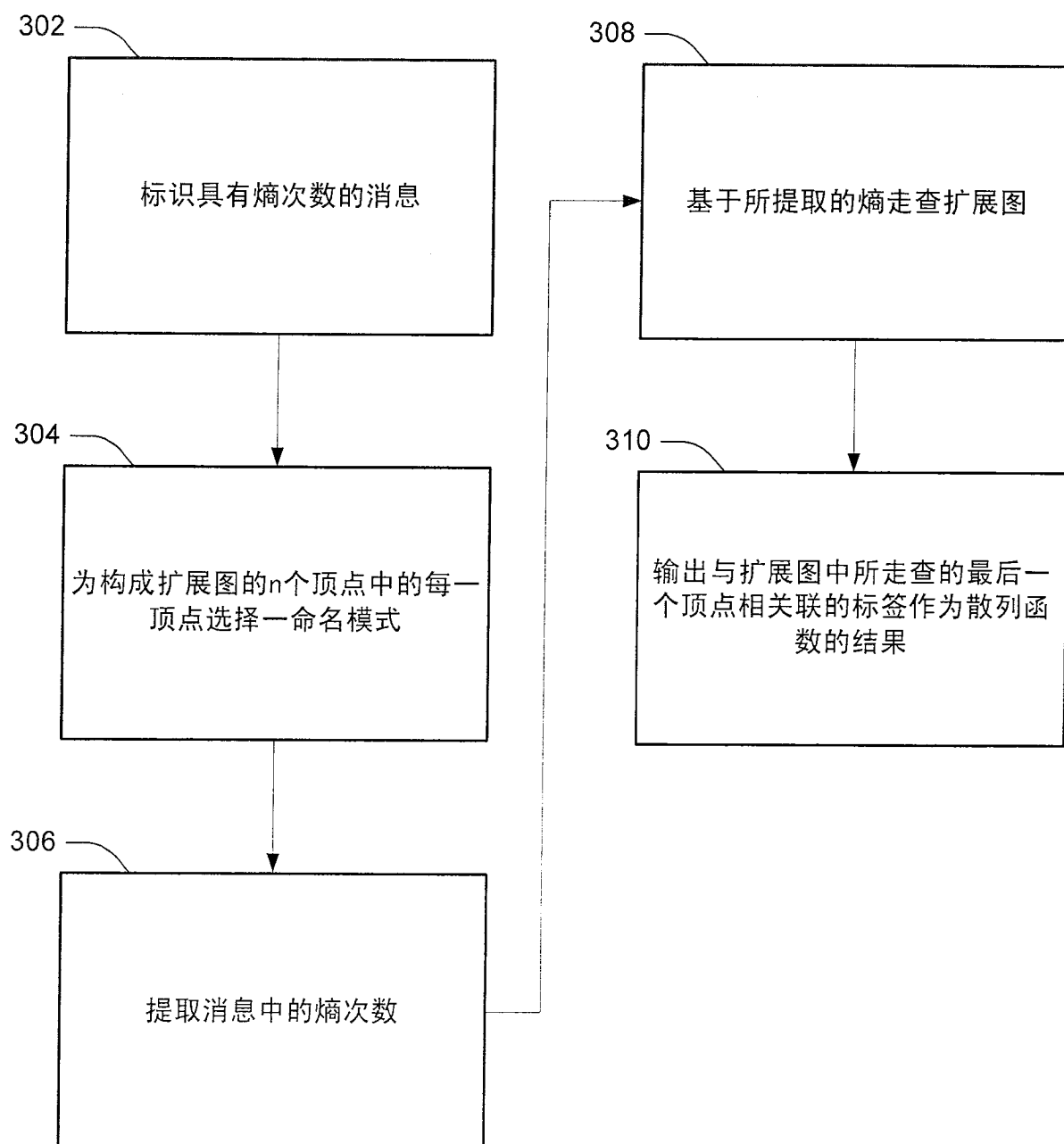


图 3

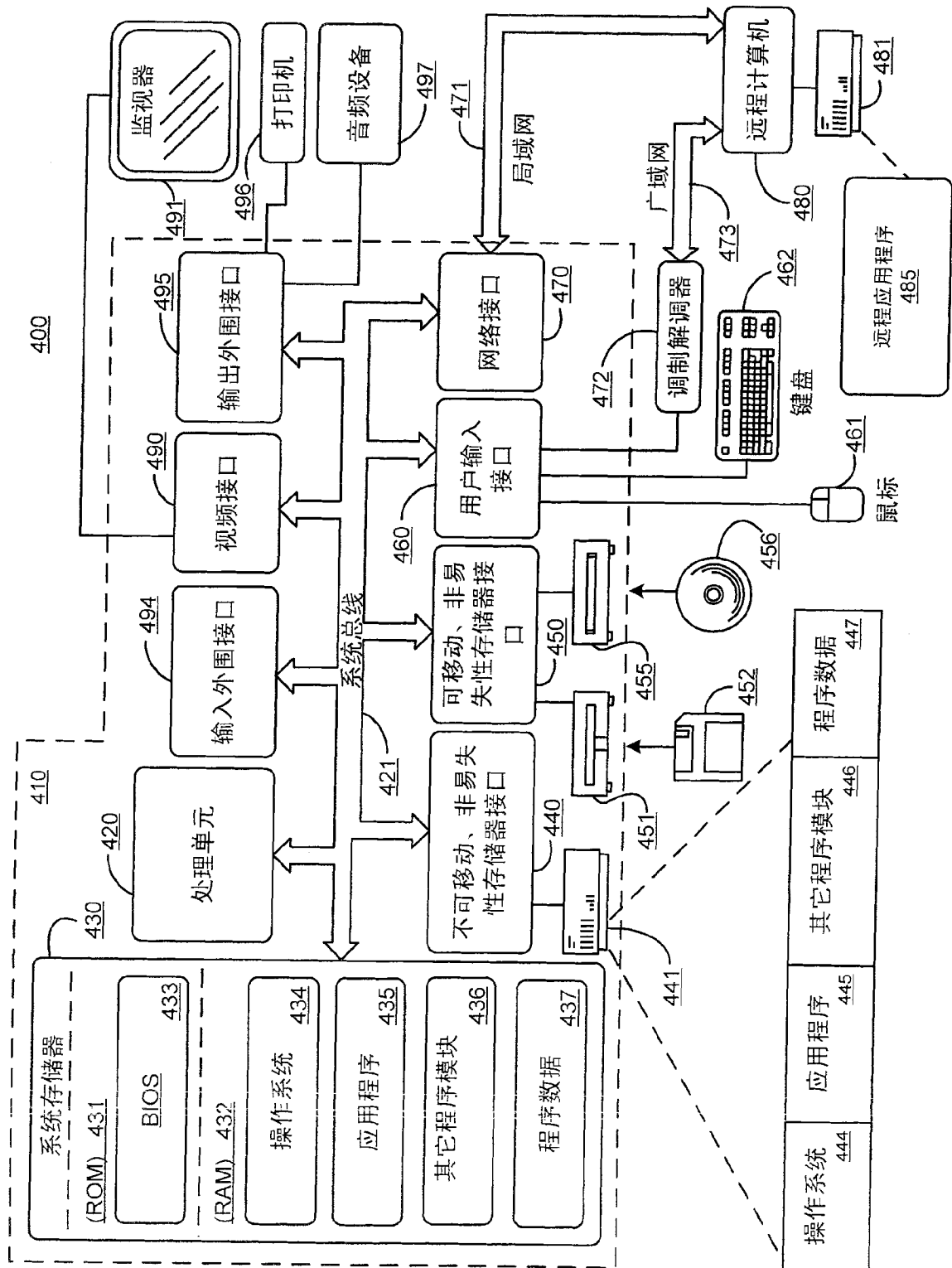


图 4