(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102422169 B
(45)授权公告日 2014.11.12

(21)申请号 201080020725.7
(22)申请日 2010.05.07
(30)优先权数据
12/463,984 2009.05.11 US
(85)PCT国际申请进入国家阶段日
2011.11.11
(86)PCT国际申请的申请数据
PCT/US2010/034110 2010.05.07
(87)PCT国际申请的公布数据
WO2010/132308 EN 2010.11.18
(73)专利权人 英派尔科技开发有限公司
地址 美国特拉华州
(72)发明人 米奥德拉格·波特科尼亚克
(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 吕俊刚
(51)Int.Cl.
*G06F 21/76*(2013.01)
*G06F 17/12*(2006.01)
(56)对比文件
CN 1486506 A,2004.03.31,
US 2004/0181303 A1,2004.09.16,
CN 1346473 A,2002.04.24,
US 2006/0253664 A1,2006.11.09,
审查员 徐辉

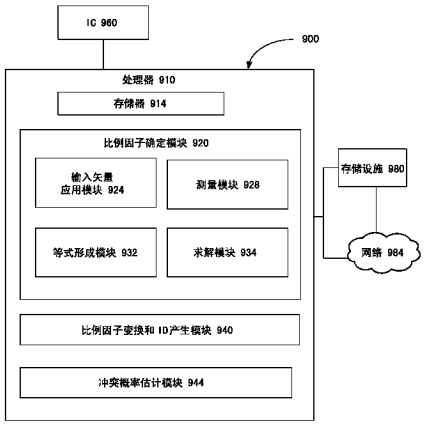
权利要求书4页 说明书20页 附图9页

(54)发明名称

集成电路的标识

(57)摘要

一般地描述了针对集成电路(IC)产生标识号的技术。在一些示例中,用于产生IC的标识的方法可以包括:选择IC的电路元件;估计针对所选电路元件的IC的属性的测量,其中各个测量与先前应用于IC的相应输入矢量相关联;对至少部分地基于针对所选电路元件的IC的属性所获取的测量而形成的多个等式进行求解,以确定所选电路元件的比例因子;以及对针对所选电路元件的比例因子进行变换,以产生IC的标识号。还公开了其它变体和实施例。




CN 102422169 B

1. 一种使计算设备产生包括电路元件的集成电路 IC 的标识号的方法，所述方法包括：

选择 IC 的电路元件；

针对所选电路元件估计 IC 属性的测量结果，其中各个测量结果与先前应用于 IC 的对应输入矢量相关联；

对至少部分地基于针对所选电路元件所获取的 IC 属性的测量结果而形成的多个等式进行求解，以确定针对所选电路元件的比例因子，其中，电路元件的属性的比例因子为所述电路元件中属性的实际值与属性的标称值之比；以及

对针对所选电路元件而确定的比例因子进行变换，以产生 IC 的标识号。

2. 根据权利要求 1 所述的方法，其中对多个等式进行求解包括：对还基于针对所选电路元件的 IC 的另一属性的其它测量结果而形成的多个等式进行求解。

3. 根据权利要求 2 所述的方法，其中所述属性和另一属性包括下述两个：漏电流、延迟、切换功率、寄生电容、电感、电阻、增益、偏置电压、阈值电压、工作温度、功耗或空闲电流。

4. 根据权利要求 1 所述的方法，其中对多个等式进行求解包括：至少部分地基于测量结果中的误差，对包括对应误差项的多个等式进行求解。

5. 根据权利要求 4 所述的方法，其中对多个等式进行求解包括：

用公式表示最优化问题，该最优化问题包括减小多个等式的误差项的范数的目标函数。

6. 根据权利要求 1 所述的方法，其中对所确定的比例因子进行变换包括：

选择比例因子中的一个或多个；

将一个或多个所选择的比例因子映射到对应的二进制码；以及

使用针对所选择的比例因子而映射的二进制码，产生 IC 的标识号。

7. 根据权利要求 1 所述的方法，其中所述变换包括：

产生比例因子的概率分布函数 PDF；

将 PDF 之下的区域分为单独的部分，使得单独的部分中的每一个具有大致相等的面积；

将二进制码分配给单独的部分，使得每个单独的部分与相应的二进制码相关联；

基于分配给单独的部分的二进制码，将二进制码分配给单独的部分中包括的单独的比例因子；以及

使用分配给单独的比例因子的二进制码，产生 IC 的标识号。

8. 根据权利要求 1 所述的方法，还包括：

对产生的标识号的冲突概率进行估计。

9. 根据权利要求 8 所述的方法，其中选择所述电路元件还包括：选择第一多个电路元件，其中所产生的标识号是第一标识号，所述方法还包括：

确定所述冲突概率高于阈值冲突概率；

基于确定所述冲突概率高于阈值冲突概率来选择第二多个电路元件，其中所述第二多个电路元件包括与第一多个电路元件相比更多的电路元件；以及

产生 IC 的第二标识号，使得所述第二标识号具有比所述第一标识号相对低的冲突概率。

10. 一种使计算设备产生包括电路元件的集成电路 IC 的标识号的方法，所述方法包括：

启动将输入矢量应用于包括在 IC 中的电路元件中的一个或多个；

响应于输入矢量的应用，接收测量值，其中所述测量值与响应于输入矢量的应用、针对所述一个或多个电路元件的一个或多个属性而测量的值相对应；

基于对应的测量值来形成多个等式，其中所述多个等式中的每一个包括对应的一个或多个电路元件的一个或多个比例因子，其中，所述一个或多个电路元件的属性的比例因子为所述一个或多个电路元件中属性的实际值与属性的标称值之比；

对所述多个等式进行求解，以确定对应的一个或多个电路元件的一个或多个比例因子；以及

对所确定的一个或多个比例因子进行变换，以产生 IC 的标识号。

11. 根据权利要求 10 所述的方法，其中一个或多个属性中的每一个包括以下之一：漏电流、延迟、切换功率、寄生电容、电感、电阻、增益、偏置电压、阈值电压、工作温度、功耗或空闲电流。

12. 根据权利要求 10 所述的方法，其中对多个等式进行求解包括：对包括与一个或多个电路元件相对应的一个或多个项的等式进行求解，其中一个或多个项中的每一个包括：对应的电路元件的属性的标称值和对应的电路元件的比例因子。

13. 根据权利要求 10 所述的方法，其中对多个等式进行求解包括：至少部分地基于对应测量值中的误差，对还包括对应误差项的等式进行求解。

14. 根据权利要求 13 所述的方法，还包括：

用公式表示最优化问题，该最优化问题包括减小各个等式的误差项的范数的目标函数。

15. 根据权利要求 14 所述的方法，还包括：

使用线性规划、逐条线性规划、非线性规划、二次规划、或凸规划来对最优化问题进行求解。

16. 根据权利要求 10 所述的方法，还包括：将电路元件中的一个或多个标识为多义电路元件，其中形成多个等式还包括：形成多个等式，使得从多个等式中的各个等式排除多义电路元件中的一个或多个。

17. 根据权利要求 10 所述的方法，还包括：

引起 IC 的工作条件的改变，以降低测量值所需的精度。

18. 根据权利要求 10 所述的方法，其中对所确定的一个或多个比例因子进行变换包括：

选择比例因子中的一个或多个；

将一个或多个所选择的比例因子映射到对应的二进制码；以及

使用所述二进制码，产生 IC 的标识号。

19. 根据权利要求 18 所述的方法，还包括：

标识与已经选择了比例因子的一个或多个电路元件相对应的指示符字符串中的一个或多个比特；以及

将所标识的一个或多个比特设置为 1，使得所述指示符字符串指示其比例因子已经被

使用的电路元件产生 IC 的标识号。

20. 根据权利要求 18 所述的方法，其中选择比例因子中的一个或多个还包括：

产生比例因子的概率分布函数 PDF；

将 PDF 之下的区域分为单独的部分；

将单独的部分分为第一集合的部分和第二集合的部分，使得第一集合的部分中的单独的部分和第二集合的部分中的单独的部分是交错的；以及

选择处于第一集合的部分中的一个或多个比例因子。

21. 根据权利要求 20 所述的方法，其中所述映射包括：

将二进制码分配给第一集合的部分中的单独的部分，使得第一集合的部分中的每个单独的部分与相应的二进制码相关联；以及

基于分配给单独的部分的二进制码，将二进制码分配给第一集合的部分中的单独的部分中包括的比例因子。

22. 根据权利要求 10 所述的方法，其中对所确定的一个或多个比例因子进行变换包括：

产生比例因子的概率分布函数 PDF；

将 PDF 之下的区域分为单独的部分，每一个部分具有大致相等的面积；

将二进制码分配给单独的部分，使得每个单独的部分与相应的二进制码相关联；

基于分配给单独的部分的二进制码，将二进制码分配给单独的部分中包括的比例因子；以及

使用分配给比例因子的二进制码，产生 IC 的标识号。

23. 根据权利要求 10 所述的方法，还包括：

响应于确定一个或多个比例因子和 / 或产生 IC 的标识号，对 IC 进行认证。

24. 根据权利要求 23 所述的方法，其中对 IC 进行认证包括：

通过启动将一个或多个输入矢量应用于 IC 中包括的电路元件中的一个或多个，询问 IC 的标识；

响应于所述询问，接收响应值，其中所述响应值包括一个或多个电路元件的一个或多个操作特性的指示；

将接收到的响应值与存储在 IC 外部的数据库中的响应值进行比较；以及

至少部分地基于所述比较来对 IC 进行认证。

25. 根据权利要求 23 所述的方法，还包括：

至少部分地基于对 IC 进行认证，许可 IC 或 IC 的用户对一个或多个服务或设备的访问或操作权。

26. 根据权利要求 10 所述的方法，还包括：

确定向 IC 的一个或多个电路元件的数据分配的调度，使得 IC 的总漏电流、温度、寄生电容或老化速度降低。

27. 根据权利要求 10 所述的方法，还包括：

至少部分地基于所确定的一个或多个电路元件的一个或多个比例因子，针对在持续时段内要在 IC 上执行的任务，确定 IC 的工作电压，使得 IC 的总漏电流、温度、寄生电容或老化速度降低。

28. 一种被设置为确定包括电路元件的集成电路 IC 的标识号的设备，所述设备包括：

用于启动将输入矢量应用于包括在 IC 中的电路元件中的一个或多个的装置；

用于响应于输入矢量的应用接收测量值的装置，其中所述测量值与响应于输入矢量的应用、针对所述一个或多个电路元件的一个或多个属性所测量的值相对应；

用于基于相应的测量值来形成多个等式的装置，其中所述多个等式中的每一个包括对应的一个或多个电路元件的一个或多个比例因子，其中，所述一个或多个电路元件的属性的比例因子为所述一个或多个电路元件中属性的实际值与属性的标称值之比；

用于对所述多个等式进行求解以确定对应的一个或多个电路元件的一个或多个比例因子的装置；以及

用于对所确定的一个或多个比例因子进行变换以产生 IC 的标识号的装置。

29. 根据权利要求 28 所述的设备，其中用于对所确定的一个或多个比例因子进行变换以产生 IC 的标识号的装置包括：

用于选择比例因子中的一个或多个的装置；

用于将一个或多个所选择的比例因子映射到对应的二进制码的装置；以及

用于使用所述二进制码产生 IC 的标识号的装置。

# 集成电路的标识

## 技术领域

[0001] 本申请一般涉及集成电路领域，更具体地，涉及集成电路的标识。

## 背景技术

[0002] 集成电路 (IC) 已经广泛地用于大量电子设备。在一些应用中，集成电路的标识和认证是有用的，例如，出于安全性目的。传统的标识和认证技术需要在 IC 中包括附加电路、非易失性存储器和 / 或固件，这并不总是可行的。

## 发明内容

[0003] 通常，本公开的实施例提出了与集成电路的标识相关联的各种方法、设备、存储介质和 / 或系统。在各个实施例中，使计算设备产生包括电路元件的集成电路 (IC) 的标识号的方法可以包括 :选择 IC 的电路元件，以及针对所选电路元件估计 IC 的属性的测量结果。各个测量结果可以与先前应用于 IC 的对应输入矢量相关联。该方法还可以包括 :对至少部分地基于针对所选电路元件的所获取的 IC 属性的测量结果而形成的多个等式进行求解，以确定所选电路元件的比例因子，以及对针对所选电路元件确定的比例因子进行变换，以产生 IC 的标识号。

[0004] 在各个实施例中，对多个等式进行求解可以包括 :对还基于针对所选电路元件的 IC 的另一属性的其它测量结果而形成的多个等式进行求解。该属性和该另一属性可以包括漏电流、延迟、切换功率、寄生电容、电感、电阻、增益、偏置电压、阈值电压、工作温度、功耗或空闲电流中的两个。在各个实施例中，对多个等式进行求解可以包括 :至少部分地基于测量结果中的误差，对还包括对应的误差项的多个等式进行求解。此外，对多个等式进行求解还可以包括 :用公式表示包括减小多个等式的误差项的范数 (norm) 的目标函数的最优化问题。

[0005] 在各个实施例中，对所确定的比例因子进行变换还可以包括 :选择比例因子中的一个或多个，将一个或多个所选比例因子映射到对应的二进制码，以及使用针对所选比例因子的所映射的二进制码，产生 IC 的标识号。在各个实施例中，该变换可以包括 :产生比例因子的概率分布函数 (PDF)，将 PDF 之下的区域分为单独 (individual) 的部分，使得单独的部分中的每一个具有大致相等的面积，将二进制码分配给单独的部分，使得每个单独的部分与相应的二进制码相关联，基于分配给单独的部分的二进制码，将二进制码分配给单独的部分中包括的单独的比例因子，以及使用分配给单独的比例因子的二进制码，产生 IC 的标识号。

[0006] 在各个实施例中，该方法还可以包括 :对所产生的标识的冲突概率进行估计。此外，选择电路元件还可以包括 :选择第一数量的电路元件。所产生的标识号可以是第一标识号。该方法还可以包括 :确定冲突概率高于阈值冲突概率，基于确定冲突概率较高来选择第二数量的电路元件，以及产生 IC 的第二标识号，使得第二标识号具有比第一标识号相对低的冲突概率。第二数量的电路元件可以包括比第一数量的电路元件更多的电路元件。

[0007] 在各个实施例中，使计算设备产生包括电路元件的集成电路 (IC) 的标识号的方法可以包括：启动将输入矢量应用于包括在 IC 中的电路元件中的一个或多个，以及响应于输入矢量的应用而接收测量值。该测量值可以与响应于输入矢量的应用的、针对所述一个或多个电路元件的一个或多个属性所测量的值相对应。该方法还可以包括：基于对应的测量值来形成多个等式，对所述多个等式进行求解以确定对应的一个或多个电路元件的一个或多个比例因子，以及对所确定的一个或多个比例因子进行变换以产生 IC 的标识号。所述多个等式中的每一个可以包括对应的一个或多个电路元件的一个或多个比例因子。

[0008] 在各个实施例中，一个或多个属性中的每一个可以包括：漏电流、延迟、切换功率、寄生电容、电感、电阻、增益、偏置电压、阈值电压、工作温度、功耗或空闲电流之一。此外，对多个等式进行求解可以包括：对包括与一个或多个电路元件相对应的一个或多个项的等式进行求解。一个或多个项中的每一个包括：对应的电路元件的属性的标称值和对应的电路元件的比例因子。此外，对多个等式进行求解可以包括：至少部分地基于对应测量值中的误差，对还包括对应误差项的等式进行求解。对于这些实施例，该方法还可以包括：用公式表示包括减小多个等式的误差项的范数的目标函数的最优化问题，和 / 或使用线性规划、逐条线性规划、非线性规划、二次规划、或凸规划来对最优化问题进行求解。

[0009] 在各个实施例中，该方法还可以包括：将电路元件中的一个或多个标识为多义 (ambiguous) 电路元件。形成多个等式还可以包括：形成多个等式，使得从多个等式中的单独等式中排除多义电路元件中的一个或多个。该方法还可以包括：引起 IC 的工作条件的改变，以降低测量值所需的精度。

[0010] 在各个实施例中，对所确定的一个或多个比例因子进行变换还可以包括：选择比例因子中的一个或多个，将一个或多个所选比例因子映射到对应的二进制码，以及使用所述二进制码产生 IC 的标识号。该方法还可以包括：标识与已经选择了比例因子的一个或多个电路元件相对应的指示符字符串中的一个或多个比特，将所标识的一个或多个比特设置为 1，使得所述指示符字符串指示其比例因子已经用于产生 IC 的标识号的电路元件。选择比例因子中的一个或多个还可以包括：产生比例因子的概率分布函数 (PDF)，将 PDF 之下的区域分为单独的部分，将单独的部分分为第一集合的部分和第二集合的部分，使得第一集合的部分中的单独的部分和第二集合的部分中的单独的部分是交错的 (interleaved)，以及选择处于第一集合的部分中的一个或多个比例因子。映射可以包括：将二进制码分配给第一集合的部分中的单独的部分，使得第一集合的部分中的每个单独的部分与相应的二进制码相关联，并基于分配给单独的部分的二进制码，将二进制码分配给第一集合的部分中的单独的部分中包括的比例因子。

[0011] 在各个实施例中，对所确定的一个或多个比例因子进行变换还可以包括：产生比例因子的概率分布函数 (PDF)，将 PDF 之下的区域分为单独的部分，每一个部分具有大致相等的面积，将二进制码分配给单独的部分，使得每个单独的部分与相应的二进制码相关联，基于分配给单独的部分的二进制码，将二进制码分配给单独的部分中包括的比例因子，以及使用分配给比例因子的二进制码产生 IC 的标识号。

[0012] 在各个实施例中，该方法还包括：响应于确定一个或多个比例因子和 / 或产生 IC 的标识号，对 IC 进行认证。对 IC 进行认证还可以包括：通过启动将一个或多个输入矢量应用于 IC 中包括的电路元件中的一个或多个，询问 (challenge) IC 的标识；响应于所述询问，

接收响应值；将接收到的响应值与存储在 IC 外部的数据库中的响应值进行比较；以及至少部分地基于所述比较来对 IC 进行认证。响应值可以包括一个或多个电路元件的一个或多个操作特性的指示。该方法还可以包括：至少部分地基于对 IC 的认证，许可 IC 或 IC 的用户对一个或多个服务或设备的访问或操作权。

[0013] 在各个实施例中，该方法还可以包括：确定向 IC 的一个或多个电路元件的数据分配的调度，使得总漏电流、温度、寄生电容或 IC 老化速度降低。在各个实施例中，该方法还可以包括：至少部分地基于所确定的一个或多个电路元件的比例因子，针对在持续时段内要在 IC 上执行的任务，确定 IC 的工作电压，使得总漏电流、温度、寄生电容或 IC 老化速度降低。

[0014] 在各个实施例中，一种设备可以包括：处理器，以及具有编程指令的存储介质，被配置为：响应于处理器执行指令，使所述设备执行先前描述的方法的一些或所有方面。在各个实施例中，计算机可读存储介质可以具有所述编程指令。

[0015] 以上发明内容只是示意性的，并不是限制性的。除了上述示意性的方面、实施例和特征之外，其它方面、实施例和特征将通过参照附图和以下详细实施例也会变得明显。

## 附图说明

[0016] 在说明书的结尾部分特别指出并清楚地表明了本发明的主旨。结合附图，本公开的前述和其它特征将从以下描述和所附权利要求中变得更加明显。应当理解，这些附图仅描述了根据本公开的若干实施例，并不意在限定其范围，将通过使用附图，以额外的明确性和细节描述本公开。将参照附图来描述各个实施例，其中类似的参考符号表示类似的元件，其中：

[0017] 图 1 示出了用于产生 IC 的标识号 (ID) 的方法；

[0018] 图 2a 示出了被配置为至少部分地基于示例电路元件 -- 标称大小的与非门 -- 的输入而存储该示例电路元件的示例标称漏电流的示例表格；

[0019] 图 2b 示出了可以适合于实践各个实施例的示例 IC 的一部分；

[0020] 图 2c 示出了被配置为存储针对两个示例 IC 的多个与非门的比例因子的示例表格；

[0021] 图 2d 示出了被配置为针对各种输入矢量，存储两个示例 IC 的一个或多个电路元件中的总漏电流的示例表格；

[0022] 图 3a 示出了可以适合于实践各个实施例的示例 IC 的一部分；

[0023] 图 3b 示出了被配置为存储与非门和或非门的示例标称漏电流对比各个门的输入的示例表格；

[0024] 图 4 示出了用于确定 IC 的相应多个电路元件的多个比例因子的方法；

[0025] 图 5 示出了 IC 的示例比例因子的概率分布函数 (PDF)；

[0026] 图 6a 示出了用于以二进制形式对多个比例因子进行编码的恒定裕度 (margin) 编码技术；

[0027] 图 6b 示出了用于至少部分地基于 IC 的对应多个电路元件的所确定的多个比例因子来产生 IC 的标识 (ID) 的方法；

[0028] 图 7a 示出了用于以二进制形式对多个比例因子进行编码的等面积编码技术；

[0029] 图 7b 示出了用于至少部分地基于 IC 的对应多个电路元件的所确定的多个比例因子来产生 IC 的 ID 的方法；

[0030] 图 8 示出了阐明 IC 的 ID 的冲突概率的示例图；

[0031] 图 9 示出了可以适合于实践各个实施例的示例计算系统；以及

[0032] 图 10 示出了根据各个实施例的示例计算程序产品，全部按照本公开的至少一些实施例进行设置。

## 具体实施方式

[0033] 以下描述提供了各种示例和特定细节，以提供对所要求保护的主旨的全面理解。然而，本领域技术人员将会理解，可以不按照这里所公开的特定细节中的一些或更多来实践所要求保护的主旨。此外，在一些环境下，并未详细描述公知的方法、过程、系统、组件和 / 或电路，以避免不必要地使所要求保护的主旨变得不清楚。在以下具体实施方式中，参照作为其中一部分的附图。在附图中，除非上下文另有指明，否则类似的符号典型地标识类似的组件。在具体实施方式、附图和权利要求中描述的示例性实施例并不起限定作用。可以使用其它实施例，并且可以在不偏离这里所呈现的主旨的精神或范围的情况下做出其它改变。将易于理解，可以以各种不同配置来设置、替换、组合和设计这里所通常描述的并在附图中示出的本公开的各方面，可以明确地设想到所有这些，并且将其作为本公开的一部分。

[0034] 在以下描述中，可以出现针对在计算系统（如计算机和 / 或计算系统存储器）内存储的数据比特和 / 或二进制数字信号的操作的算法和 / 或符号表示。算法通常被认为是导致期望结果的前后一致的操作序列和 / 或类似处理，其中，该操作可以涉及针对采用能够被存储、传递、组合、比较和 / 或操作的电、磁和 / 或电磁信号形式的物理量的物理操作。在各种上下文中，这种信号可以被称为比特、数据、值、要素、符号、字符、项、数、数字等。然而，本领域技术人员将会认识到，这种术语可以用于表示物理量。因而，当在说明书中使用诸如“存储”、“处理”、“检索”、“计算”、“确定”等术语时，它们可以指计算平台（如，计算机或诸如蜂窝电话之类的类似电子计算设备）的动作 / 操作 / 功能，用于对计算平台的处理器、存储器、寄存器等内的表示为物理量（包括电和 / 或磁物理量）的数据进行操作和 / 或变换。

[0035] 本公开尤其涉及与 IC 的标识相关的方法、设备、系统和计算机程序产品。

[0036] 产生 IC 的标识号

[0037] 图 1 示出了根据本公开的各个实施例的、用于产生包括一个或多个电路元件的 IC 的 ID 号的方法 100。针对所示出的实施例，方法 100 可以包括块 102、104、106 和 / 或 108。

[0038] 在块 102，方法 100 可以包括选择 IC 的电路元件。作为示例，IC 可以具有多个电路元件、数字逻辑门、触发器、晶体管、电阻器、电容器、电感器、比较器、放大器等，可以在块 102 处对其中的一个或多个进行选择。

[0039] 处理可以从块 102 继续至块 104。在块 104，方法 100 可以包括对所选电路元件的 IC 的属性的测量结果进行估计，其中单独的测量结果与先前应用于 IC 的对应的输入矢量相关联。作为示例，可以将一个或多个输入矢量应用于所选电路元件中的一个或多个，而且可以获得并估计对应的属性测量结果。

[0040] 处理可以从块 104 继续至块 106。在块 106，方法 100 可以包括对至少部分地基于

针对所选电路元件所获得的 IC 的属性测量结果而形成的多个等式进行求解，以确定所选电路元件的比例因子。

[0041] 处理可以从块 106 继续至块 108。在块 108，方法 100 可以包括对所选电路元件的所确定的比例因子进行变换，以产生 IC 的标识号。方法 100 可以在块 108 之后结束。

[0042] 即使在过去的几十年中极大地发展了集成电路的制造过程，在这种制造过程期间也会出现固有的变化。由于这种制造变化和 / 或各种其它原因（例如，所利用的制造过程类型等），两个不同 IC 中的两个类似电路元件（例如，数字逻辑门、触发器、晶体管、电阻器、电容器、电感器、比较器、放大器等中的一个或多个类型）在一个或多个属性（例如，漏电流、延迟、切换功率、工作温度、寄生电容、偏移电压、增益等）中会有变化。例如，基本类似大小并具有类似输入、且包括在两个不同的 IC 中的两个与非门可以具有不同的漏电流量。类似地，相同 IC 中的两个类似电路元件在一个或多个属性（例如，电容、电感、电阻、增益、偏移电压、阈值电压、工作温度、功耗、空闲电流、漏电流等）中会有变化。

[0043] 因而，在各个实施例中，IC 的一个或多个电路元件的制造变化性可以用于标识和认证 IC，这将在之后详细讨论。

[0044] 图 2a 示出了根据各个实施例的、被配置为存储至少部分地基于示例电路元件 -- 标称大小的两输入与非门 -- 的输入的、该示例电路元件的示例标称漏电流的示例表格。表 10 中的单独的行 10a、...、10d 示出了与非门的不同输入和与非门的对应标称漏电流（以毫微安或 nA 为单位测量）。例如，对于输入 01，标称漏电流可以是大约 100.3nA（如表 10 的行 10b 所示）。如图所示，与非门的漏电流可以至少部分地基于该门的输入。

[0045] 在各个实施例中，电路元件（例如，与非门）的漏电流可以包括单独的门的子阈值漏电流（例如，$I_{sub}$）和 / 或栅极隧穿漏电流（$I_{gate}$）。可以将这两个电流（例如，$I_{sub}$ 和 $I_{gate}$）建模为可以由对数正态分布来近似的指数函数。全芯片漏电流分布可以是各个门的对数正态分布之和。理论上可能不知道该和具有闭合形式，但是使用本领域技术人员公知的方法，该和可以近似为对数正态分布。

[0046] 再次参照图 2a，表 10 中示出的漏电流可以是与非门的标称或通常漏电流值。然而，如先前所讨论的，由于制造过程中的变化，漏电流可能随一个与非门到另一个与非门而改变。因而，表 10 中示出的标称漏电流值可以是标称大小的与非门的典型、通常、标称、期望或平均值。表 10 的产生可以由根据本公开所理解的任何合理的方法来实现。

[0047] 在各个实施例中，标称漏电流可以至少部分地基于与非门的工作环境（例如，温度、电源电压等），而且表 10 的标称漏电流可以针对特定工作环境。尽管表 10 可以示出典型与非门的标称漏电流，但是可以针对与非门的其它属性（延迟、切换功率等）产生类似的表。此外，也可以针对其它各种类型的电路元件（例如，或非门、其它逻辑门，晶体管、触发器等）的一个或多个属性产生类似的表。

[0048] 图 2b 示出了可以适合于实践各个实施例的示例 IC30 的一部分。IC30 可以包括若干电路元件，但在图 2b 中仅示出 IC30 的四个示例电路元件（四个与非门 G1、...、G4）。还示出了电路元件的五个基本输入（$i_1$、...、$i_5$）、各个基本输入的示例值（例如，$i_1 = 1$、$i_2 = 0$、...、$i_5 = 1$）、各个中间信号和输出 $O_1$。

[0049] 在各个实施例中，由于各种原因（例如，制造过程中的变化），各个与非门中的一个或多个属性（例如，漏电流、延迟、切换功率等）可以是不同的。在各个实施例中，各个

门 G1、...、G4 的漏电流可以是不同的。例如，针对输入 01，与非门的标称漏电流可以是大约 100.3nA（据表 10），但针对相同输入，门 $G_2$ 可以具有大约 130.39nA 的漏电流。也就是说，针对输入 01，门 $G_2$ 的漏电流可以是典型与非门的标称漏电流的大约 1.3 倍（例如，130.39/100.3 = 1.3）。另一方面，针对输入 01，门 $G_3$ 可以具有例如大约 210.63nA 的漏电流。也就是说，针对输入 01，门 $G_3$ 的漏电流可以是典型与非门的标称漏电流的大约 2.1 倍（例如，210.63/100.3 = 2.1）。在各个实施例中，电路元件的属性的比例因子可以是电路元件中属性的实际值与属性的标称值之比。例如，在以上两个示例中，与非门 $G_2$ 和 $G_3$ 的比例因子可以分别为 1.3 和 2.1。

[0050] 图 2c 示出了根据各个实施例的、被配置为存储针对两个示例 IC 的多个与非门的比例因子的示例表格 50。表 50 中的两个 IC 被标识为 IC1 和 IC2。在各个实施例中，两个 IC（或两个 IC 的一部分）可以是至少部分类似的。在各个实施例中，IC1 和 / 或 IC2 可以具有与图 2b 中所示类似的结构。例如，与图 2b 的 IC30 类似，IC1 和 IC2 均可以包括 4 个与非门 (G1、...、G4)。表 50 的各行 50a、...、50d 可以表示 IC1 和 IC2 的与非门的比例因子。例如，如行 50d 中所示，IC1 和 IC2 的门 G4 可以分别具有大约 3 和 0.9 的比例因子。如表 10 的行 10d 所示，典型与非门的输入 11 的标称漏电流可以是 454.5nA。因此，针对输入 11，IC1 的门 G4 的漏电流可以是例如大约 1363.5nA（例如，3*454.5nA），以及 IC2 的门 G4 的漏电流可以是例如大约 409.05nA（例如，0.9*454.5nA）。在另一示例中，如表 10 的行 10c 所示，典型与非门的输入 10 的标称漏电流可以是 95.7nA。因此，IC1 的门 G2 的漏电流可以是例如大约 124.41nA（例如，1.3*95.7nA），以及 IC2 的门 G2 的漏电流可以是例如大约 382.8nA（例如，4*95.7nA）。

[0051] 尽管未在图 2c 中示出，在各个实施例中，使用表 10 和 50，可以针对与非门的各个输入（例如，00，01，10 和 / 或 11）确定 IC1 和 IC2 的四个与非门 G1、...、G4 的漏电流。

[0052] 图 2d 示出了根据各个实施例的、被配置为针对各种输入矢量，存储两个示例 IC 的一个或多个电路元件中的总漏电流的示例表格 70。例如，表 70 的各行 70a、...、70d 示出了针对五个基本输入（例如，$i_1$、...、$i_5$）的不同值的、在 IC1 和 IC2 的四个与非门 G1、...、G4 中的总漏电流。

[0053] 例如，行 70b 可以示出针对输入矢量 10101（例如，当 $i_1 = 1$、$i_2 = 0$、...、$i_5 = 1$）的、在 IC1 和 IC2 的四个与非门 G1、...、G4 中的总漏电流。针对该示例输入矢量，在图 2b 中示出了各种中间信号和输出的状态。例如，在这种情况下，门 G1、...、G4 的输入可以分别是 10、11、00 和 11。在各个实施例中，考虑 IC2 具有 10101 的示例输入矢量。针对该输入矢量，门 G1 的输入可以是 10（例如，参见图 2b），以及门 G1 的相应漏电流可以是大约 95.7*2.4nA（分别根据表 10 和 30 的行 10c 和 50a）或大约 229.68nA。类似地，门 G2 的输入可以是 11，门 G2 的相应漏电流可以是大约 454.5*0.6nA 或大约 272.7nA。门 G3 的输入可以具有值 00，以及门 G3 的相应漏电流可以大致与 37.84*4nA 或大约 151.36nA 相对应。门 G4 的输入可以是 11，以及门 G4 的相应漏电流可以是大约 454.5*0.9nA 或大约 409.05nA。因此，针对输入矢量 10101，IC2 的四个与非门的组合漏电流可以是大约 (229.68+272.7+151.36+409.05)*1nA ≈ 1063nA，如表 70 的行 70b 所示。表 70 的其它条目类似地示出了针对各种其他示例输入矢量的、IC1 和 IC2 的四个与非门的总的或组合的漏电流。

[0054] 尽管图 2a、2c 和 2d 中的表格提及了根据示例配置设置的四个示例与非门的示例

属性（例如，漏电流），但是在各个实施例中，可以针对各种其它类型和配置的电路元件（例如，其它类型的逻辑门、晶体管等）的各种其它属性（延迟、切换功率、或任何其它适合属性），产生类似表格。

[0055] 在各个实施例中，可以使用例如表 1a 和 1b 中的信息来产生表 70。在各个实施例中，尽管可以提前知道与非门的标称漏电流（如在表 10 中），但是 IC 中的各个与非门的比例因子（如在表 50 中）并不总是已知的，并且针对相同或不同的 IC 中的不同与非门，这种比例因子可以是不同的。

[0056] 然而，在各个实施例中，可以测量总漏电流（例如，表 70 的漏电流）。根据所测量的总漏电流，可以确定相关电路元件的比例因子。在各个实施例中，使用所确定的比例因子，可以标识并认证 IC，这将在之后进行详述。

[0057] 确定集成电路的比例因子

[0058] 图 3a 示出了适合于实践根据本公开的各个实施例的示例 IC200 的一部分。IC200 可以包括多个电路元件，但是在图 3a 中，仅示出了六个示例电路元件（三个与非门 X、Y 和 V 和三个或非门 U、W 和 Z）。还示出了电路元件的六个基本输入（$i_1$、...、$i_6$）、各个基本输入的示例值（例如，$\{i_1、...、i_6\} = 000000$）、各个中间信号、以及输出 $O_1$、$O_2$ 和 $O_3$。

[0059] 图 3b 示出了根据本公开的各个实施例的、被配置为存储与非和或非门的示例标称漏电流对比各个门的输入的示例表格 240。为了本公开的目的，除非特别说明，在各个实施例中，$I_{ABC}(xx)$ 可以表示电路元件 ABC 中的示例标称漏电流，其中括号内的自变量可以是电路元件的输入。例如，$I_{NAND}(01)$ 和 $I_{NOR}(11)$ 可以分别表示针对输入 01 的标称大小的 2 输入与非门的示例标称漏电流和针对输入 11 的标称大小的 2 输入或非门的示例标称漏电流。

[0060] 如前所述，在各个实施例中，由于各种原因（例如，制造过程中的变化），IC200 的各个电路元件的一个或多个属性（例如，漏电流、延迟、切换功率等）可以不同于相应的标称值。因而，如之前所讨论的，图 3a 的一个或多个与非和 / 或或非门的漏电流是表 240 的标称漏电流的相应的比例因子的倍数。在各个实施例中，图 3a 中示出的六个门 U、V、...、Z 的比例因子可以由 $S_U$、SV、...、$S_Z$ 表示。在各个实施例中，可以基于一个或多个门 U、V、...、Z 的漏电流的测量来确定这些比例因子。

[0061] 图 3a 中示出的电路元件的总漏电流可以至少部分地基于输入 $i_1$、...、$i_6$。这些输入可以取多个值之一（例如，$\{i_1、...、i_6\} = 000000, 000001, 010101$ 等）。为了本公开的目的，基本输入可以形成相应的输入矢量。因而，010101 的输入矢量可以指 $i_1 = 0$、$i_2 = 1$、$i_3 = 0$、$i_4 = 1$、$i_5 = 0$、$i_6 = 1$ 的输入。在各个实施例中，多个输入矢量中的一个或多个（例如，000000, 010101, 111111, 101010 等）可以应用于 IC200 的电路元件。

[0062] 在各个实施例中，$I_{leak}(\bullet)$ 可以表示针对图 3a 中所示的六个电路元件测量到的漏电流，其中括号内的自变量可以是可以针对其测量漏电流的输入矢量。例如，漏电流 $I_{leak}(000000)$ 可以是针对输入矢量 000000 的、图 3a 的六个门中的测量到的漏电流。在各个实施例中，由于例如测量中的限制或误差，测量到的漏电流可能有误差（由 $e_1$ 表示）。

[0063] 在各个实施例中，测量到的漏电流 $I_{leak}(000000)$ 可以由各个门的漏电流和误差项 $e_1$ 来表示。例如，针对输入矢量 000000，门 X 的输入可以是 00，门 X 的相应漏电流可以是 $S_X . I_{NAND}(00)$，其中 $S_X$ 可以是未知的，$I_{NAND}(00)$ 的值（例如，37.84nA）可以从表 240 的行 240a 中得到。在另一示例中，针对输入矢量 000000，门 U 的输入可以是 10，门 U 的相应漏电流

可以是 $S_U$. $I_{NOR}(10)$，其中 $S_U$ 可以是未知的，$I_{NOR}(10)$ 的值（例如，213nA）可以从表 240 的行 240c 中得到。因而，IC200 的漏电流 $I_{leak}(000000)$ 可以表示如下：

[0064] $I_{leak}(000000)+e_1 = S_X. I_{NAND}(00)+S_Y. I_{NAND}(00)+S_Z. I_{NOR}(00)+S_U. I_{NOR}(01)+S_V. I_{NAND}(11)+S_W. I_{NOR}(11)$

[0065] 等式 1

[0066] 在各个实施例中，针对各种其它输入矢量，可以形成类似等式。例如：

[0067] $I_{leak}(010101)+e_2 = S_X. I_{NAND}(01)+S_Y. I_{NAND}(01)+S_Z. I_{NOR}(01)+S_U. I_{NOR}(11)+S_V. I_{NAND}(11)+S_W. I_{NOR}(10)$

[0068] 等式 2

[0069] 在各个实施例中，针对相应的 M 个不同的输入矢量，可以形成 M 个不同的等式（例如，等式 1，...，M）。例如，等式 M 可以是

[0070] $I_{leak}(111000)+e_i = S_X. I_{NAND}(11)+S_Y. I_{NAND}(10)+S_Z. I_{NOR}(00)+S_U. I_{NOR}(01)+S_V. I_{NAND}(11)+S_W. I_{NOR}(11)$。

[0071] 等式 M

[0072] 其中，等式 M 针对示例输入矢量 111000。

[0073] 针对给定的输入矢量，M 个线性等式可以表示六个门 U、...、Z 的总测量漏电流与各个门的比例因子 $S_U$、...、$S_Z$ 之间的线性关系，其中比例因子可能不是预先知晓的。在各个实施例中，可以用公式表示最优化问题，以确定比例因子 $S_U$、...、$S_Z$。例如，等式 1、...、M 可以形成最优化问题的约束。目标函数 (OF) 可以优化测量误差的特定范数 (specific norm)。例如，函数 f(E) 可以表示用于测量误差度量的函数，其中 $E=\{e_i\}_{i=1}^{M}$，而且 OF 经受 M 个约束（例如，M 个等式）可以将 f(E) 最小化（例如，OF :minf(E)）。这里所使用的术语“最小化”和 / 或类似术语可以包括全局最小化、局部最小化、近似全局最小化、和 / 或近似局部最小化。类似地，还应理解，这里所使用的术语“最大化”和 / 或类似术语可以包括全局最大化、局部最大化、近似全局最大化、和 / 或近似局部最大化。

[0074] 在各个实施例中，函数 f(•) 可以采用各种形式之一。例如，误差函数的任何适合的 $L_P$ 范数可以用于函数 f(•)，其中 $L_P$ 范数可以定义为 $L_p=(\sum_{m=1}^{M} w_m |e_m|^p)^{1/p}$，$1\leq p\leq\infty$，，以及 $L_p=\max_{m=1}^{M} w_m |e_m|$，若 $p=\infty$，...

[0075] 等式 (M+1)，

[0076] 其中 $w_m$ 可以是适合的加权因子。

[0077] 在各个实施例中，最优化问题可以至少部分地基于 OF 的形式和 / 或函数 f(E) 而采用许多不同的格式。在各个实施例中，$L_P$ 误差范数可以包括 OF 中的非线性项，可以使用可用的非线性最优化方法来进行求解。在各个实施例中，非线性问题可以以公式表示或变换为线性、二次方程式、或凸最优化问题，并进行相应的求解。

[0078] 例如，$L_1$ 范数可以用于以公式表示函数 f(E)。在该情况下，可以以线性程序的形式，将 OF 写作：

[0079] $\min \sum_{m=1}^{M} |e_m|$

[0080] 线性程序可以经受等式 1、...、M 的 M 个约束。在这种情况下，可以通过引入 M 个辅助变量$e_m^+$，m = 1,...,M，并添加 2M 个约束（例如，针对各个 m，$e_m^+ \geq e_m$，且$e_m^+ \geq -e_m$），将绝对函数 $|e_m|$（尽管是非线性的）转换为线性形式。在各个实施例中，可以使用本领域技术人员已知的各种可用线性规划技术来对最优化问题进行求解，以确定一个或多个比例因子 $S_U$、...、$S_Z$。

[0081] 在另一示例中，$L_2$ 范数可以用于以公式表示函数 f(E)。在该情况下，OF 可以写作：

[0082] $$\min \sqrt{\sum_{m=1}^{M} e_m^2}$$

[0083] 它可以等同于

[0084] $$\min \sum_{m=1}^{M} e_m^2$$。

[0085] OF 可以是二次方程形式的，可以使用本领域技术人员已知的各种可用的非线性和 / 或二次规划技术来对最优化问题进行求解，以确定一个或多个比例因子 $S_U$、...、$S_Z$。

[0086] 在另一示例中，$L_\infty$ 范数可以用于以公式表示函数 f(E)。在该情况下，可以以公式表示新变量 $e_{max}$，针对 m = 1,...,M，满足约束 $e_{max} \leqslant e_m$。OF 可以简化为 $OF = \min(e_{max})$，可以使用本领域技术人员已知的各种可用的线性规划技术之一来对最优化问题进行求解，以确定一个或多个比例因子 $S_U$、...、$S_Z$。

[0087] 在各个实施例中，可以假设一个或多个误差项 $e_i$，i = 1,...,M，遵循独立同分布 (i.i.d.) 高斯分布 $N(0, \sigma^2)$。在这种情况下，对数似然函数可以表示为：

[0088] $$\max \sum_{m=1}^{M} \log(\exp^{\frac{e_m^2}{2\sigma^2}}) \equiv \max \sum_{m=1}^{M} -e_m^2 \equiv \min \sum_{m=1}^{M} e_m^2$$

[0089] 该表示可以等同于先前讨论的 OF 的二次方程形式，并且可以使用本领域技术人员已知的各种可用的非线性和 / 或二次规划技术之一来对最优化问题进行求解，以确定一个或多个比例因子 $S_U$、...、$S_Z$。

[0090] 因而，如所讨论的，可以通过测量各种输入矢量的总漏电流 $I_{leak}(\cdot)$、以公式表示并求解相关最优化问题来确定比例因子 $S_U$、...、$S_Z$。在各个实施例中，作为针对各个门的漏电流确定比例因子的替代和 / 或除此之外，可以以类似的方式确定一个或多个其它属性的比例因子。例如，可以确定针对各个门的切换延迟的比例因子和 / 或针对各个门的切换功率需求的比例因子。在各个实施例中，可以确定一个或多个电路元件的多于一个属性的比例因子，并在后续用于产生 IC 的标识 (ID)。

[0091] 在各个实施例中，并不总是存在 IC 的对应的一个或多个电路元件的一个或多个比例因子的唯一解。可能存在一个或多个多义电路元件，对于该多义电路元件，并不总是能够确定对应的比例因子。多义电路元件可以指其组合可以实现比例因子的相同比例、和 / 或其比例因子可能是不可分辨（因而是无法唯一确定）的那些电路元件。例如，可以串联地设置三个逆变器 Inv A、Inv B 和 Inv C（例如，比例因子分别为 $S_A$、$S_B$ 和 $S_C$），使得 Inv A 的输出与 Inv B 的输入耦合，Inv B 的输出与 Inv C 的输入耦合。针对这种设置，可以在对应的漏电流等式集合中出现项 ($S_A\ I_{inv}(0)+S_B\ I_{inv}(1)+S_C\ I_{inv}(0)$) 和 / 或项 ($S_A\ I_{inv}(1)+S_B\ I_{inv}(0)+S_C\ I_{inv}(1)$)，其中 $I_{inv}(\cdot)$ 可以表示逆变器针对对应输入的标称漏电流。在各个实

施例中，根据这两项中的一个（或两个），不可能通过对相关的最优化问题进行求解来区分比例因子 $S_A$、$S_B$ 和 / 或 $S_C$，因为例如缺少足够的自由度。

[0092] 还可以存在 IC 中的多义电路元件的许多其它示例（例如，由于重汇聚扇出）。在各个实施例中，在以公式表示和 / 或求解与确定比例因子相关联的最优化问题的同时，可以考虑多义电路元件。例如，可以对漏电流等式进行求解，以识别一个或多个多义电路元件。在各个实施例中，可以将一个或多个多义电路元件固化为一个实体，和 / 或在产生 IC 的 ID 的过程中可以不使用一个或多个多义电路元件的特性（例如，比例因子）。

[0093] 图 4 示出了根据本公开的各个实施例的、用于确定 IC 的对应多个电路元件的多个比例因子的示例方法 300。在各个实施例中，方法 300 可以包括块 304、308、312 和 / 或 316 中的一个或多个。

[0094] 在块 304，方法 300 可以包括：将多个输入矢量应用于 IC 中包括的多个电路元件。例如，多个输入矢量可以应用于图 3a 的 IC200 的门 U、...、Z。处理可以从块 304 继续至块 308。

[0095] 在块 308，方法 300 可以包括：响应于应用多个输入矢量，测量 IC 的一个或多个属性的多个值，其中可以响应于应用对应的输入矢量，测量各个属性值。例如，属性可以是漏电流、切换功率、延迟、和 / 或任何其它适合的属性。例如，如前所述，属性可以是图 3a 中示出的六个电路元件的总漏电流 $I_{leak}(\bullet)$。针对各个输入矢量，可以测量漏电流 $I_{leak}(\bullet)$ 的对应值。处理可以从块 308 继续至块 312。

[0096] 在块 312，方法 300 可以包括：基于对应的多个测量值，形成多个等式，其中多个等式中的每个可以包括对应的一个或多个电路元件的一个或多个比例因子。例如，基于总漏电流 $I_{leak}(\bullet)$ 的测量值，可以形成等式 1，...，M。各个等式可以对应于与相应地应用的输入矢量相对应的总漏电流 $I_{leak}(\bullet)$ 的测量值。例如，可以基于总漏电流 $I_{leak}(000000)$ 形成等式 1，如前所述，可以响应于应用输入矢量 000000 来测量总漏电流 $I_{leak}(000000)$。在各个实施例中，PI（例如，针对 IC200 等于 6）可以是所考虑的电路元件的基本输入（$i_1$、...、$i_6$）的数量，G（例如，6）可以是所考虑的电路元件（例如，门 U、...、Z）的数量。在这种情况下，所产生的等式的数量可以等于 $\min\{2^{PI}, 3G\}$。处理可以从块 312 继续至块 316。

[0097] 在块 316，方法 300 可以包括：对多个等式进行求解，以确定一个或多个比例因子。例如，可以使用之前所讨论的若干最优化技术之一来对等式 1，...，M 进行求解。方法 300 可以在块 316 之后结束。

[0098] 在各个实施例中，可以操作 IC，使得测量一个或多个属性值的误差可以相对较低，和 / 或可以以相对较低的精度需求来测量一个或多个属性值。也就是说，可以改变 IC 的一个或多个工作条件（例如，一个或多个电路元件的温度、工作电压等）来降低测量一个或多个属性值所需的精度。例如，当测量与漏电流、延迟或切换功率相对应的值时（例如，当使用漏电流和 / 或切换功率作为属性时），可以有意地提高 IC 的温度（例如，使用自加热），这会增加 IC 的各个电路元件的漏电流、切换延迟和 / 或切换功率，从而降低对于测量误差的敏感度。在各个实施例中，在切换延迟可以用作属性的情况下，可以降低 IC 的电源电压，这会导致各个电路元件的切换延迟的增加，从而降低对于测量的敏感度。由于这些工作条件的改变（例如，各个电路元件的温度和工作电压的改变）会成比例地影响可以针对其确定比例因子的各个电路元件，因而这些改变不会影响比例因子。例如，图 3a 的六个门的温度

的提高会基本成比例地影响六个门的漏电流（例如，将各个门的漏电流增大例如 5％）。可以从各个等式 1，...，M 的两侧抵消漏电流的增大，从而不对各个门的比例因子产生影响。

[0099] IC 标识中的比例因子变换

[0100] 在各个实施例中，在确定了 IC 的一个或多个电路元件的比例因子之后，所确定的比例因子可以用于产生 IC 的 ID。可以以各种方式将比例因子变换为 IC 的 ID。

[0101] 在简单的示例场景中，等于或大于 1 的比例因子可以由 IC 的 ID 号中的 1 来表示，而小于 1 的比例因子可以由 IC 的 ID 号中的 0 来表示。例如，如图 2c 的表 50 中所示，IC1 的门 G1、...、G4 的比例因子可以分别等于 0.5、1.3、2.1 和 3。因而，IC1 的示例 ID 号可以对应于 0111，该 ID 号中的每个数字被映射到门 G1、...、G4 的相应的比例因子。类似地，基于比例因子 2.4、0.6、4.0 和 0.9，表 50 的 IC2 的 ID 号可以对应于 1010。

[0102] 比例因子可以以各种方式变换为或映射为 IC 的 ID。ID 的产生可以基于多种因素。例如，考虑各种电路元件的比例因子的顺序会影响这种 ID 的产生。在各个实施例中，IC 的指示符字符串的长度可以指可以用于产生 IC ID 的 IC 设计的连线表 (netlist) 中的电路元件的数量（例如，门的数量）。连线表可以描述电子设计中各种电路元件的连接。在各个实施例中，连线表中的电路元件的顺序可以对应于各个电路元件的 x 和 y 位置坐标。例如，具有较小 x 坐标的电路元件可以具有比具有相对较大 x 坐标的电路元件低的位置。如果两个电路元件具有相同的 x 坐标，则具有较小 y 坐标的电路元件可以具有比具有相对较大 y 坐标的电路元件低的位置。因而，可以基于相应的坐标来对一个或多个电路元件进行排序，在产生针对关联 IC 的 ID 期间，可以使用电路元件的这种排序。

[0103] 在各个实施例中，例如由于多义电路元件的出现、以公式表示和 / 或求解相关最优化问题的复杂度、缺少一个或多个电路元件的漏电流的测量等，可能无法确定 IC 中的每个电路元件的比例因子。在各个实施例中，可能不需要 IC 中每个电路元件的特征从而以公式表示 IC 的 ID。如果电路元件可以用于标识，则指示符字符串中的对应比特可以设置为 1。类似地，如果电路元件不可以用于标识，则指示符字符串中的对应比特可以设置为 0。在各个实施例中，指示符字符串可以表示其比例因子可以用于产生 IC 的 ID 的电路元件。

[0104] 在各个实施例中，在将模拟比例因子变换为 IC 的 ID 时，可以考虑各种因素。例如，可以考虑模拟比例因子的分布来选择要用于产生 ID 的一个或多个比例因子和 / 或将模拟比例因子转换为数字标识。在各个实施例中，在提取了 IC 的多个电路元件的比例因子之后，可以产生所提取的比例因子的直方图或概率密度函数 (PDF)。

[0105] 图 5 示出了根据本公开的各个实施例的 IC 的示例比例因子的 PDF400。在各个实施例中，示例 PDF400 可以具有有着示例标准偏差 σ 的钟型曲线，但是其它形状的 PDF 也是可能的。在各个实施例中，PDF400 可以是在直方图曲线的适当平滑之后获得的所提取的比例因子的直方图。

[0106] 可以使用各种二进制编码技术之一，以利用例如所提取的比例因子的 PDF 或直方图，将一个或多个比例因子变换为二进制形式。例如，二进制编码技术可以利用将在以下讨论的恒定裕量编码和 / 或等面积编码的概念。

[0107] 恒定裕量编码

[0108] 图 6a 示出了根据本公开的各个实施例的、用于以二进制形式对多个比例因子进行编码的恒定裕度编码技术。图 6a 包括比例因子的 PDF500。恒定裕量编码可以通过将

PDF500 分为多个区域或部分，来找到模拟比例因子码的鲁棒二进制转换。在图 6a 中，可以将区域标记为白色（例如，区域 504a、504b、504c 等）或灰色（例如，区域 502a、502b、502c 等）。白色和暗色区域可以是交错的。

[0109] 在各个实施例中，一个或多个白色区域可以具有类似的宽度，一个或多个灰色区域可以具有类似的宽度。在一些实施例中，各个白色区域可以具有类似的宽度，各个灰色区域可以具有类似的宽度，白色区域的平均宽度可以相对大于灰色区域的平均宽度。在一些其它实施例中，各个白色区域和各个灰色区域可以具有类似的宽度。PDF500 中的白色和 / 或灰色区域的数量和 / 或宽度仅是示例，具有不同数量的区域和 / 或不同宽度的白色和 / 或灰色区域的 PDF 也是可设想到的，并且在本公开的范围内。

[0110] 在各个实施例中，在 IC 的 ID 形成期间，可以允许或禁止具有类似颜色编码的区域。例如，可以允许白色区域 504a、504b、504c 等，而禁止灰色区域 502a、502b、502c 等。因而，如果电路元件的比例因子的值落入被禁止的区域（例如，区域 502b），则在 ID 信息中不会考虑该比例因子，指示符字符串中的对应比特可以设置为 0。类似地，如果电路元件的比例因子的值落入被允许的区域（例如，区域 504a），则在 ID 信息中可以考虑该比例因子，指示符字符串中的对应比特可以设置为 1。

[0111] 在各个实施例中，可以将二进制码赋予各个被允许的区域。例如，可以将码 000、001 和 010 分别赋予白色区域 504a、504b 和 504c。落入特定白色区域（例如，区域 504b）中的比例因子可以获得相应区域的二进制码（例如，001）。可以确定落入被允许的区域的各个比例因子的二进制码，它们可以形成 IC 的 ID。

[0112] 在一些实施例中，二进制码的长度可以至少部分地基于分区的数量。相对大量的分区（例如，具有较小区域宽度）可以增加 IC ID 的长度，但是会降低二进制码的鲁棒性。因而，分区的数量可以提供 ID 长度与二进制码的鲁棒性之间的折衷。

[0113] 图 6b 示出了根据本公开的各个实施例的、用于至少部分地基于 IC 的对应多个电路元件所确定的多个比例因子来产生 IC 的 ID 的方法 520。在各个实施例中，可以使用例如图 4 的方法 300 来确定多个比例因子。

[0114] 参照图 6a 和 6b，在各个实施例中，方法 520 可以包括块 524、528、532、536、540、544、548 和 / 或 552 中的一个或多个。

[0115] 在块 524，方法 520 可以包括 ：产生多个比例因子的 PDF（例如，图 6a 的 PDF500）。

[0116] 处理可以从块 524 继续至块 528，块 528 可以包括 ：将 PDF 下的区域分为多个部分，使得各个部分具有大致相等的宽度。例如，如图 6a 所示，PDF500 下的区域可以被分为多个部分 502a、...、502c、504a、...、504c 等，使得各个部分具有大致相等的宽度。处理可以从块 528 继续至块 532。

[0117] 在块 532，方法 520 可以包括 ：将多个部分分为第一集合的部分（例如，白色区域 504a、...、504c）和第二集合的部分（例如，灰色区域 502a、...、502c），使得第一集合的部分中的各个部分和第二集合的部分中的各个部分是交错的（例如，各个白色和灰色部分是交错的）。处理可以从块 532 继续至块 536。

[0118] 在块 536，方法 520 可以包括 ：选择落入第一集合的部分中的一个或多个部分的一个或多个比例因子。例如，可以选择落入白色部分中的一个或多个部分的一个或多个比例因子来产生 IC 的 ID。在各个实施例中，如前所述，在指示符字符串中，与所选比例因子相对

应的比特可以设置为 1。处理可以从块 536 继续至块 540。

[0119] 在块 540，方法 520 可以包括：将二进制码分配给第一集合的部分中的各个部分，使得第一集合的部分中的每个单独的部分与相应的二进制码相关联。例如，可以向白色部分 504a、504b、504c 分别分配二进制码 000、001 和 101。处理可以从块 540 继续至块 544。

[0120] 在块 544，方法 520 可以包括：基于分配给各个部分的二进制码，将二进制码分配给包括在第一集合的部分之中的各个部分中的比例因子。例如，可以将二进制码 001 分配给包括在部分 504b 中的各个比例因子。处理可以从块 544 继续至块 548。

[0121] 在块 548，方法 520 可以包括：将一个或多个所选比例因子中的各个比例因子映射到对应的二进制码。例如，在块 544 处执行的将二进制码向各个所选择的比例因子的分配可以是块 548 处的映射的一部分。处理可以从块 548 继续至块 552。

[0122] 在块 552，方法 520 可以包括：使用所映射的二进制码来产生 IC 的 ID 号。方法 520 可以在块 552 之后结束。

[0123] 等面积编码

[0124] 图 7a 示出了根据各个实施例的、以二进制形式对多个比例因子进行编码的等面积编码技术。图 7a 包括比例因子的 PDF600。等面积编码可以通过将 PDF 曲线 600 下的区域分为多个区域或部分（例如，区域 604a、604b、604c、604d 等），来找到模拟比例因子码的鲁棒二进制转换。在各个实施例中，可以对区域进行划分，使得各个区域的 PDF 曲线下的面积可以大致相等。因而，属于任一区域的比例因子的概率可以基本相似。在图 7a 的示例分区中，PDF600 可以分为 8 个区域，但是可以有不同数量的区域。在各个实施例中，可以向各个区域分配二进制比特码。例如，针对 8 区域分区，3 比特码可以用于标识各个区域，如图 7a 所示（例如，可以向区域 604b 分配 101）。

[0125] 在一些实施例中，图 7a 中的一个或多个（或全部）区域可以用于产生 IC 的 ID。落入特定区域（例如，区域 604b）的比例因子可以获得相应区域的二进制码（例如，101）。可以确定各个比例因子的二进制码，它们可以形成 IC 的 ID。

[0126] 在一些其它实施例中，由于各种因素（例如，测量误差、确定比例因子过程中的误差等），假设处于某区域（例如，具有码 101 的区域 604b）的比例因子实际会落入相邻区域（例如，区域 604a 或 604c）。在一些实施例中，可以通过在验证或认证 IC 的 ID 期间考虑这些部分的顺序来获得 ID 的鲁棒性。例如，将比例因子的值改变相对小的量会解译为将比例因子移至图 7a 的前一或后一区域。编码方案可以考虑这种改变。例如，门的比例因子可以落入区域 604b，并且可以编码为 101。针对 ID 验证，可以考虑同一门的比例因子等于可以具有码 100、101 或 111 的任意门。因而，所分配的 ID 对于比例因子的小变化来说可以是鲁棒的，只要比例因子待在预期区域（例如，区域 604b）或在相邻区域（例如，区域 604a 或 604c）中。

[0127] 图 7b 示出了根据本公开的各个实施例的、用于至少部分地基于 IC 的对应多个电路元件所确定的多个比例因子来产生 IC 的 ID 的方法 620。在各个实施例中，可以使用例如图 4 的方法 300 来确定多个比例因子。参照图 7a 和 7b，在各个实施例中，方法 620 可以包括块 624、628、632、636 和 / 或 640 中的一个或多个。

[0128] 在块 624，方法 620 可以包括：产生多个比例因子的 PDF（例如，图 7a 的 PDF600）。处理可以从块 624 继续至块 628。

[0129] 在块628，方法620可以包括：将PDF下的区域分为多个部分（例如，部分604a、...、604d等），使得各个部分可以具有大致相等的面积。处理可以从块628继续至块632。

[0130] 在块632，方法620可以包括：将二进制码分配给各个部分，使得每个单独的部分与相应的二进制码相关联（例如，将二进制码101分配给部分604b）。处理可以从块632继续至块636。

[0131] 在块636，方法620可以包括：基于分配给各个部分的二进制码，将二进制码分配给包括在各个部分中的比例因子。例如，可以向包括在部分604b中的各个比例因子分配二进制码101。在各个实施例中，二进制码向各个比例因子的分配可以将比例因子映射到对应的二进制码。处理可以从块636继续至块640。

[0132] 在块640，方法620可以包括：使用所分配的二进制码来产生IC的ID。方法620可以在块640之后结束。

[0133] ID冲突的概率分析

[0134] 一旦产生了ID，便可以分析所产生的ID的稳健性（例如，所产生的ID是否唯一的概率）。在各个实施例中，所产生的ID可以包括K个二进制序列的集合，各个序列的长度为M。例如，K个比例因子可以用于产生二进制码，其中各个二进制码可以具有长度M（例如，3）。具有相同ID的多于一个IC的概率可以等于K个串中冲突的概率。在各个实施例中，可以有总共 $n = 2^M$ 个二进制长度为M的序列。变量Pi可以表示IC的ID位于序列i中的概率，令 $P = (P1, \ldots Pn)$ 是全部 $n = 2^M$ 个序列的概率的集合。

[0135] 可以通过下式给出K个序列之间无匹配的概率：

[0136] $$P(M, K, n^{-1}) = \frac{2^M!}{K^{2M}(2^M - K)!}$$

[0137] 可以通过下式给出冲突概率：

[0138] $$P(\text{collision}) = 1 - \frac{2^M!}{K^{2M}(2^M - K)!}$$

[0139] 当序列可能不太类似时，可以通过下式给出冲突概率：

[0140] $$P(collision) = 1 - P(M, K, P) = 1 - K! \sum_{1 \le v1 < K \le n} P_{v1} P_{v2K} P_{vK}, \quad \cdots \text{等式 (M+2)}$$

[0141] 其中P(M,K,P)可以是无冲突发生的表示（complimentary）概率。该等式可以表示ID的冲突概率。该概率可以至少部分地基于ID产生问题的公式化。

[0142] 例如，在第一情况下，所产生的ID的序列中的比特可以是独立同分布（i.i.d），P（任意比特为1）= π，且P（任意比特为0）= 1-π。在这种情况下，可以通过 $P_i = (1-\pi)^{n_0 i} \pi^{n_1 i}$ 给出概率 $P_i$，其中 $n_0 i$ 可以表示序列i中0的总数，以及 $n_1 i$ 可以表示序列i中1的总数。

[0143] 在第二情况下，各个序列中的比特可以是独立但不同分布的，

[0144] P（比特m为1）= $\pi_m$

[0145] P（比特m为0）= $1-\pi_m$

[0146] 函数 $I(b_m)$ 可以定义为：

[0147] $$I(b_m)=\begin{cases}\pi_m, & b_m=1\\ 1-\pi_m, & b_m=0\end{cases}$$。

[0148] 概率 Pi 可以表示为：

[0149] $$P_i=\prod_{m=1}^{M}I(b_m)$$。

[0150] 在第三情况下，各个序列中的比特可以是相关的，如前所述，它们的累积分布函数 (CDF) 可以是 P。

[0151] 在各个实施例中，如果冲突概率（例如，两个 IC 的 ID 相类似的概率）实质上较高（例如，高于阈值），则可以产生更稳健的 ID（例如，可具有相对较小冲突概率的 ID）。例如，可以增加为产生 ID 而选择的电路元件，可以增大 ID 的长度（例如，通过增加要被考虑用于产生 ID 的比例因子的数量），和 / 或可以增加要使用的属性的数量。

[0152] ID 冲突的统计分析

[0153] 图 8 示出了根据本公开的各个实施例的阐明 IC 的 ID 的冲突概率的示例图 700。例如，使用蒙特卡罗模拟方法来产生该图。在图 700 中示出了相应电路元件的两个比例因子的模拟值（例如，特征 A 和特征 B）。各个电路元件的所提取的模拟比例因子可以用作图中的坐标。

[0154] 尽管这里仅示出了两个比例因子来产生图 700，但是可以使用多于两个比例因子来产生这种图（但是这种图会具有较高维度）。例如，M’个特征（例如，M’个比例因子）可以产生 M’个维度空间。

[0155] 在各个实施例中，可以有 K 个 IC，其中可以考虑各个 IC 的 M’个比例因子来产生相应 IC 的 ID。可以计算 ID 的冲突概率（例如，多于一个 IC 具有相同 ID 的概率）。为了计算冲突概率，M’个维度的范围 (sphere) 可以被定位多次（例如，图 8 中的 10 个二维范围 702a、...。702c 等）。各个范围的中心可以表示 ID 的位置。可以向落入一个圈中的点分配相同的 ID（例如，落入一个圈 702a 中的点 704a 和 704b）。由于可以多次重复实验（例如，圈产生），因而可以由于对测量的有限分解来对各个圈内可能的点的数量进行计数。

[0156] 可以将整个空间的冲突概率计算如下：

[0157] $$P(collision)=\sum_{n=1}^{N_{MC}}P(collision\,|\,C_n)P(C_n)$$

[0158] $N_{MC}$ 可以表示蒙特卡罗模拟方法运行的次数，n 可以是各个模拟的索引，以及 $C_n$ 可以是针对一次模拟运行所产生的范围。蒙特卡罗分析的参数可以是范围的半径和随机运行数量 ($N_{MC}$)。

[0159] 在各个实施例中，如果冲突概率（例如，两个 IC 的 ID 相类似的概率）实质上较高（例如，高于阈值），则可以产生更稳健的 ID（例如，可具有相对较小冲突概率的 ID）。例如，可以增大 ID 的长度（例如，通过增加要被考虑用于产生 ID 的比例因子的数量），和 / 或可以增加要使用的属性的数量。

[0160] 在多种应用中，可以使用所产生的比例因子和 IC 的 ID。例如，可以产生多个电路元件的一个或多个属性的比例因子，以及所产生的比例因子可以用于改进 IC 的工作条件。例如，比例因子可以指示 IC 中的一个或多个电路元件的漏电流。在各个实施例中，在 IC 工作期间，可以选择输入矢量，使得减小 IC 的漏电流。例如，与具有相对较低漏电流的电路元

件相比，可以相对较不频繁地（或在较短的持续时间或时钟周期内）使用（根据相应的比例因子）被标识为具有较高漏电流的电路元件。例如，可以通过适当地选择输入矢量来实现对电路元件的这种选择性使用。

[0161] 在各个实施例中，可以确定输入矢量或数据分配的调度，使得可以减小一个或多个属性的不利影响（例如，切换延迟、切换功率、工作温度、寄生电容、偏移电压、增益）。例如，减小这些属性中的一个或多个可以导致 IC 改进的功率和热管理、改进的工作条件、持久的工作寿命等。在各个实施例中，还可以确定在给定持续时间内要在 IC 上执行的任务的工作电压，使得降低 IC 的总漏电流、温度、寄生电容或老化速度。这种确定可以至少部分地基于一个或多个电路元件的比例因子。

[0162] 在各个实施例中，可以使用 IC 的 ID 和 / 或比例因子来认证 IC。例如，IC 的 ID（或 IC 的一个或多个电路元件的比例因子）可以是唯一的。在各个实施例中，IC 可以使用 IC 的唯一 ID（或 IC 的一个或多个电路元件的比例因子）来向设备（例如，服务器、负责认证的设备等）认证 IC 自身。该设备可以通过启动向包括在 IC 中的电路元件中的一个或多个应用一个或多个输入矢量，来询问 IC 的标识。响应于所应有的输入矢量，该设备可以测量一个或多个响应值，其中响应值可以包括对电路元件的一个或多个工作特性（例如，漏电流、切换延迟、切换功率、工作温度、寄生电容、偏移电压、增益）的指示。响应值可以与电路元件的比例因子相关联。该设备可以将接收到的响应值与存储在 IC 外部的数据库中的响应值进行比较。基于该比较，设备可以认证 IC。在各个实施例中，设备可以至少部分地基于对 IC 的认证，许可 IC 或 IC 的用户对一个或多个服务或设备的访问或操作权。

[0163] 例如，车钥匙可以具有嵌入其中的 IC。每次将车钥匙插入（与车钥匙相关联的）车时，车中的认证设备可以将输入矢量应用于车钥匙中的 IC，并接收响应值，其中响应值可以包括对 IC 的一个或多个电路元件的一个或多个工作特性的指示。认证设备可以将该响应值与存储在可由认证设备访问的数据库中存储的响应值进行比较，并基于肯定比较来认证 IC。一旦认证了 IC，例如，认证设备可以运行车钥匙的用户启动车。

[0164] 在各个实施例中，可以在许多其它安全和认证应用中使用 IC 的 ID 和 / 或比例因子，例如，以获取对被阻止的电视频道的访问、向信用卡销货授权等。

[0165] 计算系统

[0166] 图 9 示出了可以适合于实践本公开的各个实施例的示例计算系统 900。计算系统 900 可以包括处理器 910 和存储器 914。计算系统 900 还可以包括一个或多个数据模型和 / 或计算模型，被配置为实践本公开的一个或多个方法。例如，计算系统 900 可以包括 :比例因子确定模块 920，被配置为确定与计算系统 900 操作耦合的 IC960 的比例因子。比例因子确定模块 920 还可以包括 :输入矢量应用模块 924，被配置为选择并向 IC960 中的一个或多个电路元件应用多个输入矢量，或使多个输入矢量应用于 IC960 中的一个或多个电路元件。在各个实施例中，输入矢量应用模块 924 可以被配置为指示（计算系统 900 中和 / 或 IC960 上的）其它组件将输入矢量应用于一个或多个电路元件。

[0167] 比例因子确定模块 920 还可以包括测量模块 928，被设置为测量 IC960 的一个或多个属性（例如，漏电流 $I_{leak}(\bullet)$），或使其获得对一个或多个属性的测量。在各个实施例中，测量模块 928 适于从 IC960 接收这种测量。比例因子确定模块 920 还可以包括等式形成模块，被配置为至少部分地基于一个或多个属性的测量来形成一个或多个等式（例如，等式

1、...、M)。比例因子确定模块 920 还可以包括求解模块 934，被配置为以公式表示并求解最优化问题，以确定 IC960 中的一个或多个相应电路元件的一个或多个比例因子。

[0168] 在各个实施例中，计算系统900可以包括比例因子变换和ID产生模块940，被配置为将所确定的比例因子变换为 IC960 的 ID。在各个实施例中，计算系统 900 可以包括冲突概率估计模块 944，被配置为估计所产生的 ID 的冲突概率。

[0169] 尽管计算系统 900 的各个模块可以示为独立的模块，但是在各个实施例中，这些模块中的一些货全部可以组合为不同的块。在各个实施例中，所示出的模块中的一个或多个还可以包括在第二计算系统（与计算系统 900 分离）中，第二计算系统可以与计算系统 900 部分类似和 / 或部分不同。在各个实施例中，所示出的模块中的一个或多个可以包括在 IC960 中。

[0170] 计算系统 900 还可以与被配置为存储数据的外部存储设施 980 耦合。在各个实施例中，计算系统 900 可以与网络 984 操作耦合，通过网络 984，计算系统 900 可以与存储设施 980 和 / 或一个或多个其它计算系统（图 9 中未示出）操作耦合。在各个实施例中，计算系统 900 可以在存储设施 980 中存储数据（例如，先前所讨论的一个或多个表格）。尽管未在图 9 中示出，但是在各个实施例中，计算系统 900 可以通过网络 984 来访问 IC960、和 / 或与 IC960 操作耦合并被配置为执行 IC960 的一个或多个测试的测试设备（未在图 9 中示出）。

[0171] 在一些实施例中，处理器 910 可以是通用目的处理器。在一些其他实施例中，处理器 910 可以是特定应用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或构建特定功能或将特定功能直接编程至其中的一些其它逻辑设备。

[0172] 存储器 914 可以是硬驱动、固态驱动、随机访问存储器 (RAM)、或一些其它适合类型的存储器。在各个实施例中，多个编程指令可以存储在存储器 914 或其它存储器中，并被配置为对处理器 910 编程以具有根据本公开的各种特征（例如，方法、程序、功能、操作和 / 或模块）的功能。

[0173] 尽管未在图 9 中示出，但是计算系统 900 可以包括本领域技术人员已知的一个或多个组件。例如，计算系统 900 可以包括 :一个或多个适合的驱动、存储介质、通过其输入命令和数据的用户输入设备（例如，电子数字转换器、麦克风、键盘和通常被称为鼠标、轨迹球、触摸板、操纵杆、游戏面板、圆盘式卫星天线、扫描仪等的指向设备）、一个或多个接口（例如，并口、游戏端口、通用串行总线 (USB) 接口）等，并且可与一个或多个外设（例如，扬声器、打印机等）耦合。计算系统 900 可以使用与诸如同网络接口连接的远程计算机（如，个人计算机、服务器、路由器、网络 PC、对等设备或其它普通网络节点等）之类的一个或多个计算机的逻辑连接，在联网环境下（例如，广域网 WAN、局域网 LAN、内联网、因特网等）操作。

[0174] 图 10 示出了根据本公开的各个实施例设置的示例计算程序产品 1001。在各个实施例中，计算程序产品 1001 可以包括编程指令存储其中的信号承载介质 1003。在各个实施例中，信号承载介质 1003 可以包括计算机可读介质 1007，包括但不限于 CD、DVD、固态驱动、硬驱动、计算机盘、闪存或其它适合类型的计算可读介质。在各个实施例中，信号承载介质 1003 还可以包括可记录介质 1009，包括但不限于软盘、硬驱动、CD、DVD、数字带、计算机存储器、闪存或其它适合类型的计算可记录介质。在各个实施例中，信号承载介质 1003 可

以包括通信介质 1011，包括但不限于光纤电缆、波导、有线或无线通信链路等。

[0175] 例如，计算编程产品 1001 可以用于确定包括在可以与计算产品 1001 耦合的 IC 中的一个或多个电路元件的一个或多个比例因子，和 / 或针对该 IC 产生 ID。实施例不限于任何类型的计算程序产品。

[0176] 信号承载介质 1003 可以包含一个或多个指令 1005，被配置为实践本公开的一个或多个方面。实施例可以具有图 10 中描述的指令中的一些或全部。计算程序产品 1001 的实施例可以具有根据在本说明书的范围内描述的实施例的其它指令。

[0177] 在一些实施例中，一个或多个指令 1005 可以包括用于向在 IC 中包括的一个或多个电路元件应用多个输入矢量的指令。在各个实施例中，一个或多个指令 1005 可以包括响应于应用多个输入矢量来测量 IC 的一个或多个属性的多个值的指令，其中响应于应用相应的输入矢量来测量属性的各个值。在一些实施例中，一个或多个指令 1005 可以包括基于相应的多个测量值来形成多个等式的指令，其中各个等式包括相应的一个或多个电路元件的一个或多个比例因子。在各个实施例中，一个或多个指令 1005 可以包括用于对多个等式进行求解以确定一个或多个比例因子的指令。在一些实施例中，一个或多个指令 1005 可以包括用于对所确定的一个或多个比例因子进行变换以产生 IC 的标识号的指令。在各个实施例中，一个或多个指令 1005 可以包括用于对所产生的标识的冲突概率进行估计的指令。在一些实施例中，一个或多个指令 1005 可以包括通过对至少部分地基于向 IC 应用或应用了相应的多个输入矢量而获得的 IC 的属性的相应多个测量来形成的多个等式进行求解，以确定 IC 的相应多个电路元件的多个比例因子的指令。在各个实施例中，一个或多个指令 1005 可以包括用于对所确定的比例因子进行变换以产生 IC 的标识号的指令。

[0178] 所要求保护的主旨在范围上并不限于这里所描述的特定实施方式。例如，一些实施方式可以是硬件，如用于在设备或设备的组合上操作，而其它实施方式可以是软件和 / 或固件。同样，尽管所要求保护的主旨在范围上不限于此，但是一些实施方式可以包括一个或多个物品，如存储介质或存储媒介。例如，该存储媒介（如 CD-ROM、计算机盘、闪存等）可以具有存储于其上的指令，当由诸如计算机系统、计算平台或其它系统之类的系统来执行指令时，会导致根据所要求保护的主旨的处理器的执行，如先前所描述的实施方式之一。作为一种可能，计算平台可以包括一个或多个处理单元或处理器、一个或多个输入 / 输出设备（如显示器、键盘和 / 鼠标）、以及诸如静态随机访问存储器、动态随机访问存储器、闪存和 / 或硬驱动之类的一个或多个存储器。

[0179] 在说明书中对“实施方式”、“一种实施方式”、“一些实施方式”或“其它实施方式”的引用可以意味着，结合一个或多个实施方式描述的特定特征、结构或特性可以包括在至少一些实施方式中，但不必包括在所有实施方式中。在前面的描述中的“实施方式”、“一种实施方式”、“一些实施方式”或“其它实施方式”的出现不必全部指相同的实施方式。此外，当在此或在所附权利要求中使用诸如“耦合”或“响应”或“响应于”或“与 ... 通信”之类的术语或词时，应广义地对这些术语进行解释。例如，词“与 ... 耦合”可以指与使用了该词的上下文相适合的通信、电气和 / 或操作耦合。

[0180] 在前面的描述中，已经描述了所要求保护的主旨的各个方面。为了解释的目的，特定数字、系统和 / 或配置提供了对所要求保护的主旨的全面理解。然而，本领域技术人员显而易见的并且本公开的益处是，可以在没有这些特定细节的情况下实践所要求保护的主

旨。在其它实例中，省略和 / 或简化了公知特征，以使所要求保护的主旨更加明确。尽管这里示出和 / 或描述了特定特征，但是现在或将来，本领域技术人员可以做出许多修改、替换、改变和 / 或等同物。因而，将会理解，所附权利要求意在覆盖在所要求保护的主旨的真实精神之内的所有这种修改和 / 或改变。

[0181] 在系统方案的硬件和软件实现方式之间存在一些小差别；硬件或软件的使用一般（但并非总是，因为在特定情况下硬件和软件之间的选择可能变得很重要）是一种体现成本与效率之间权衡的设计选择。可以各种手段（例如，硬件、软件和 / 或固件）来实施这里所描述的工艺和 / 或系统和 / 或其他技术，并且优选的工艺将随着所述工艺和 / 或系统和 / 或其他技术所应用的环境而改变。例如，如果实现方确定速度和准确性是最重要的，则实现方可以选择主要为硬件和 / 或固件的手段；如果灵活性是最重要的，则实现方可以选择主要是软件的实施方式；或者，同样也是可选地，实现方可以选择硬件、软件和 / 或固件的特定组合。

[0182] 以上的详细描述通过使用方框图、流程图和 / 或示例，已经阐述了设备和 / 或工艺的众多实施例。在这种方框图、流程图和 / 或示例包含一个或多个功能和 / 或操作的情况下，本领域技术人员应理解，这种方框图、流程图或示例中的每一功能和 / 或操作可以通过各种硬件、软件、固件或实质上它们的任意组合来单独和 / 或共同实现。在一个实施例中，本公开所述主题的若干部分可以通过专用集成电路 (ASIC)、现场可编程门阵列 (FPGA)、数字信号处理器 (DSP)、或其他集成格式来实现。然而，本领域技术人员应认识到，这里所公开的实施例的一些方面在整体上或部分地可以等同地实现在集成电路中，实现为在一台或多台计算机上运行的一个或多个计算机程序（例如，实现为在一台或多台计算机系统上运行的一个或多个程序），实现为在一个或多个处理器上运行的一个或多个程序（例如，实现为在一个或多个微处理器上运行的一个或多个程序），实现为固件，或者实质上实现为上述方式的任意组合，并且本领域技术人员根据本公开，将具备设计电路和 / 或写入软件和 / 或固件代码的能力。此外，本领域技术人员将认识到，本公开所述主题的机制能够作为多种形式的程序产品进行分发，并且无论实际用来执行分发的信号承载介质的具体类型如何，本公开所述主题的示例性实施例均适用。信号承载介质的示例包括但不限于：可记录型介质，如软盘、硬盘驱动器、紧致盘 (CD)、数字通用盘 (DVD)、数字磁带、计算机存储器等；以及传输型介质，如数字和 / 或模拟通信介质（例如，光纤光缆、波导、有线通信链路、无线通信链路等）。

[0183] 本领域技术人员应认识到，上文详细描述了设备和 / 或工艺，此后使用工程实践来将所描述的设备和 / 或工艺集成到数据处理系统中是本领域的常用手段。也即，这里所述的设备和 / 或工艺的至少一部分可以通过合理数量的试验而被集成到数据处理系统中。本领域技术人员将认识到，典型的数据处理系统一般包括以下各项中的一项或多项：系统单元外壳；视频显示设备；存储器，如易失性和非易失性存储器；处理器，如微处理器和数字信号处理器；计算实体，如操作系统、驱动程序、图形用户接口、以及应用程序；一个或多个交互设备，如触摸板或屏幕；和 / 或控制系统，包括反馈环和控制电机（例如，用于感测位置和 / 或速度的反馈；用于移动和 / 或调节成分和 / 或数量的控制电机）。典型的数据处理系统可以利用任意合适的商用部件（如数据计算 / 通信和 / 或网络计算 / 通信系统中常用的部件）予以实现。

[0184] 本公开所述的主题有时说明不同部件包含在不同的其他部件内或者不同部件与不同的其他部件相连。应当理解，这样描述的架构只是示例，事实上可以实现许多能够实现相同功能的其他架构。在概念上，有效地“关联”用以实现相同功能的部件的任意设置，从而实现所需功能。因此，这里组合实现具体功能的任意两个部件可以被视为彼此“关联”从而实现所需功能，而无论架构或中间部件如何。同样，任意两个如此关联的部件也可以看作是彼此“可操作地连接”或“可操作地耦合”以实现所需功能，且能够如此关联的任意两个部件也可以被视为彼此“能可操作地耦合”以实现所需功能。能可操作地耦合的具体示例包括但不限于物理上可配对和 / 或物理上交互的部件，和 / 或无线交互和 / 或可无线交互的部件，和 / 或逻辑交互和 / 或可逻辑交互的部件。

[0185] 至于本文中任何关于多数和 / 或单数术语的使用，本领域技术人员可以从多数形式转换为单数形式，和 / 或从单数形式转换为多数形式，以适合具体环境和应用。为清楚起见，在此明确声明单数形式 / 多数形式可互换。

[0186] 本领域技术人员应当理解，一般而言，所使用的术语，特别是所附权利要求中（例如，在所附权利要求的主体部分中）使用的术语，一般地应理解为“开放”术语（例如，术语“包括”应解释为“包括但不限于”，术语“具有”应解释为“至少具有”等）。本领域技术人员还应理解，如果意在所引入的权利要求中标明具体数目，则这种意图将在该权利要求中明确指出，而在没有这种明确标明的情况下，则不存在这种意图。例如，为帮助理解，所附权利要求可能使用了引导短语“至少一个”和“一个或多个”来引入权利要求中的特征。然而，这种短语的使用不应被解释为暗示着由不定冠词“一”或“一个”引入的权利要求特征将包含该特征的任意特定权利要求限制为仅包含一个该特征的实施例，即便是该权利要求既包括引导短语“一个或多个”或“至少一个”又包括不定冠词如“一”或“一个”（例如，“一”和 / 或“一个”应当被解释为意指“至少一个”或“一个或多个”）；在使用定冠词来引入权利要求中的特征时，同样如此。另外，即使明确指出了所引入权利要求特征的具体数目，本领域技术人员应认识到，这种列举应解释为意指至少是所列数目（例如，不存在其他修饰语的短语“两个特征”意指至少两个该特征，或者两个或更多该特征）。另外，在使用类似于“A、B 和 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B 和 C 中至少一个的系统”应包括但不限于单独具有 A、单独具有 B、单独具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和 / 或具有 A、B、C 的系统等）。在使用类似于“A、B 或 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B 或 C 中至少一个的系统”应包括但不限于单独具有 A、单独具有 B、单独具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和 / 或具有 A、B、C 的系统等）。本领域技术人员还应理解，实质上任意表示两个或更多可选项目的转折连词和 / 或短语，无论是在说明书、权利要求书还是附图中，都应被理解为给出了包括这些项目之一、这些项目任一方、或两个项目的可能性。例如，短语“A 或 B”应当被理解为包括“A”或“B”、或“A 和 B”的可能性。

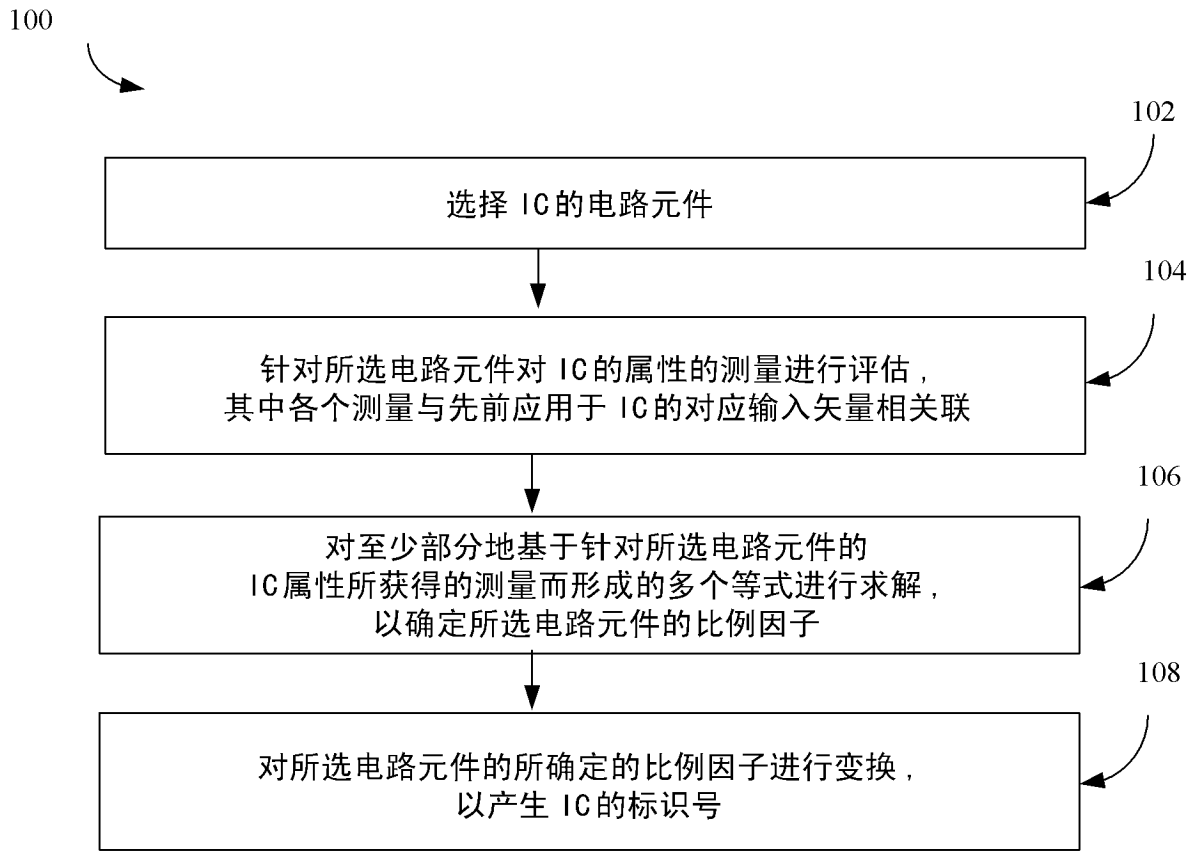
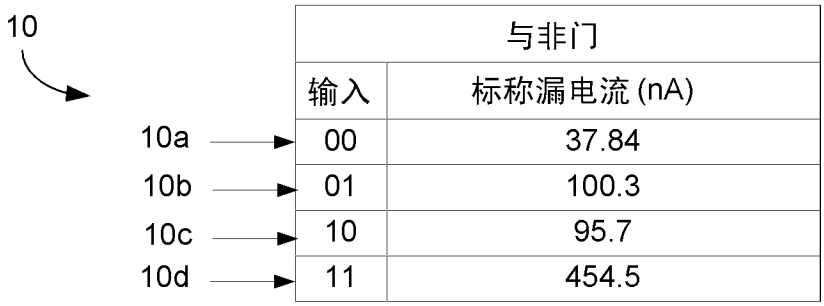



图 1




| 与非门 | |
|---|---|
| 输入 | 标称漏电流 (nA) |
| 00 | 37.84 |
| 01 | 100.3 |
| 10 | 95.7 |
| 11 | 454.5 |

图 2a

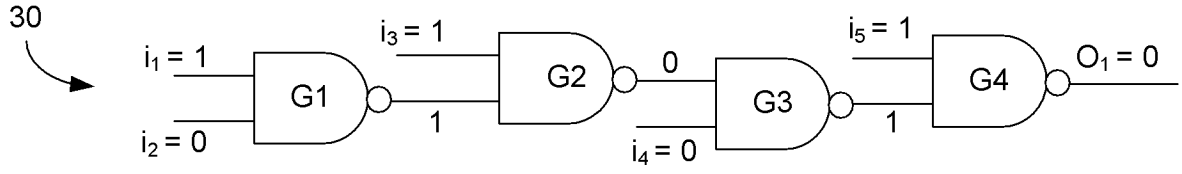



图 2b

50

| | 门 | 比例因子 | |
|---|---|---|---|
| | | IC1 | IC2 |
| 50a | G1 | .5 | 2.4 |
| 50b | G2 | 1.3 | 0.6 |
| 50c | G3 | 2.1 | 4 |
| 50d | G4 | 3 | 0.9 |

图 2c

70

| | 输入矢量 | 总漏电流 (nA) | |
|---|---|---|---|
| | | IC1 | IC2 |
| 70a | 00011 | 1391 | 2055 |
| 70b | 10101 | 2082 | 1063 |
| 70c | 01110 | 1243 | 2150 |
| 70d | 11001 | 1841 | 1905 |

图 2d

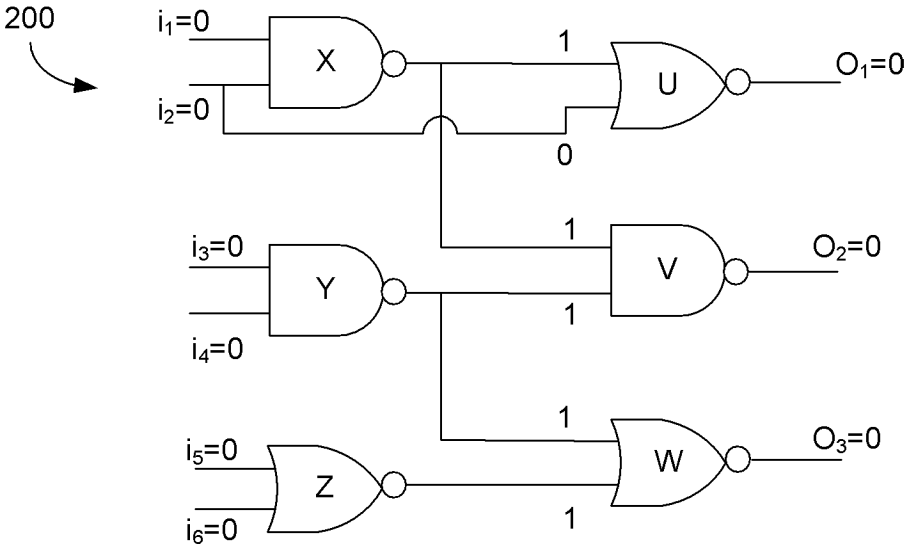



图 3a

240

| | 输入 | 标称漏电流 (nA) | |
|---|---|---|---|
| | | 与非 | 或非 |
| 240a | 00 | 37.84 | 250.6 |
| 240b | 01 | 100.3 | 227.2 |
| 240c | 10 | 95.7 | 213 |
| 240d | 11 | 454.5 | 92.05 |

图 3b

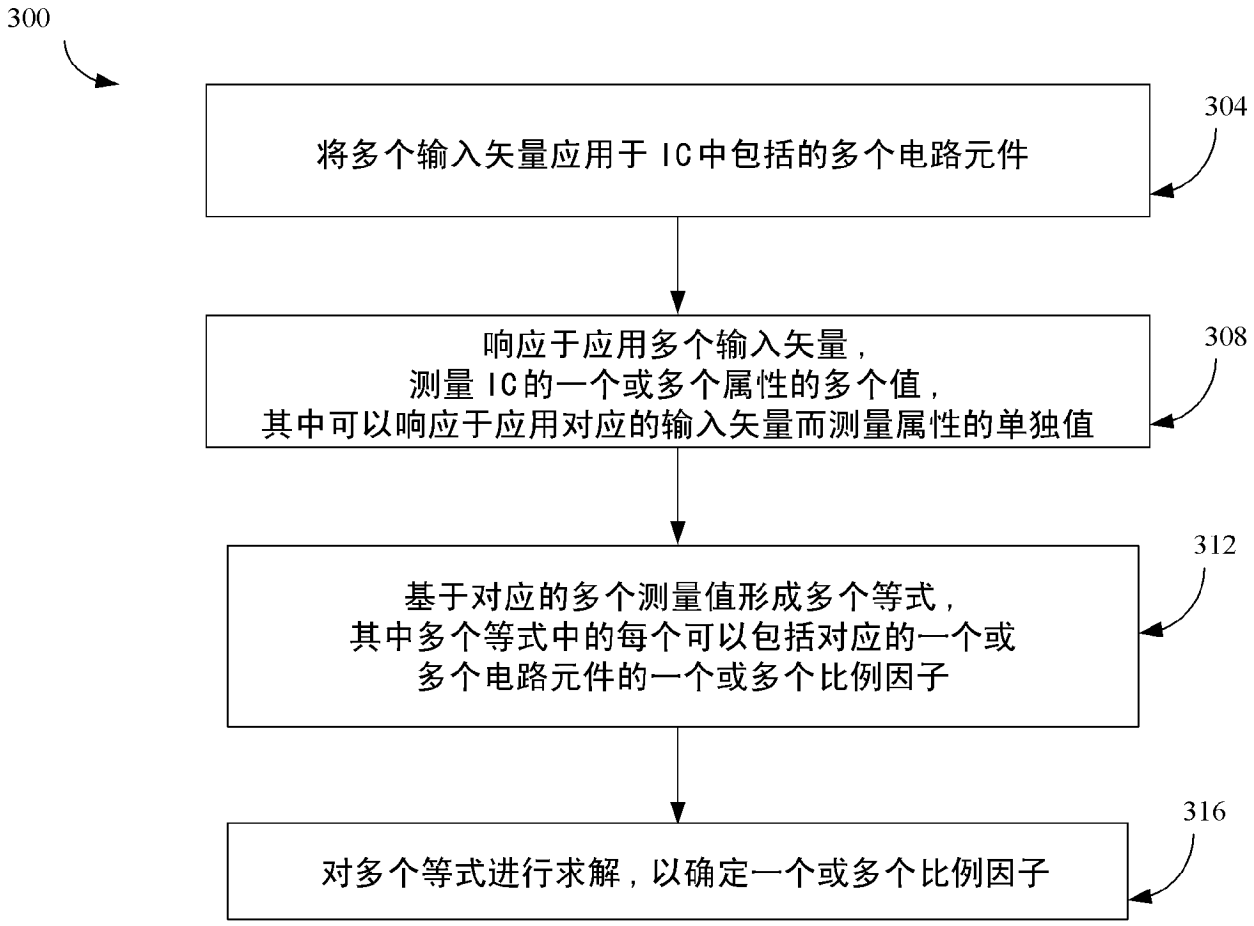



图 4

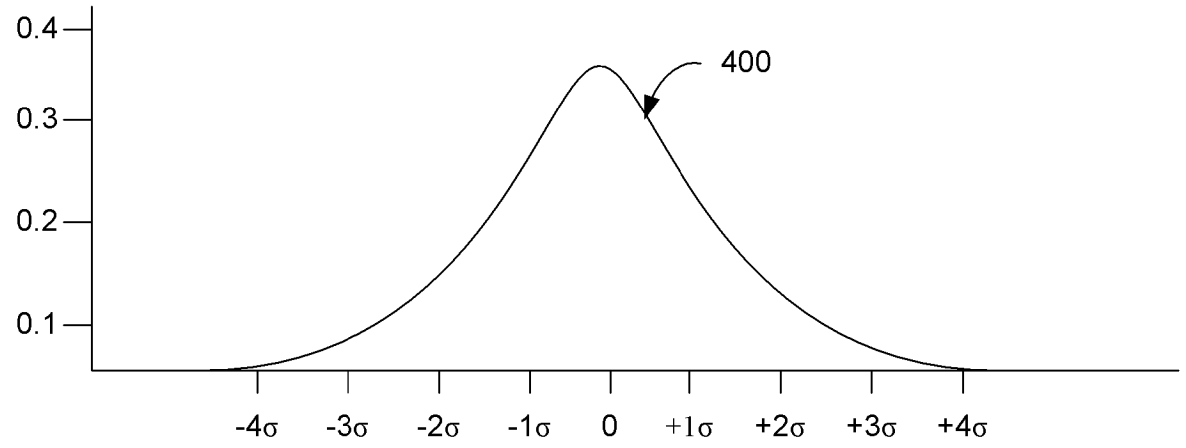

0.4
0.3
0.2
0.1
400
-4σ
-3σ
-2σ
-1σ
0
+1σ
+2σ
+3σ
+4σ

图 5

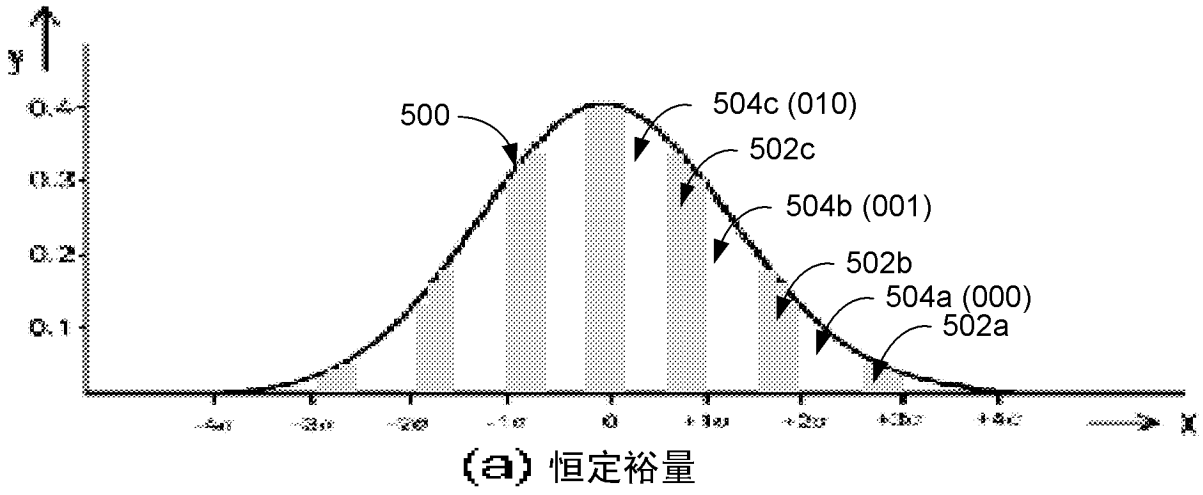

y
x
500
504c (010)
502c
504b (001)
502b
504a (000)
502a
(a) 恒定裕量

图 6a

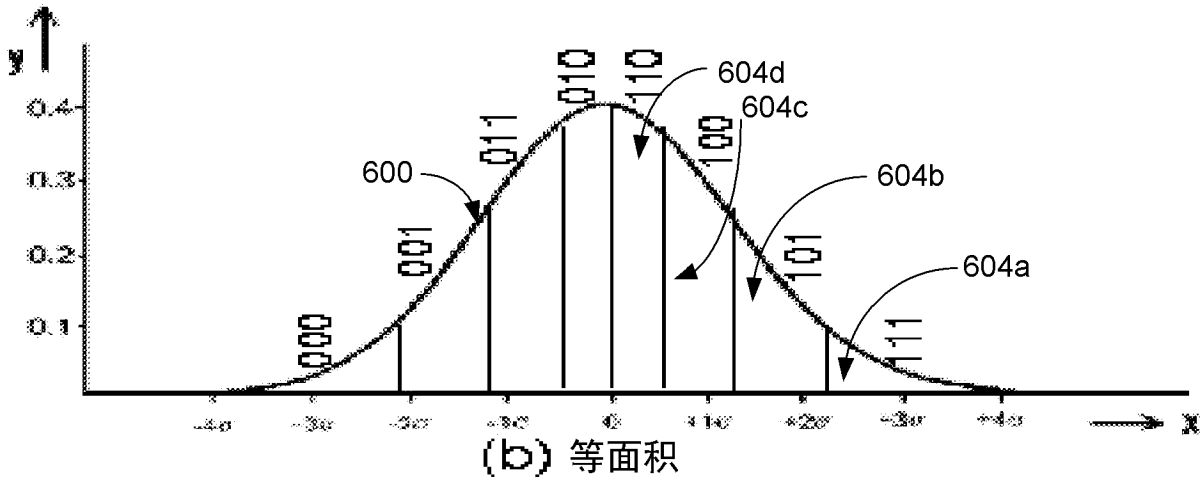

y
x
600
000
001
011
010
110
100
101
111
604d
604c
604b
604a
(b) 等面积

图 7a

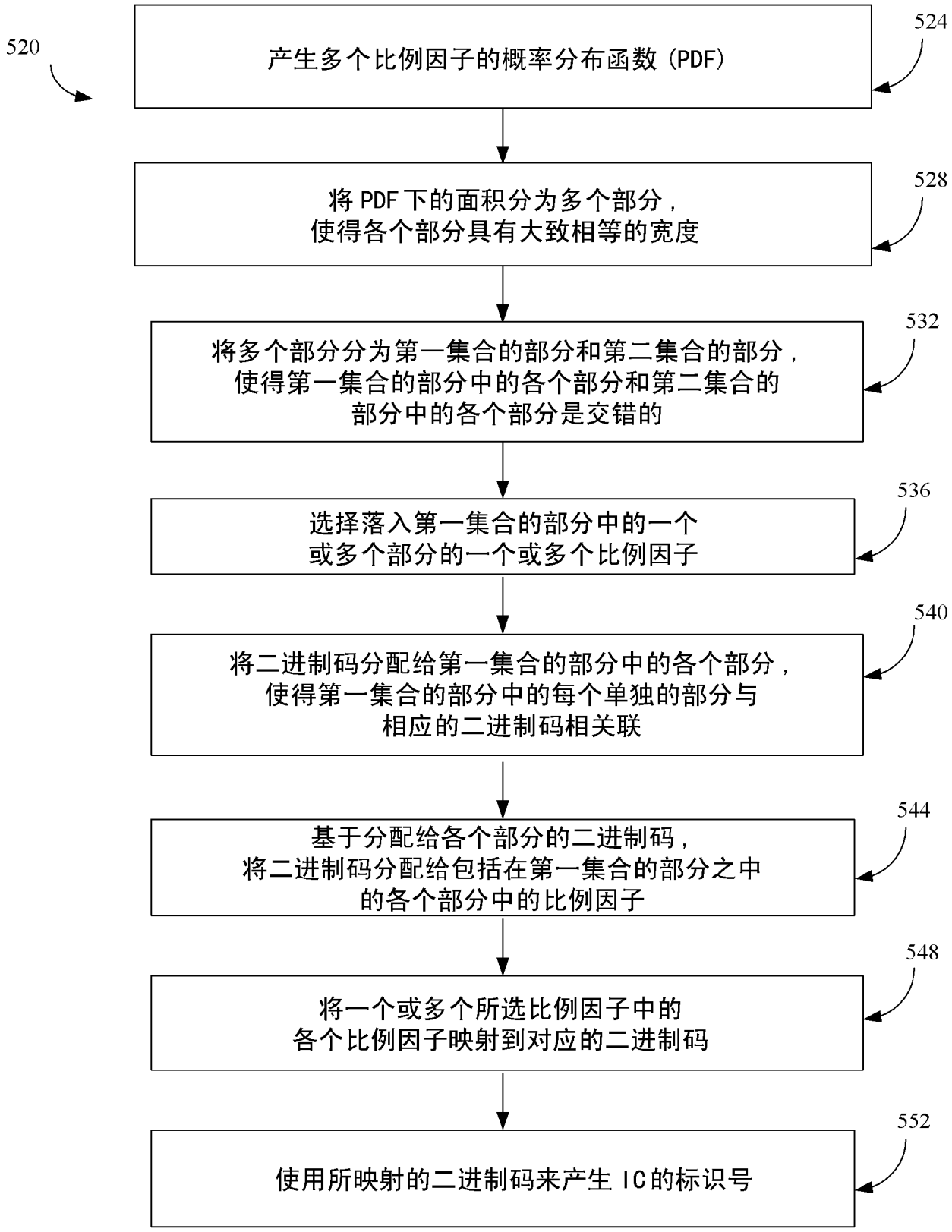

520
产生多个比例因子的概率分布函数（PDF）
524
将 PDF 下的面积分为多个部分，
使得各个部分具有大致相等的宽度
528
将多个部分分为第一集合的部分和第二集合的部分，
使得第一集合的部分中的各个部分和第二集合的
部分中的各个部分是交错的
532
选择落入第一集合的部分中的一个
或多个部分的一个或多个比例因子
536
将二进制码分配给第一集合的部分中的各个部分，
使得第一集合的部分中的每个单独的部分与
相应的二进制码相关联
540
基于分配给各个部分的二进制码，
将二进制码分配给包括在第一集合的部分之中
的各个部分中的比例因子
544
将一个或多个所选比例因子中的
各个比例因子映射到对应的二进制码
548
使用所映射的二进制码来产生 IC 的标识号
552

图 6b

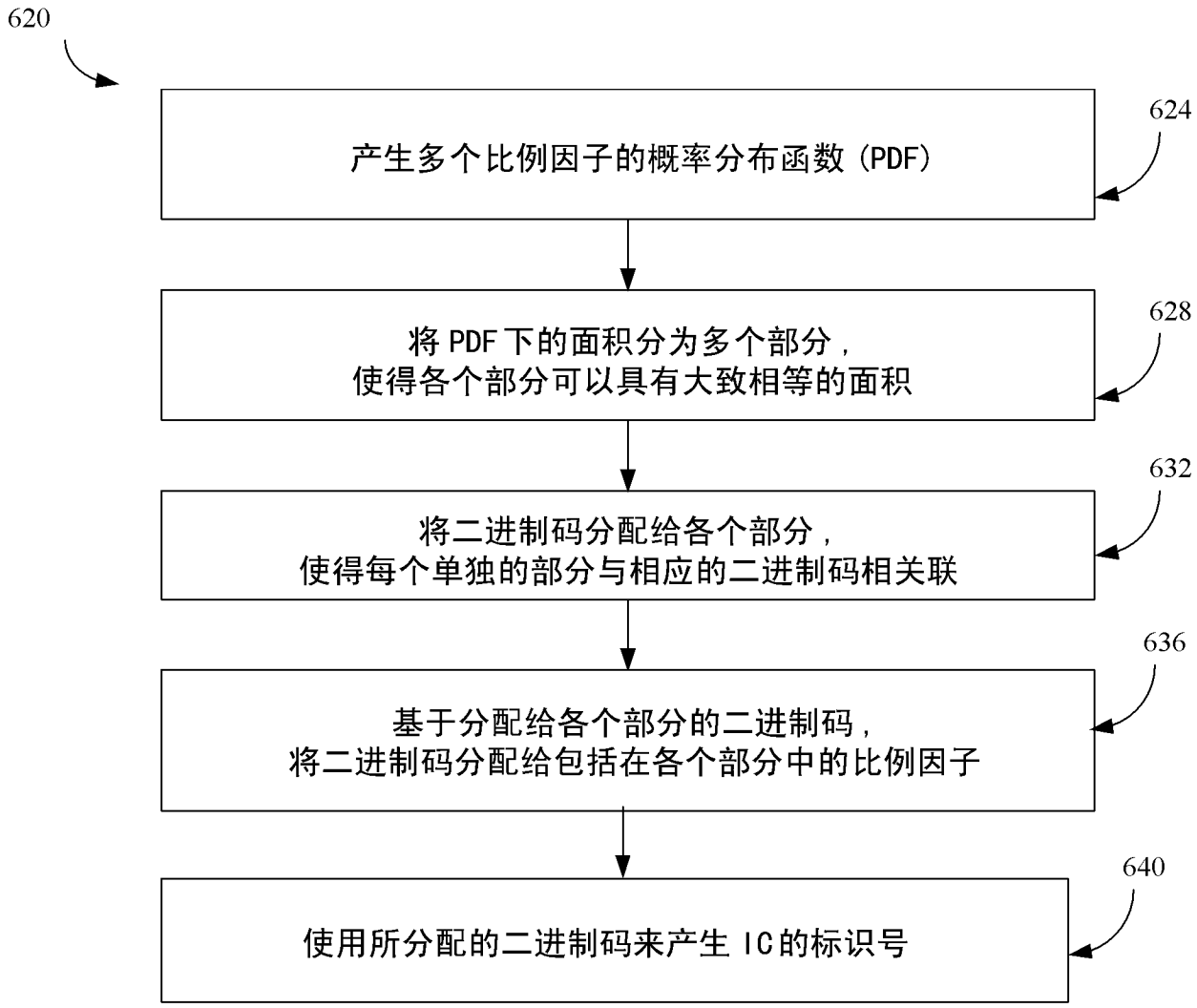

620
产生多个比例因子的概率分布函数（PDF）
624
将 PDF 下的面积分为多个部分，
使得各个部分可以具有大致相等的面积
628
将二进制码分配给各个部分，
使得每个单独的部分与相应的二进制码相关联
632
基于分配给各个部分的二进制码，
将二进制码分配给包括在各个部分中的比例因子
636
使用所分配的二进制码来产生 IC 的标识号
640

图 7b

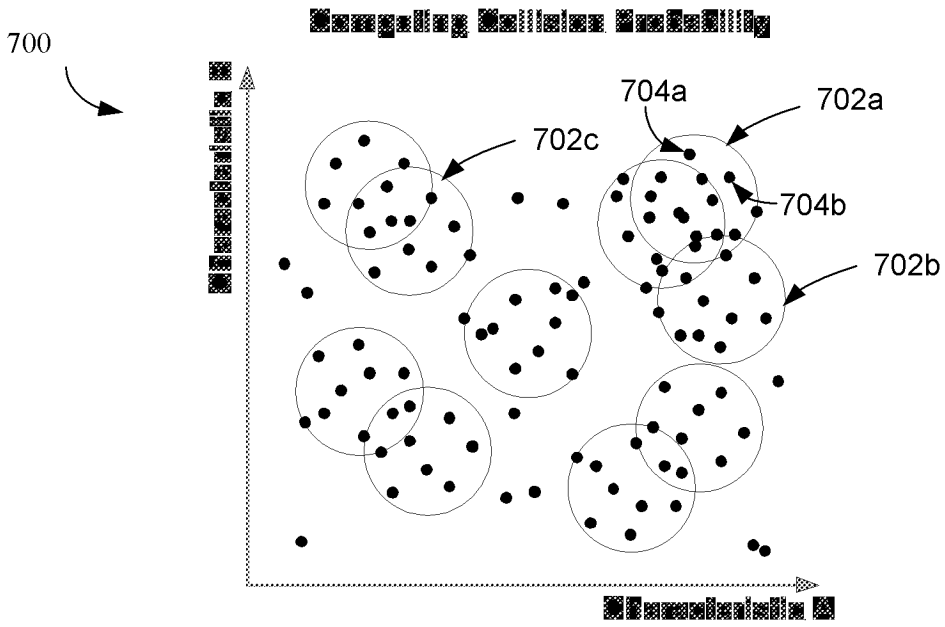



图 8

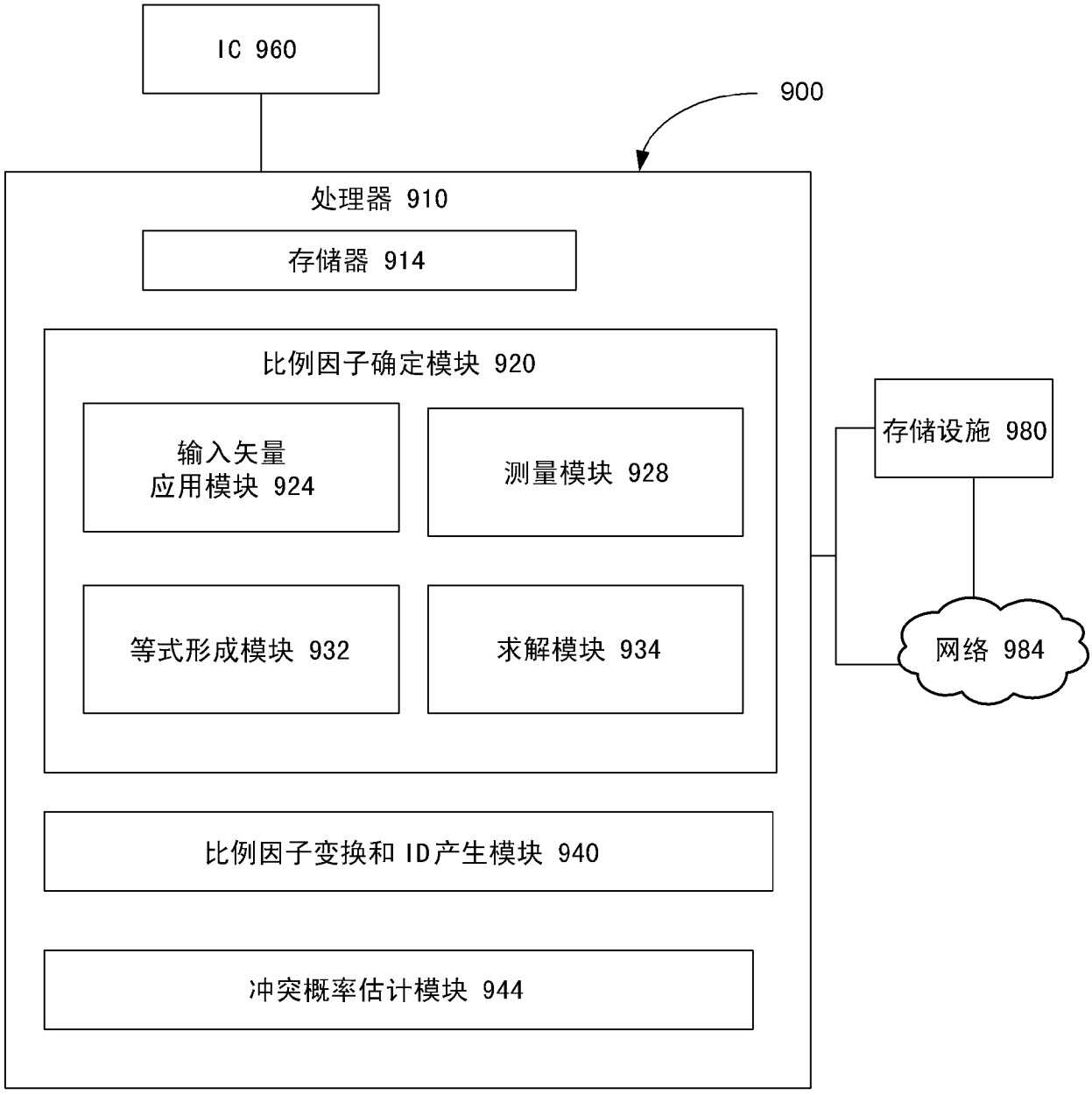

IC 960
900
处理器 910
存储器 914
比例因子确定模块 920
输入矢量
应用模块 924
测量模块 928
等式形成模块 932
求解模块 934
比例因子变换和 ID产生模块 940
冲突概率估计模块 944
存储设施 980
网络 984

图 9

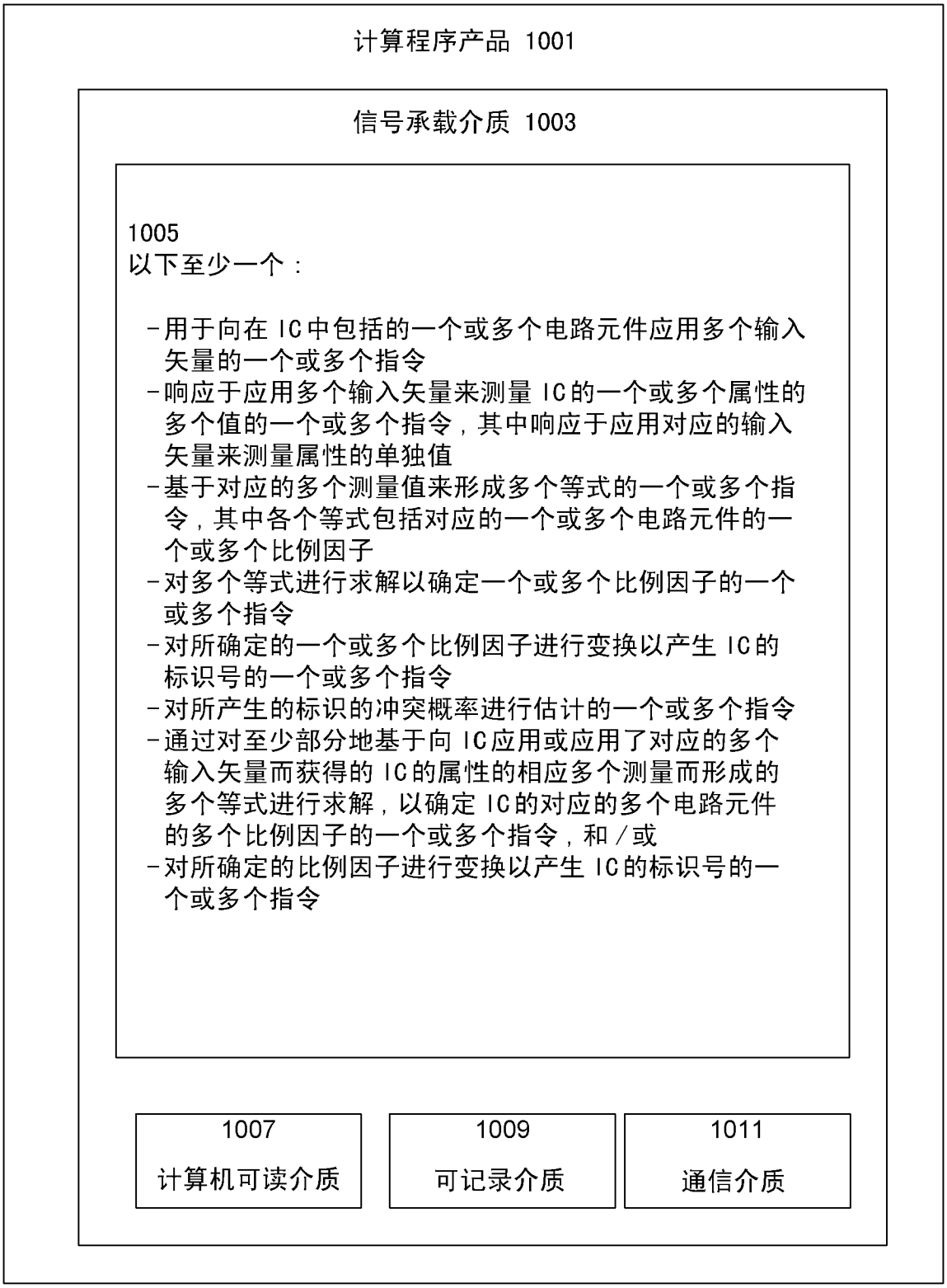

计算程序产品 1001
信号承载介质 1003
1005
以下至少一个：
-用于向在 IC 中包括的一个或多个电路元件应用多个输入矢量的一个或多个指令
-响应于应用多个输入矢量来测量 IC 的一个或多个属性的多个值的一个或多个指令，其中响应于应用对应的输入矢量来测量属性的单独值
-基于对应的多个测量值来形成多个等式的一个或多个指令，其中各个等式包括对应的一个或多个电路元件的一个或多个比例因子
-对多个等式进行求解以确定一个或多个比例因子的一个或多个指令
-对所确定的一个或多个比例因子进行变换以产生 IC 的标识号的一个或多个指令
-对所产生的标识的冲突概率进行估计的一个或多个指令
-通过对至少部分地基于向 IC 应用或应用了对应的多个输入矢量而获得的 IC 的属性的相应多个测量而形成的多个等式进行求解，以确定 IC 的对应的多个电路元件的多个比例因子的一个或多个指令，和 / 或
-对所确定的比例因子进行变换以产生 IC 的标识号的一个或多个指令
1007
计算机可读介质
1009
可记录介质
1011
通信介质

图 10