



(12) 发明专利

(10) 授权公告号 CN 109475327 B

(45) 授权公告日 2023. 01. 24

(21) 申请号 201780028643.9

(22) 申请日 2017.03.07

(65) 同一申请的已公布的文献号  
申请公布号 CN 109475327 A

(43) 申请公布日 2019.03.15

(30) 优先权数据  
62/305,173 2016.03.08 US

(85) PCT国际申请进入国家阶段日  
2018.11.08

(86) PCT国际申请的申请数据  
PCT/US2017/021117 2017.03.07

(87) PCT国际申请的公布数据  
W02017/155967 EN 2017.09.14

(73) 专利权人 达斯特一致有限责任公司  
地址 美国马萨诸塞州

(72) 发明人 O·高尔顿 J·霍奇

(74) 专利代理机构 北京林达刘知识产权代理事  
务所(普通合伙) 11277  
专利代理师 刘新宇

(51) Int.Cl.  
A61B 5/11 (2006.01)

审查员 林晨

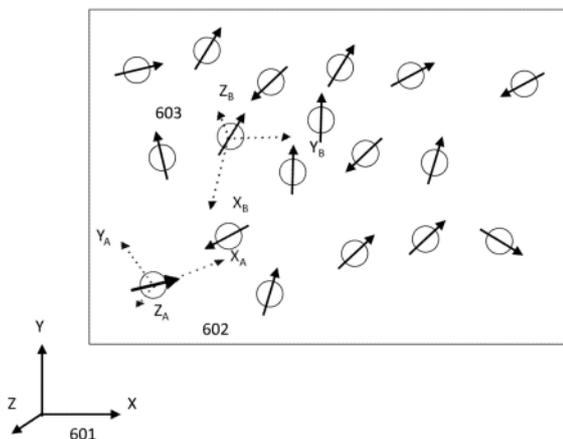
权利要求书10页 说明书26页 附图18页

(54) 发明名称

根据取向信息生成唯一码

(57) 摘要

在一般方面,使用取向信息来生成唯一码。在一些方面,从对象提取取向信息。对象包括多个元素,并且取向信息指示各个元素的相对空间取向。例如,可以通过用于检测元素的扫描器系统提取取向信息。基于取向信息来针对对象生成唯一码。在一些示例中,元素是各自具有一个或多个色心的金刚石颗粒,并且通过检测色心来提取取向信息。



1. 一种用于生成对象的唯一码的方法,包括:  
接收包含元素的对象;  
从所述对象提取取向信息,所述取向信息指示各个元素相对于彼此的相对空间取向,所述取向信息是被用于检测所述元素的扫描器系统提取的,所述元素具有限定该元素的取向的内部或外部结构;以及  
基于所述取向信息来生成所述对象的唯一码。
2. 根据权利要求1所述的方法,其中,提取所述取向信息包括:获得对施加到所述对象的照射的光学响应。
3. 根据权利要求1所述的方法,其中,提取所述取向信息包括:获得对施加到所述对象的照射的荧光响应。
4. 根据权利要求3所述的方法,其中,提取所述取向信息包括:  
获得所述对象的荧光图像;以及  
根据所述荧光图像确定各个元素相对于彼此的相对空间取向。
5. 根据权利要求3所述的方法,其中,获得对照射的光学响应包括:检测所述元素的响应于所述照射的变化的荧光变化,并且基于所检测到的荧光变化来确定所述相对空间取向。
6. 根据权利要求3所述的方法,其中,根据所述取向信息生成的所述唯一码独立于所述照射施加到所述对象的任何角度。
7. 根据权利要求1所述的方法,其中,提取所述取向信息包括:  
获得对施加到所述对象的振荡电磁场的磁共振响应;以及  
基于所述磁共振响应来确定所述相对空间取向。
8. 根据权利要求7所述的方法,其中,获得所述磁共振响应包括:  
将所述对象定位在外部磁场中;  
将所述振荡电磁场施加到所述外部磁场中的所述对象;以及  
光学地检测所述元素的响应于所述外部磁场和所述振荡电磁场至少之一的相对变化的磁共振变化。
9. 根据权利要求1所述的方法,其中,所述对象包括元素的超集,所述方法还包括:  
提取指示所述超集中的仅元素子集的相对空间取向的取向信息;以及  
基于仅所述元素子集的相对空间取向来生成所述唯一码。
10. 根据权利要求1所述的方法,其中,所述对象包括元素的超集,所述方法还包括:  
提取指示所述超集中的所有元素的相对空间取向的取向信息;  
识别指示所述超集中的元素子集的相对空间取向的所述取向信息的子集;以及  
基于仅所述元素子集的相对空间取向来生成所述唯一码。
11. 根据权利要求1至10中任一项所述的方法,其中,所述取向信息是独立于所述对象相对于所述扫描器系统的配准而提取的。
12. 根据权利要求1至10中任一项所述的方法,其中,所述元素是晶体颗粒,并且所述对象包括固定在介质中的所述晶体颗粒。
13. 根据权利要求12所述的方法,其中,所述晶体颗粒是各自包含色心的金刚石颗粒,并且提取所述取向信息包括:检测所述色心的相对取向。

14. 根据权利要求1至10中任一项所述的方法,还包括:  
从所述对象提取位置信息,所述位置信息指示各个元素相对于彼此的相对空间位置;  
以及  
基于所述取向信息和所述位置信息来生成所述对象的唯一码。
15. 根据权利要求1至10中任一项所述的方法,还包括:  
从所述对象提取地形信息,所述地形信息指示各个元素相对于彼此的相对空间地形;  
以及  
基于所述取向信息和所述地形信息来生成所述对象的唯一码。
16. 根据权利要求1至10中任一项所述的方法,还包括:  
从所述对象提取磁环境信息,所述磁环境信息指示各个元素的磁环境;以及  
基于所述取向信息和所述磁环境信息来生成所述对象的唯一码。
17. 根据权利要求1至10中任一项所述的方法,其中,所述取向信息指示所述元素在三维坐标空间中的相对空间取向。
18. 根据权利要求1至10中任一项所述的方法,其中,所述取向信息指示所述元素在二维坐标空间中的相对空间取向。
19. 根据权利要求1至10中任一项所述的方法,其中,所述唯一码包括第一唯一码,并且所述方法还包括:  
通过修改所述对象来改变所述元素中的至少一些元素的相对空间取向;以及  
基于在改变相对空间取向之后从所述对象提取的取向信息,来生成所述对象的不同的第二唯一码。
20. 根据权利要求19所述的方法,还包括:使用所述相对空间取向作为与所述对象有关的信息的分类帐。
21. 根据权利要求1至10中任一项所述的方法,还包括:利用具有所述相对空间取向的元素形成所述对象。
22. 根据权利要求1至10中任一项所述的方法,其中,所述取向信息包括描述各个元素相对于彼此的相对空间取向的坐标变换的列表。
23. 根据权利要求1至10中任一项所述的方法,其中,所述取向信息以对所述对象的坐标系全局旋转不变的格式指示所述相对空间取向。
24. 一种扫描器系统,包括:  
样本区域,其被配置为接收包括元素的对象;  
探测器,其被配置为通过相对于彼此来检测所述元素来从所述对象提取取向信息,所述取向信息指示各个元素相对于彼此的相对空间取向,所述元素具有限定该元素的取向的内部或外部结构;以及  
处理器,其被配置为基于所述取向信息来生成所述对象的唯一码。
25. 根据权利要求24所述的扫描器系统,其中,所述探测器包括光学成像系统,并且提取所述取向信息包括:获得对施加到所述对象的照射的光学响应。
26. 根据权利要求24所述的扫描器系统,其中,所述探测器包括磁共振系统,并且提取所述取向信息包括:获得对施加到所述对象的振荡电磁场的磁共振响应。
27. 根据权利要求24所述的扫描器系统,其中,根据所述取向信息生成的所述唯一码独

立于照射施加到所述对象的任何角度。

28. 根据权利要求24所述的扫描器系统,其中,所述对象包括元素的超集,并且所述唯一码是基于仅所述元素的子集的相对空间取向生成的。

29. 根据权利要求24所述的扫描器系统,其中,所述元素是各自包含色心的金刚石颗粒,并且所述探测器被配置为通过检测所述色心的相对取向来提取所述取向信息。

30. 根据权利要求24所述的扫描器系统,其中,所述探测器被配置为从所述对象提取元素信息,并且所述处理器被配置为基于所述元素信息来生成所述对象的唯一码,所述元素信息包括所述取向信息以及以下至少之一:

指示各个元素相对于彼此的相对空间位置的位置信息;

指示各个元素相对于彼此的相对空间地形的地形信息;以及

指示各个元素的磁环境的磁环境信息。

31. 一种用于生成对象的唯一码的方法,包括:

获得从对象提取的取向信息,所述取向信息指示所述对象中的各个元素相对于彼此的相对空间取向,所述元素具有限定该元素的取向的内部或外部结构;以及

通过一个或多个处理器的操作,根据所述取向信息生成所述对象的唯一码。

32. 根据权利要求31所述的方法,还包括:

获得从所述对象提取的位置信息,所述位置信息指示所述元素相对于彼此的相对空间位置;以及

通过一个或多个处理器的操作,根据所述取向信息和所述位置信息生成所述唯一码。

33. 根据权利要求31所述的方法,还包括:

获得从所述对象提取的地形信息,所述地形信息指示所述元素的相对空间地形;以及通过一个或多个处理器的操作,根据所述取向信息和所述地形信息生成所述唯一码。

34. 根据权利要求31所述的方法,还包括:

获得从所述对象提取的磁环境信息,所述磁环境信息指示所述元素的磁环境;以及

通过一个或多个处理器的操作,根据所述取向信息和所述磁环境信息生成所述唯一码。

35. 根据权利要求31所述的方法,还包括:将所述唯一码用在挑战-响应协议中。

36. 根据权利要求35所述的方法,其中,基于所述挑战-响应协议的挑战数据提取所述取向信息,使用所述唯一码来生成所述挑战-响应协议的响应数据,并且所述方法还包括:将所述响应数据发送至认证器。

37. 根据权利要求31所述的方法,还包括:将所述唯一码用在认证过程中。

38. 根据权利要求37所述的方法,还包括:执行所述认证过程以认证所述对象的来源。

39. 根据权利要求37所述的方法,还包括:执行所述认证过程以验证所述对象的完整性。

40. 根据权利要求37所述的方法,还包括:执行所述认证过程以验证所述对象的监管链。

41. 根据权利要求37所述的方法,还包括:执行所述认证过程以跟踪所述对象的监管。

42. 根据权利要求31所述的方法,还包括:将所述唯一码用在加密过程中。

43. 根据权利要求42所述的方法,还包括:使用所述唯一码来获得加密协议的密钥。

44. 根据权利要求42所述的方法,还包括:使用所述唯一码来获得数字签名协议的秘密密钥。

45. 根据权利要求31至44中任一项所述的方法,还包括:通过用于检测所述元素的扫描器系统的操作来提取所述取向信息。

46. 根据权利要求31至44中任一项所述的方法,其中,提取所述取向信息包括:获得对施加到所述对象的照射的光学响应。

47. 根据权利要求31至44中任一项所述的方法,其中,通过所述元素的光学检测到的磁共振来提取所述取向信息。

48. 根据权利要求31至44中任一项所述的方法,其中,所述对象包括元素的超集,所述取向信息指示所述超集中的仅元素子集的相对空间取向,并且基于仅所述元素子集的相对空间取向来生成所述唯一码。

49. 根据权利要求31至44中任一项所述的方法,其中,所述对象包括元素的超集,所述取向信息指示所述超集中的所有元素的相对空间取向,并且所述方法还包括:

识别指示所述元素子集相对于彼此的相对空间取向的所述取向信息的子集;以及  
基于仅元素子集相对于彼此的相对空间取向来生成所述唯一码。

50. 根据权利要求31至44中任一项所述的方法,其中,所述取向信息指示独立于所述对象的任何配准参考的相对空间取向。

51. 根据权利要求31至44中任一项所述的方法,其中,所述元素是金刚石颗粒,并且所述方法还包括:使用所述金刚石颗粒作为物理不可克隆功能即PUF。

52. 根据权利要求31至44中任一项所述的方法,其中,所述元素是各自包含色心的金刚石颗粒,并且所述取向信息指示所述色心的相对空间取向。

53. 根据权利要求52所述的方法,其中,所述取向信息包括描述各个金刚石颗粒的相对空间取向的坐标变换的列表。

54. 根据权利要求53所述的方法,其中,所述列表包括各金刚石颗粒的复合变换矩阵,并且各金刚石颗粒的所述复合变换矩阵表示:

所述对象的坐标系和所述金刚石颗粒的坐标系之间的第一变换;以及  
所述金刚石颗粒的坐标系和所述金刚石颗粒中的色心的坐标系之间的第二变换,  
其中,复合变换矩阵的所述列表对所述对象的坐标系是全局旋转不变的。

55. 一种用于生成对象的唯一码的系统,包括:

数据处理设备;以及

非暂时性计算机可读介质,其存储指令,所述指令在由所述数据处理设备执行的情况下,进行包括以下的操作:

获得从对象提取的取向信息,所述取向信息指示所述对象中的各个元素相对于彼此的相对空间取向,所述元素具有限定该元素的取向的内部或外部结构;以及

根据所述取向信息生成所述对象的唯一码。

56. 根据权利要求55所述的系统,其中,所述唯一码是根据元素信息生成的,所述元素信息包括所述取向信息以及以下至少之一:

指示各个元素相对于彼此的相对空间位置的位置信息;

指示各个元素相对于彼此的相对空间地形的地形信息;以及

指示各个元素的磁环境的磁环境信息。

57. 根据权利要求55所述的系统,所述操作还包括:将所述唯一码用在挑战-响应协议中。

58. 根据权利要求55所述的系统,所述操作还包括:将所述唯一码用在认证过程中。

59. 根据权利要求55所述的系统,所述操作还包括:将所述唯一码用在加密过程中。

60. 根据权利要求55所述的系统,还包括扫描器系统,所述扫描器系统能够操作以从所述对象提取所述取向信息。

61. 根据权利要求55所述的系统,其中,所述对象包括元素的超集,所述取向信息指示所述超集中的仅元素子集的相对空间取向,并且基于仅所述元素子集相对于彼此的相对空间取向来生成所述唯一码。

62. 根据权利要求55所述的系统,其中,所述对象包括元素的超集,所述取向信息指示所述超集中的所有元素相对于彼此的相对空间取向,并且所述操作还包括:

识别指示所述元素的子集相对于彼此的相对空间取向的所述取向信息的子集;以及基于仅元素子集相对于彼此的相对空间取向来生成所述唯一码。

63. 根据权利要求55所述的系统,其中,所述取向信息包括描述各个金刚石颗粒的相对空间取向的坐标变换的列表。

64. 根据权利要求63所述的系统,其中,

所述列表包括各金刚石颗粒的复合变换矩阵,并且各金刚石颗粒的所述复合变换矩阵表示:

所述对象的坐标系和所述金刚石颗粒的坐标系之间的第一变换;以及所述金刚石颗粒的坐标系和所述金刚石颗粒中的色心的坐标系之间的第二变换,其中,复合变换矩阵的所述列表对所述对象的坐标系是全局旋转不变的。

65. 一种用于生成对象的唯一码的方法,包括:

在对象中形成金刚石颗粒的悬浮;以及

使用所述金刚石颗粒相对于彼此的相对空间取向来生成所述对象的唯一码。

66. 根据权利要求65所述的方法,其中,通过将所述金刚石颗粒分布在所述对象的表面来形成所述悬浮。

67. 根据权利要求66所述的方法,其中,将所述金刚石颗粒分布在所述对象的表面包括:将包含所述金刚石颗粒的涂料应用到所述对象的表面。

68. 根据权利要求66所述的方法,其中,将所述金刚石颗粒分布在所述对象的表面包括:将包含所述金刚石颗粒的保形涂层材料应用到所述对象的表面。

69. 根据权利要求65所述的方法,其中,形成所述悬浮包括:

将所述金刚石颗粒分布在材料中;以及

用包含所述金刚石颗粒的所述材料形成所述对象。

70. 根据权利要求69所述的方法,其中,用所述材料形成所述对象包括:通过注射成型工艺形成所述对象。

71. 根据权利要求69所述的方法,其中,用所述材料形成所述对象包括:通过增材制造工艺形成所述对象。

72. 根据权利要求69所述的方法,其中,用所述材料形成所述对象包括:通过打印工艺

形成所述对象。

73. 根据权利要求69所述的方法,其中,用所述材料形成所述对象包括:  
用所述材料形成工件;以及  
从所述工件中去除材料。

74. 根据权利要求65至73中任一项所述的方法,其中,使用所述金刚石颗粒的悬浮来生成所述唯一码包括:

通过扫描器系统的操作,从所述对象提取取向信息,所述取向信息指示所述金刚石颗粒的相对空间取向;以及

通过计算机系统的操作,基于所述取向信息来生成所述对象的所述唯一码。

75. 根据权利要求74所述的方法,其中,所述取向信息包括描述各个金刚石颗粒的相对空间取向的坐标变换的列表。

76. 根据权利要求65至73中任一项所述的方法,还包括:

将所述对象从发送实体发送至接收实体;以及

在所述发送实体和所述接收实体之间执行的认证过程中使用所述唯一码。

77. 根据权利要求76所述的方法,其中,通过中间实体在所述发送实体和所述接收实体之间执行所述认证过程。

78. 根据权利要求65至73中任一项所述的方法,还包括:使用所述金刚石颗粒的悬浮作为物理不可克隆功能即PUF。

79. 根据权利要求65至73中任一项所述的方法,还包括:使用所述金刚石颗粒的悬浮作为与所述对象相关的信息的安全分类帐。

80. 一种用于生成对象的唯一码的系统,包括:

制造系统,其被配置为在对象中形成金刚石颗粒的悬浮;

扫描器系统,其被配置为从所述对象提取颗粒信息,所述颗粒信息指示所述悬浮中的各个金刚石颗粒的性质;以及

计算机系统,其被配置为基于所述颗粒信息中的金刚石颗粒相对于彼此的相对空间取向,生成所述对象的唯一码。

81. 根据权利要求80所述的系统,其中,通过将所述金刚石颗粒分布在所述对象的表面来形成所述悬浮。

82. 根据权利要求80所述的系统,其中,形成所述悬浮包括:

将所述金刚石颗粒分布在材料中;以及

用包含所述金刚石颗粒的所述材料形成所述对象。

83. 根据权利要求80所述的系统,其中,所述颗粒信息包括指示各个金刚石颗粒的相对空间取向的取向信息。

84. 一种生成认证码并进行关联的方法,包括:

接收指示对象中的各个元素相对于彼此的相对空间取向的取向信息,所述元素具有有限定该元素的取向的内部或外部结构;

通过一个或多个处理器的操作,根据所述取向信息生成认证码;以及

使所述认证码与所述对象的对象标识符相关联。

85. 根据权利要求84所述的方法,其中,所述对象包括应用于物品的独特标记物,并且

所述对象标识符包括所述物品的序列号。

86. 根据权利要求85所述的方法,还包括:分发所述物品,并且将所述认证码和所述序列号存储在安全认证数据库中。

87. 根据权利要求86所述的方法,其中,通过扫描器系统的操作来从所述独特标记物提取所述取向信息,并且所述方法还包括:将所述扫描器系统为了提取所述取向信息所使用的扫描器设置存储在所述安全认证数据库中。

88. 根据权利要求85所述的方法,其中,所述独特标记物使得所述物品的接收方能够认证所述物品。

89. 根据权利要求84所述的方法,其中,所述元素是各自包含色心的金刚石颗粒,并且所述方法还包括:通过检测所述色心的相对取向来提取所述取向信息。

90. 根据权利要求89所述的方法,其中,提取所述取向信息包括:获得对施加到所述金刚石颗粒的照射的荧光响应。

91. 根据权利要求89所述的方法,其中,提取所述取向信息包括:获得对施加到所述金刚石颗粒的照射的光学响应。

92. 根据权利要求89所述的方法,其中,通过所述金刚石颗粒的光学检测到的磁共振来提取所述取向信息。

93. 根据权利要求89所述的方法,还包括:将所述认证码和所述对象标识符用在认证过程中以认证所述对象。

94. 一种非暂时性计算机可读介质,其存储指令,所述指令在由数据处理设备执行的情况下能够操作,以进行包括以下的操作:

接收指示对象中的各个元素相对于彼此的相对空间取向的取向信息,所述元素具有限定该元素的取向的内部或外部结构;

根据所述取向信息生成认证码;以及

使所述认证码与所述对象的对象标识符相关联。

95. 根据权利要求94所述的计算机可读介质,其中,所述对象包括应用于物品的独特标记物,并且所述对象标识符包括所述物品的序列号。

96. 根据权利要求94所述的计算机可读介质,其中,通过扫描器系统的操作来从独特标记物提取所述取向信息,并且所述操作还包括:将所述认证码、所述对象标识符和所述扫描器系统为了提取所述取向信息所使用的扫描器设置存储在安全认证数据库中。

97. 根据权利要求94所述的计算机可读介质,所述操作还包括:将所述认证码和所述对象标识符用在认证过程中以认证所述对象。

98. 一种认证方法,包括:

接收对象的对象标识符;

接收所述对象的认证码,所述认证码基于所检测到的所述对象中的各个元素相对于彼此的相对取向,所述元素具有限定该元素的取向的内部或外部结构;以及

通过一个或多个处理器的操作,基于所述认证码和所述对象标识符来认证所述对象。

99. 根据权利要求98所述的方法,其中,所述对象包括应用于物品的独特标记物,并且所述对象标识符包括所述物品的序列号。

100. 根据权利要求98所述的方法,其中,认证所述对象包括:将所述认证码和所述对象

标识符通信至认证器。

101. 根据权利要求98所述的方法,其中,认证所述对象包括:基于安全认证数据库中的信息来评价所述认证码。

102. 根据权利要求98所述的方法,其中,认证所述对象包括:执行认证过程以认证所述对象的来源。

103. 根据权利要求98所述的方法,其中,认证所述对象包括:执行认证过程以认证所述对象的完整性。

104. 根据权利要求98所述的方法,其中,认证所述对象包括:执行认证过程以认证监管链。

105. 根据权利要求98所述的方法,其中,所述元素是各自包含色心的金刚石颗粒,并且所述方法还包括:通过检测所述色心的相对取向来提取取向信息。

106. 根据权利要求105所述的方法,其中,提取所述取向信息包括:获得对施加到所述金刚石颗粒的照射的光学响应。

107. 根据权利要求105所述的方法,其中,通过所述金刚石颗粒的光学检测到的磁共振来提取所述取向信息。

108. 一种非暂时性计算机可读介质,其存储指令,所述指令在由数据处理设备执行的情况下能够操作,以进行包括以下的操作:

接收对象的对象标识符;

接收所述对象的认证码,所述认证码基于所检测到的所述对象中的各个元素相对于彼此的相对取向,所述元素具有限定该元素的取向的内部或外部结构;以及

基于所述认证码和所述对象标识符来认证所述对象。

109. 根据权利要求108所述的计算机可读介质,其中,所述对象包括应用于物品的独特标记物,并且所述对象标识符包括所述物品的序列号。

110. 根据权利要求108所述的计算机可读介质,其中,认证所述对象包括:将所述认证码和所述对象标识符通信至认证器。

111. 根据权利要求108所述的计算机可读介质,其中,认证所述对象包括:基于安全认证数据库中的信息来评价所述认证码。

112. 一种用于生成挑战-响应协议的响应数据的方法,包括:

获得挑战-响应协议的挑战数据;

基于所述挑战数据,通过用于检测对象中的各个元素相对于彼此的相对空间取向的扫描器系统的操作来从所述对象提取取向信息,其中所述挑战数据包括所述扫描器系统为了检测所述相对空间取向所使用的参数,所述元素具有限定该元素的取向的内部或外部结构;以及

通过一个或多个处理器的操作,基于所述取向信息来生成所述挑战-响应协议的响应数据。

113. 根据权利要求112所述的方法,还包括:将所述响应数据发送至验证器,以验证所述挑战-响应协议的所述响应数据。

114. 根据权利要求113所述的方法,还包括:从所述验证器接收基于所述挑战数据和所述响应数据的所述挑战-响应协议的结果。

115. 根据权利要求113所述的方法,其中,获得所述挑战数据包括:从所述验证器接收所述挑战数据。

116. 根据权利要求112所述的方法,其中,获得所述挑战数据包括:在所述扫描器系统处生成所述挑战数据。

117. 一种非暂时性计算机可读介质,其存储指令,所述指令在由数据处理设备执行的情况下能够操作,以进行包括以下的操作:

获得挑战-响应协议的挑战数据;

基于所述挑战数据,通过用于检测对象中的各个元素相对于彼此的相对空间取向的扫描器系统的操作来从所述对象提取取向信息,其中所述挑战数据包括所述扫描器系统为了检测所述相对空间取向所使用的参数,所述元素具有限定该元素的取向的内部或外部结构;以及

基于所述取向信息来生成所述挑战-响应协议的响应数据。

118. 根据权利要求117所述的计算机可读介质,所述操作还包括:将所述响应数据发送至验证器,以验证所述挑战-响应协议的所述响应数据。

119. 根据权利要求117所述的计算机可读介质,所述操作还包括:从验证器接收基于所述挑战数据和所述响应数据的所述挑战-响应协议的结果。

120. 根据权利要求119所述的计算机可读介质,其中,获得所述挑战数据包括:从所述验证器接收所述挑战数据。

121. 根据权利要求117所述的计算机可读介质,其中,获得所述挑战数据包括:在所述扫描器系统处生成所述挑战数据。

122. 一种判断响应数据的有效性的方法,包括:

获得挑战-响应协议的挑战数据和响应数据,所述挑战数据包括用于从对象提取取向信息的参数,所述响应数据基于使用所述参数从所述对象提取的所述取向信息,所述取向信息指示所述对象中的各个元素相对于彼此的相对空间取向,所述元素具有限定该元素的取向的内部或外部结构;以及

通过一个或多个处理器的操作,判断所述响应数据是否表示对所述挑战数据的有效响应。

123. 根据权利要求122所述的方法,其中,判断所述响应数据是否表示对所述挑战数据的有效响应包括:基于安全认证数据库中的有效信息来评价所述取向信息。

124. 根据权利要求123所述的方法,还包括:基于所述挑战数据和所述对象的对象标识符来从所述安全认证数据库获得所述有效信息。

125. 根据权利要求122所述的方法,其中,验证器从远程扫描器系统接收所述挑战数据和所述响应数据,并且所述验证器将所述响应数据是否表示有效响应的指示发送至所述远程扫描器系统。

126. 一种非暂时性计算机可读介质,其存储指令,所述指令在由数据处理设备执行的情况下能够操作,以进行包括以下的操作:

获得挑战-响应协议的挑战数据和响应数据,所述挑战数据包括用于从对象提取取向信息的参数,所述响应数据基于使用所述参数从所述对象提取的所述取向信息,所述取向信息指示所述对象中的各个元素相对于彼此的相对空间取向,所述元素具有限定该元素的

取向的内部或外部结构;以及

通过一个或多个处理器的操作,判断所述响应数据是否表示对所述挑战数据的有效响应。

127. 根据权利要求126所述的计算机可读介质,其中,判断所述响应数据是否表示对所述挑战数据的有效响应包括:基于安全认证数据库中的有效信息来评价所述取向信息。

128. 根据权利要求127所述的计算机可读介质,所述操作还包括:基于所述挑战数据和所述对象的对象标识符来从所述安全认证数据库获得所述有效信息。

129. 根据权利要求126所述的计算机可读介质,其中,验证器从远程扫描器系统接收所述挑战数据和所述响应数据,并且所述验证器将所述响应数据是否表示有效响应的指示发送至所述远程扫描器系统。

## 根据取向信息生成唯一码

[0001] 相关申请的交叉引用

[0002] 本申请要求2016年3月8日提交的标题为“Methods and Systems for Authenticating Objects Using Unique Markers”的美国临时申请62/305,173的优先权，其通过引用而被包含于此。

### 背景技术

[0003] 以下说明涉及根据取向信息生成唯一码。

[0004] 防伪技术、密码协议和其它措施经常用于安全应用。防伪技术的示例包括全息图、荧光染料或工程DNA链。密码协议的示例包括认证方案(例如,数字签名协议、挑战-响应协议)和例如公钥基础设施(PKI)中的加密方案。

### 附图说明

[0005] 图1A示出具有唯一认证标记的示例物品。

[0006] 图1B示意性示出图1A的示例独特标记物。

[0007] 图2A示意性示出包括金刚石晶体的示例颗粒,所述金刚石晶体包含缺陷中心。

[0008] 图2B示意性示出图2A的示例金刚石晶格中的NV缺陷中心。

[0009] 图3示意性示出在独特标记物中、主体材料中或上颗粒的示例随机分布。

[0010] 图4示意性示出用于测量独特标记物中的颗粒的位置和取向的示例扫描器系统。

[0011] 图5示出从荧光扫描获得的示例图像中的颗粒位置。

[0012] 图6示意性示出在独特标记物中、主体材料中的示例颗粒取向。

[0013] 图7示出用于计算颗粒取向的示例颗粒参照系取向。

[0014] 图8示出诸如金刚石中的NV中心等颗粒的示例磁共振响应。

[0015] 图9A和9B示意性示出示例磁扫描配置。

[0016] 图10示意性示出颗粒位置和取向的示例参数化。

[0017] 图11A和11B示出两个示例颗粒位置和取向集合的比较。

[0018] 图12是示意性示出用于进行独特标记物的起始点扫描的示例过程的流程图。

[0019] 图13是示意性示出用于进行独特标记物的目的地扫描的示例过程的流程图。

[0020] 图14是示意性示出使用从对象提取的取向信息的示例过程的流程图。

[0021] 图15是示意性示出用于生成对象的唯一码的示例过程的流程图。

[0022] 图16是示意性示出示例认证过程的流程图。

[0023] 图17是示意性示出示例挑战-响应过程的流程图。

### 具体实施方式

[0024] 这里所述的一些方面涉及基于取向信息生成唯一码。例如,可以使用唯一码来认证对象。例如,可以从标记物或另一对象提取取向信息。可以以与当前用于容易地标识对象的条形码和快速响应(QR)码类似的方式,使用唯一码来认证对象。

[0025] 可以使用本文论述的方法和系统来认证各种类型的对象。对象的非限制说明性示例包括钞票和证书、信用卡等、电子支付系统、投票系统、通信系统和元件、珠宝和收藏品、金刚石和宝石、包装、纸制品、电子器材箱、电子部件和系统(例如,集成电路、芯片、电路板)、零售商品(例如,手提包、服装、运动器材)、工业组件和系统(例如,机器零部件、汽车零部件、航空航天零部件)、(加工或未加工的)原材料(例如,锭、坯、原木、板坯)、食品和包装(例如,葡萄酒、烈酒、松露,香料)、药品、药品包装和批次、医疗装置和手术工具及其包装、官方文件(例如,合同、护照、签证)、数字存储系统和元件、邮件和邮政包装、印章和防篡改标签。应当理解,该列表的示例并非穷尽性的,并且可以使用本文公开的方法和系统来认证许多其它类型的对象。

[0026] 在一些实现中,对象是包括主体材料中的晶体颗粒或其它元素的集合的构造物。晶体颗粒可以被限制在认证标记物的区域内,或者晶体颗粒可以以其它方式分布在对象的一部分中。颗粒取向可以是随机分布的;颗粒大小和相对位置可以是规则的或随机分布的。在一些示例中,不太可能制作对象的具有类似颗粒组分的副本,因此对象可以被视为唯一的。标记物例如在贴附到物品时可以用作“指纹”,从而使得能够验证其真实性。

[0027] 在一些实现中,如下对物品进行认证。在将认证标记物应用于物品之后,利用用于将晶体的相对位置和取向登记在起始点位置和取向图中的起始点扫描器来进行初始或“起始点”扫描。在一些实现中,这通过在已知施加的磁场下针对各晶体并行地进行对晶体中的荧光原子缺陷的磁共振测量来进行。在一些情况下,除晶体的位置和取向外,还确定并登记各晶体的大小以用于认证。可以根据磁场矢量沿着缺陷中心轴的投影来计算颗粒取向。取向信息不必是完整的;可以使用取向的部分投影。取向信息可被认为是几何的。我们将缺陷中心表示为以其中心为起始点的单位矢量。可以使用围绕矢量的起始点的球面坐标来描述该矢量的取向。可以完全或部分地描述和知晓经度和纬度坐标。在一些示例中,通过测量缺陷中心向幅值和取向已知的磁场的塞曼效应(Zeeman shift)移动来询问取向信息。可以通过将缺陷中心取向投影到磁场平面上的单个测量来推导部分取向信息。可以通过将具有不同磁场取向的多个这样的测量组合来提取完全取向信息。

[0028] 一旦需要物品认证(例如,一旦物品到达目的地),以与初始扫描类似的方式(但不一定利用相同的磁场或场配置)扫描物品上的认证标记物,第二扫描用于确定晶体的相对位置和取向。基于第二扫描时的磁场的预定设置来计算部分或完整的取向信息。该计算得到可以与来自先前扫描(例如,起始点扫描)的已知图进行比较的标记的取向图。

[0029] 一个示例比较是在先前扫描(起始点)图上找到如下位置值的集合,其中在该集合中的位置处,当前扫描(目的地)图上的各相应位置相差不超过值 $V$ 。例如, $V$ 可以是各颗粒大小的一部分。对于该子集中的颗粒,可以在取向图中找到这些颗粒的取向。可以计算起始点图中的颗粒取向和目的地图中的颗粒取向之间的角度。仅在受到目的地扫描器的条件(例如,磁场强度、检测时间等)约束的情况下选择的、角度差小于预定阈值 $W$ 的子集中的颗粒才被认定为匹配。如果两个图超过匹配的阈值标准,则目的地处的物品可被视为真品并被唯一标识。一个阈值标准可能是匹配颗粒的部分为起始点位置图中的颗粒总数的90%。

[0030] 在一些实现中,独特标记物中的晶体颗粒包含荧光色心,使得可以使用标准成像技术来获得这些晶体颗粒的位置和大小。还可以使用标准荧光显微镜与磁共振技术结合的变型来确定晶体颗粒的取向。颗粒的相对取向可以是随机的(颗粒的相对位置和大小也可

以是随机的),并且足够大的颗粒集合通常在其属性方面将是独特且不同的。

[0031] 可以利用金刚石中的氮空位中心(NVC)和包含色心的其它晶体颗粒的性质,以供在一些实例中用在独特标记物和其它对象中。

[0032] 晶体颗粒主体和色心的几个独特组合使得磁共振响应能够产生与颗粒有关的取向信息及其位置和大小信息。金刚石中的NVC是表现出光学检测到的磁共振的色心的一个示例。NVC在利用低于600nm(通常为530nm附近)的光学辐射被激发时,表现出宽的、在635nm~800nm光学波长范围内的荧光响应。由于金刚石晶格的对称性和NV的组成,该中心的电子基态是具有内在晶体场的自旋三重态,所述内在晶体场对来自两个自旋1次级的自旋0次级的能量进行分裂。该能量分裂在2.8GHz附近的微波范围内,其中通过共振激发来驱动0次级和 $\pm 1$ 次级之间的转变。在沿着NV-对称轴施加磁场的情况下, $\pm 1$ 次级在能量上与所施加的磁场的大小成比例地偏移(塞曼效应)。这导致两个不同频率满足共振条件。相反,如果场取向是已知的,则可以通过测量共振频率并反过来计算NV轴上的投影来获得包含NV的晶体的取向。另外,NVC的三重态/单电子构造有助于测量磁响应。在光辐射( $< 600\text{nm}$ 波长)的短暂( $< 5\mu\text{s}$ )照射之后,由于单线态和三重态之间的固有相互转换,在停止照射时的几微秒之后,自旋为0、 $\pm 1$ 次级的相对群体改变并且优先极化为0态。此外,由于 $\pm 1$ 次级与自旋为0次级相比少产生 $\sim 30\%$ 的荧光,因此这种相互转换得到自旋次级群体的区分。

[0033] 图1A示出示例物品(在该示例中为运动鞋101),其中可用于验证物品的真实性的独特标记物103a合并到该物品中。独特标记物103a可以以各种方式(包括例如采用如图1A所示的徽标102的方式)合并到物品上。独特标记物103a也可以合并到物品的标签或其它地方,并且无需肉眼可见。在充分放大率103b下,利用以下提到的技术的独特标记物(UM)可以用来展现UM中的颗粒104的集合的取向105和相对定位106。

[0034] 在一些情况下,标记的独特性源自于主体材料内的颗粒或其它元素的相对定位和取向。图2A示意性示出晶体颗粒202,该晶体颗粒202包含发射荧光的至少一个缺陷中心(还已知为色心)201。晶体颗粒主体的一个示例是包括如图2B所示的碳原子203的规则重复构造的金刚石。金刚石中的色心的一个示例是氮空位中心204,该氮空位中心204包括晶格中被氮取代的碳和距氮最近邻的被完全移除的碳。色心的取向可以例如由从氮原子向空位的矢量来定义。在一些实例中,晶格的对称性和NV中心的四重对称性可能阻止对晶体取向的绝对知晓,并且可以利用双重对称性知晓两个中心的相对取向。

[0035] 图3示出包含多个如下颗粒的主体材料301的扩展膜或体积,其中所述颗粒的子集具有至少一个色心302。这些颗粒的分离以及颗粒的取向可以是任意的。

[0036] 可以通过使用传统的光学显微技术对独特标记物成像来获得与颗粒分离和取向有关的信息。图4示意性示出用于确定颗粒的分离和取向的示例扫描器。在所示示例中,利用诸如激光器等的光源402并通过一组标准光学组件406并且通过聚焦物镜407发生反射和变换来照射独特标记物(主体膜和颗粒的复合物)401。聚焦物镜407被配置为提供足以解析独特标记物的感兴趣视野的对颗粒荧光的放大倍率。所述视野可以是整个独特标记物或该独特标记物的感兴趣区域。在利用标准滤波器和光学器件406从荧光和图像形成适当地滤除照射源之后,在摄像单元405(例如,CMOS或CCD照相机等)上拍摄到主体面的图像。图5示出示例图像500,从该图像500可以获得相对于固定坐标系的位置501和颗粒之间的相对距离502。这是用于读取独特标记物的多个可能技术的一个示例。

[0037] 可以通过观察由于在扫描器参照系中取向的电磁场相对于颗粒的相对取向引起的颗粒的荧光变化来确定颗粒的取向。一个示例是使用光学系统406中的标准波片将传播的电磁辐射(即,照射光)的横向光学偏振改变成线偏振或圆偏振。这在包含色心的许多晶体材料(包括203中的金刚石-NV系统)中产生效应。可选地,NVC(适当地为带负电的NVC)对磁场的响应也可以提供与取向有关的信息。这通过微波RF范围中的固有磁共振条件观察到。扫描器409的磁体模块微调施加到独特标记物的磁场的大小和取向。微波天线404和RF信号发生器403的输出频率被微调至磁体的不断变化的共振条件。主逻辑模块408以协调方式控制激光器(例如,振幅、时间依赖的调制)、微波或RF场(例如,振幅、相位、共振频率)的输出以及磁场取向和大小,使得可以使用一组荧光图像来确定颗粒取向。

[0038] 如此得到的图像可以类似于用望远镜(在可见光谱中)拍摄一个特定夜晚的夜空(具有各种亮斑大小和这些斑之间的许多间隔的主要为暗的背景)得到的光学图像。假定地球表面上的观察点是已知的,天空中的任一颗恒星、行星或天体的位置可以利用其相对于参考天体(例如,北极星)的位移来描述。类似地,独特标记物中的配准标记(例如,基准标记)可以引导扫描器的定位,以帮助使用类似但不一定相同的光学扫描器系统获得在不同时刻或不同位置处拍摄到的同一独特标记物的可复制图像。可以相对于这些配准标记确定扫描中荧光颗粒的位置,以给出这些荧光颗粒在标记物中的位置的绝对度量。配准标记的一个示例是(例如,使用喷墨技术)利用吸收绿色光并且发出与NVC类似的波长的荧光的不可擦除墨打印“+”符号。

[0039] 可以通过使用分配给UM的图像的像素的规则间隔开的笛卡尔网格系统501来表示该图像中的单个亮斑的位置。可以将位置指定为有序对 $(X_a, Y_a)$  503,其中: $X$ 是沿着一个维度的颗粒 $a$ 的像素坐标,并且 $Y$ 是沿着正交维度的坐标。 $X_a$ 和 $Y_a$ 可以是整数或实数。相对于给定的绝对原点 $(0,0)$ 的有序对位置的集合 $\{(X_a, Y_a), (X_b, Y_b), \dots, (X_{zz}, Y_{zz})\}$ 指定了图像的颗粒位置的独特描述。如果没有指定绝对原点,则针对各有序对创建标签并定义分隔两个颗粒的矢量,也可获得颗粒位置的独特描述。例如,如果将点 $(X_2, Y_2)$ 处的颗粒标记为“2”并且将 $(X_3, Y_3)$ 处的颗粒标记为“3”,则唯一标识符将为“ $\Delta 23 = (X_2 - X_3, Y_2 - Y_3)$ ” 503。通过计算所有的成对矢量,存在用于描述颗粒的位置的标识符的唯一列表 $L$ ,该唯一列表 $L$ 具有对网格坐标系的全局平移不变的附加性质。对于具有任意颗粒分离的给定主体膜, $L$ 是独特的集合。

[0040] 除图像中颗粒的位置外,各个颗粒具有相对于主体材料参照系的取向。在一些情况下,如果假定主体材料是有一定范围的对象,则可以在主体材料内定义原点,并且可以如图6所示在该原点601处定义右手三维笛卡尔坐标系参照系。类似地,可以针对主体材料内的各晶体颗粒定义单独的右手笛卡尔坐标系。因此,存在独特的坐标变换以在颗粒坐标系和主体材料坐标系之间移动。一个示例参数化是使用两个系统的方向余弦,另一参数化是一组欧拉旋转。与上述命名约定类似,假设点 $(X_A, Y_A)$ 处的颗粒被标记为“A”并且具有将在“A”参照系602中指定的矢量变换到主体参照系的变换矩阵 $T_a$ 。同样,点 $(X_B, Y_B)$ 处的第二颗粒被标记为“B”并且具有从“B”参照系603移动到主体参照系的变换矩阵 $T_b$ 。变换矩阵用于识别颗粒相对于坐标系的取向。类似地,如图7所示,矩阵 $T_{ab} = (T_a)^{-1} * T_b$ 指定颗粒晶体系“A”和“B”之间的相对取向701。 $T_{ab}$ 也可以经由包括框架A和B的正交轴之间的角度的方向余弦来获得。由于颗粒的单晶性质,因此颗粒内的色心相对于颗粒坐标系具有固定取向。因

而,通过测量色心相对于主体材料参照系的取向,可以使用色心的坐标轴和晶体颗粒坐标轴之间的类似坐标变换来确定颗粒的取向。通过计算所有的成对变换,存在用于描述具颗粒的相对取向的变换矩阵(例如,“AB”等)的唯一列表M,该唯一列表M有对主体网格坐标系全局旋转不变的附加属性。对于具有随机颗粒取向的给定主体膜,M是独特的集合。

[0041] 在颗粒的晶格具有高度对称性的实例下,可以自由地相对于晶体主轴指定色心坐标系。在这种情况下,可能无法仅使用色心的测量值来将色心的取向唯一地变换到晶体主轴系统。在这种情况下,提供从主体材料参照系到色心的仅单个对称轴的坐标变换的参数化就足够了。例如,可以通过对称轴和各个笛卡尔坐标轴之间的三个方向余弦来对该变换进行参数化。另一参数化是极角和取向角,其中:将前者定义为主体参照系的z笛卡尔轴和对称轴之间的角度,并且将后者定义为主体参照系的x笛卡尔轴和对称轴向主体参照系的xy笛卡尔面的投影之间的角度。

[0042] 可以使用嵌入晶体颗粒中的某些色心的性质来确定这些颗粒的取向。作为一个示例,考虑金刚石晶体颗粒中的带负电荷的氮空位色心。金刚石的碳晶格内的氮原子和空位可以定义相对于晶格坐标轴的具有不同取向的方向矢量。在利用如图8所示频率被微调到系统800的固有共振的振荡射频场照射色心时,色心的光物理可以表现出荧光的减少。例如,在约 $f_0=2870\text{MHz}$ 的频率处,色心的光致发光减少了 $\sim 30\%$ 。此外,如果沿着NV对称轴施加磁场,则针对沿着对称轴的方向为G高斯的磁场投影,该单个共振分裂成具有通过 $f_+=2870+2.8G$ 和 $f_-=2870-2.8G$ 给出的不同频率的两个共振。对于最低阶,与该对称轴正交的场不会促成频率偏移。因而,通过相对于诸如主体材料坐标等的公共坐标系维持外部磁场的大小并按已知方式改变其方向,可以确定晶体颗粒的绝对取向。利用该信息,可以使用上述技术成对地建立主体材料中的任两个颗粒的不同取向。

[0043] 假定主体材料内的颗粒数量足够小,则可以使用上述显微技术来在空间上定位从各单独颗粒发射的荧光。例如,在主体材料包含颗粒的稀疏分布(例如,填充率为20%以下)时,如此得到的荧光图像可以包含比颗粒更多的空隙。如图8所示,通过对具有由施加到主体材料的已知磁场设置的最大频率和最小频率的 $f_0$ 附近的微波频率进行采样,可以针对各个颗粒的各感兴趣区域测量共振响应800。接着,通过相对于主体膜参照系在不同取向上施加静磁场900,可以根据一系列磁共振响应确定各个颗粒的取向。例如,如图9所示,第一取向可以沿着主体材料参照系X轴901,并且第二取向可以沿着主体材料参照系Y轴902。如图10所示,在这些不同的微波频率和磁场取向下获取到的一组图像可以提供对主体膜1000中的各颗粒的空间位置和取向的完全扫描和描述。各颗粒包含唯一的位置和取向变换矩阵1001。例如,可以将独特标记物的完全取向定义为针对主体膜中的所有i个颗粒中的各颗粒的坐标和矩阵的集合: $\{(X_i, Y_i, Z_i, T_i)\}$ 。各主体膜中的颗粒集合的两个随机实例将具有不匹配的完全取向的集合,由此确保了给定一组颗粒的独特性。

[0044] 除独特标记物的位置和取向特征外,还可以视需要从颗粒的大小和形状导出附加的独特性。这可以使用用于分析颗粒的投影图像中的形状(例如,轮廓)和相对大小(例如,最大轴的长度)的图像处理技术来进行。

[0045] 如图11所示,在一些情况下,可以通过对完全取向的测试测量1101、并且使一组颗粒的位置和取向 $s = \{(X_i, Y_i, Z_i, T_i)\}$ 以充分重叠的方式与独特标记物1102的已知完全取向 $s_0 = \{(X_i, Y_i, Z_i, T_i)\}$ 匹配,来识别给定的独特标记物,以确保所测量的对象是同一物理独

特标记物： $|s-s_0| < \epsilon$ 。这里， $| \cdot |$ 表示诸如范数等的集合矢量的整体距离度量，并且 $\epsilon$ 表示确定两个集合的等价性的单个参数阈值。

[0046] 图12和13示出用于认证物品的示例过程。

[0047] 在第一示例中，在识别中涉及两个位置。起始点1200是独特标记物被首次扫描的场所。使用本文所述的技术，利用能够施加如用于完整扫描的任意磁场配置的扫描器1204来获得独特标记物1201的完整位置和取向。独特标记物与序列号1207相关联并且附加到感兴趣的物品1202。使起始点处的完整位置信息、取向信息1206和扫描器设置1203与序列号1207相关联并安全地存储。这种存储器1208可以是起始点本地的，或者位于通过因特网或其它网络接收数据的远程数据中心1351处。然后，独特物品1209离开起始点。

[0048] 在目的地1300（其可以是与起始点分开的物理位置或者如以下所述在与起始点相同的位置处），期望识别和认证贴附到独特物品1301的独特标记物1303。在该示例中，目的地利用所讨论的独特物品的序列号1302通过因特网或其它网络向认证服务器1350进行查询。认证服务器从与物品序列号相关联的安全数据库1351检索扫描参数。服务器利用目的地的扫描器1304应当被调整至的扫描器设置1305的一组挑战参数（诸如测试磁场配置和微波频率参数等）来响应目的地。在该示例中，场配置足以使目的地扫描器相对于以主体膜为中心的坐标系确定独特标记物中的各颗粒1306的位置和取向的集合。目的地扫描器进行与在起始点处完成的一系列扫描类似的一系列扫描。然后，目的地扫描器利用所测量到的位置和取向的集合1306向认证服务器1350提供响应并将序列号提供至该认证服务器。认证服务器1350知晓从起始点扫描处的初始化扫描获得的并存储在数据库1351中的、与序列号相关联的位置和取向。服务器1350比较取向和位置图，并且进行两个集合（初始化扫描和目的地扫描）的重叠的计算，并判断这些集合是否足够接近而被视为真正匹配。在该示例中，服务器1350利用两个结果1307其中之一进行响应：如果满足接近度标准则通过，而所有其它结果则失败。

[0049] 给出独特物品的单个目的地点作为第一示例的说明性示例。对于特定应用和用例（例如，钞票认证），由于独特物品可以继续在各方和各目的地点之间流通，因此可能不存在单个目的地点。此外，目的地可能不是物理分开的位置；在上述认证方法的变体中，可以在单个物理地点对独特物品进行初始化、存储和认证。

[0050] 在第二示例中，如上述的第一示例1200所述，物品的起始点扫描启动并开始。在目的地处，接收到独特物品，并从该物品中检索独特标记物以及序列号。在该第二示例中，扫描器具有不可改变但具有认证系统已知的大小和取向的磁场。扫描器单元由扫描器序列号标识。利用该单磁场配置，目的地扫描器通过捕获独特标记物的各自具有所指定的不同微波频率的成功荧光图像来进行扫描。记录各颗粒的图像位置和磁共振频率。将该信息连同物品序列号和扫描器标识号一起发送至认证服务器。

[0051] 在该示例中，认证服务器知晓独特标记物的如在初始化扫描期间捕获到的、与序列号相关联的颗粒位置和取向。认证服务器可以通过了解所施加的磁场来计算针对该特定独特标记物的预期磁共振响应。由于与扫描器序列号相关联的磁场通过使用NV中心的数学模型来提供该信息，因此认证服务器可以确定针对序列号和扫描器序列的组合的预期磁共振响应。预期磁共振响应相当于获得颗粒的部分和不完全取向。将扫描信息（颗粒位置和共振频率）从目的地发送至认证服务器，并与模型计算值进行比较。使用如上所述的具有单个

参数 $\epsilon$ 的类似阈值标准,如果目的地部分扫描与认证服务器处计算出的部分扫描足够相似,则针对物品序列号和扫描器序列号的组合,独特标记物被认为是真正匹配。

[0052] 在一些实例中,这里所述的认证技术可以提供显著的优点。例如,可以使用用于识别处于1维、2维或3维的荧光颗粒的物理独特分布的层级系统。对于唯一识别,不仅使用颗粒的位置,而且还使用颗粒相对于彼此的随机取向。例如使用诸如原子力显微镜等的纳米定位工具来进行逐个颗粒的拾取和放置过程以重建指纹,使用位置和取向信息这两者克隆物理指纹可能是不切实际的或甚至是不可能的。

[0053] 除取向外,在一些情况下可以根据需要从荧光中观察增强独特标记物的安全性、独特性和不可克隆性的颗粒的其它物理性质。这些性质可以包括但不限于各颗粒的晶体应变、各颗粒的自旋移相时间(例如, $T_2$ 时间)、个体颗粒环境本地的磁噪声的独特特征、个体颗粒环境本地的电场噪声的独特特征、颗粒中的局部核自旋系综的独特共振特征(例如,超精细分裂)、以及局部偶极场引起的与荧光偶极能量(FRET)共振的荧光寿命的独特特征。

[0054] 在一些情况下,这里所述的技术可以避免需要依赖于荧光的光谱特征。测量具有波长小变化的光谱特征涉及大的衍射光栅和长的反射路径,使得特别是在现场可部署的情况下,限制了这些指纹方法的实际使用。

[0055] 在一些实现中,与对颗粒中的色心的磁共振响应的测量相结合地或分开地,可以使用颗粒的荧光强度来获得与颗粒取向有关的信息。对于NV-色心中的一些磁场强度(诸如大于几百高斯的磁场强度等),在垂直于NV中心对称轴施加大的磁场分量时,观察到荧光响应“淬灭”。该技术使得能够在无需使用RF或微波的情况下获得取向信息。

[0056] 在一些情况下,可以通过向UM或者在UM附近添加磁性颗粒或标记物来提供附加的安全层。磁性标记物的一个示例是含有磁化的超顺磁性氧化铁颗粒的薄聚合物膜。在这种情况下,目的地扫描器使被测试的独特标记物接近磁性标记物,由此表面上的磁域或颗粒生成跨越用于扫描独特标记物的视场的局部磁场。以上述方式使独特标记物成像并且记录磁共振响应。按照如在本文中前面针对独特标记物所述的独特性的相同标准,磁性标记物可被认为是独特的。预先对独特磁性标记物进行表征,并且将与独特标记物的磁场有关的信息(大小和取向)存储在认证器1350处。利用该信息,认证器可以计算针对给定的扫描器独特磁性标记物的标识号和独特标记物的序列号的预期响应。分析在目的地扫描器处测量到的响应和所计算的响应的相似性,并且通过上述阈值标准判断认证。

[0057] 在一些实现中,独特磁性标记物和独特标记物融合为组合物理标记物。磁性颗粒(MP)可以嵌入在物品中、例如在UM下方。MP在UM附近创建特定磁场模式。如果将UM从物品的原始位置删除或者使UM从该原始位置偏移,则认证将失败。在一些实现中,MP可以合并到UM的粘合剂中或者合并到物品的悬浮介质中。

[0058] 在一些实现中,独特标记物可以用作物理不可克隆功能(PUF)。PUF通过挑战/响应行为操作,由此可以改变系统的一些参数(即,挑战)并且可以容易地测量物理系统对这些参数的响应。由于装置中的内在随机性,因此难以克隆PUF。随机性也使得难以基于输入(即,挑战)参数来预测物理系统的响应(即,功能输出)。独特标记物在被放置在参数控制的磁环境中时可以充当PUF。作为示例,可以通过设置参数(诸如微型线圈的集合中的电流等)来改变局部磁场的强度和取向。这些电流在PUF内产生磁场。PUF挑战可能是线圈的一组电流值,并且PUF响应将是对独特标记物内的各颗粒的共振频率响应。

[0059] 在一些实现中,无需针对各扫描在目的地扫描器和认证器之间通信用于设置磁场的挑战参数。相反,认证器知晓在目的地扫描器处安装的唯一随机密钥种子。认证器和目的地扫描器还共享公共同步时钟。然后,目的地扫描器使用时钟值和随机种子作为向单向(例如,散列)函数的输入,该单向函数的输出参数设置磁场参数。在这种方案中,认证器可以根据扫描器和认证器这两者都知晓的相互信息确定磁场参数,并且进行阈值匹配。扫描器参数的这种随机化添加了附加的安全层。

[0060] 在一些实现中,UM可以用作唯一指纹或物理不可克隆功能(PUF)以供认证和加密用。取向模式生成用于对消息进行编码或者作为另一加密协议的种子的随机位串密钥。

[0061] 在一些实现中,代替认证器提供认证的简单通过/失败消息,认证器向目的地提供预期扫描器响应。认证器利用包含扫描器/标签对的部分取向信息的信息进行响应,该部分取向信息是根据扫描器序列号和贴附至物品期间在起始点处的初始化扫描处捕获到的UM的完整取向信息计算出的。目的地扫描器不会将其测量值发送至认证器,而是验证该目的地扫描器利用认证器提供的预期响应进行测量的扫描。目的地将消息与扫描信息进行比较,并在响应满足阈值条件的情况下认证对象。比较起始点数据和目的地数据的认证步骤可以在目的地处或者在从两个扫描器接收数据的系统中进行。

[0062] 在一些实现中,独特标记物在离开起始点扫描时也可以在其物理组成方面有意改变。作为示例,扫描器或另一装置可以改变或修改UM。这些改变可以通过UM的物理变形或者通过将UM加热到高于设置温度来进行。例如,可以使用激光束来加热UM中的区域并使悬浮介质回流,使得颗粒的取向和位置改变。完全且完整的改变可用于标记重置,使得先前的扫描器将不匹配将来的扫描器。换句话说,在无需原始扫描器(或任何现有系统)具有与UM新配置有关的信息的情况下重新初始化标记物。

[0063] 在一些实现中,物理改变也可以用于在使用之后销毁UM(对于单次使用应用)。例如,UM可用于认证包装上的印章(例如,作为无篡改证据)。在打开包装并且不再需要UM时,印章被破坏。为了避免尝试重复使用标记物(诸如将真正的UM贴附到非独特物品等),可以销毁UM。

[0064] 在一些实现中,部分物理改变也可用于确保UM的监管链。作为示例,扫描器(例如,目的地扫描器)可以部分地改变UM以引入一些标记物性质的变化,诸如标记的一个区域中的颗粒位置和取向等。这些修改在修改扫描器处测量,并且可以根据应用需求在本地或外部存储。这可以用作分类帐(ledger)以记录直接关于该UM的扫描事件。UM包含足够的信息来对标记物进行认证,而且包括附加的空间/信息/颗粒以允许UM的修改部分的记录和认证。这可以对同一UM多次进行。例如,该技术可用于跟踪使用不同的检查点扫描器的供应链中的物品。

[0065] 在一些实现中,使用UM作为加密密钥,由此在存储加密数据的目的地处物理地改变独特标记物。UM取向的知识可以是在制造时已知,但可以由扫描器在加密时改变,以拒绝其它方先前监管密钥的UM将来知识。密钥的不可克隆性防止了秘密访问者在现场复制密钥。在一些示例中,接受明文(未加密)数据的装置需要UM作为对称加密/解密所用的密钥。

[0066] 除将本文所述的独特标记物应用于商品的认证外,独特标记物还可具有其它应用。替代应用的一个示例是多因素认证。独特标记物是不可克隆的,并且可以利用认证服务器存储该独特标记物的性质的知识。试图对交易、事件、对象、数据等进行认证的用户可以

提供该物理标记物(密钥)和用于证明他/她的身份的密码。在另一示例中,使用用户密码来在扫描器装置中生成特定的预定磁性图案,并由此提供附加的安全层。与认证系统共享用户ID、扫描器ID和标记物扫描。这除不需要供电外类似于硬件安全令牌,但需要专用的读取器装置。

[0067] 另一替代示例应用是生成用作加密密钥的随机位。可以使用给定独特标记物的取向和位置信息来生成加密所使用的随机位串。如果故意不存储与独特标记物相关联的数据、而是仅在起始点位置处使用该数据以导出随机字符串,则将需要物理不可克隆密钥来解密该信息。

[0068] 图14是示意性示出使用从对象提取的取向信息的示例过程1400的流程图。示例过程1400可以包括包含由附加或不同的实体进行的操作的附加或不同的操作,并且这些操作可以按所示顺序或按另一顺序进行。在一些情况下,图14所示的操作中的一个或多个操作可被实现为包括由一个或多个系统进行的多个操作、子过程或其它类型的例程的过程。例如,在一些实例中,可以使用图1A、1B、2A、2B、3~8、9A、9B、10、11A、11B、12、13或15所示的系统、组件和过程来进行图14所示的示例操作中的一个或多个操作。在一些情况下,操作可以组合、并行进行、迭代或以其它方式重复、或者以另一方式进行。

[0069] 图14示出第一实体1402、第二实体1404和第三实体1406这三个实体所进行的示例过程1400。图14所示的实体可以表示制造过程、工业过程、供应链、分销渠道、财务过程、公司工作流程或另一类型的过程中的不同实体。如图14所示,各实体从同一对象的元素获得唯一码,然后该实体使用该唯一码。

[0070] 在一些情况下,示例过程1400中的对象可以是或包括例如上述类型的独特标记物(UM)。例如,在一些实现中,对象可以是图1A所示的运动鞋101或独特标记物103a、图4所示的独特标记物401、图12所示的物品1202或独特标记物1201、图13所示的独特物品1301或独特标记物1303。在一些情况下,对象可以是或包括另一类型的独特标记物(UM)或者包括UM的另一类型的系统、装置或组件。在一些情况下,对象可以是或包括可用于验证结构完整性的防篡改装置。

[0071] 在一些示例中,第一实体1402是组件制造商,第二实体1404是系统制造商,并且第三实体1406是零售分销商。对象可以是第一实体1402所制造的组件(或该组件的一部分),并且第二实体1404可以将来自第一实体1402的组件合并到第三实体1406所销售或分销的产品中。第二实体1404和第三实体1406可以使用唯一码,例如以跟踪和追溯组件或者认证组件的来源、类型或另一属性。作为示例,组件可以是电池、芯片组、或者消费电子装置、医疗装置等所用的另一零部件。

[0072] 在一些示例中,第一实体1402是商业文档的制造商或打印机,并且第二实体1404和第三实体1406是金融机构。对象可以是第一实体1402所制造的商业文档(或商业文档的一部分)。例如,可以使用唯一码来认证商业文档的来源、类型或另一属性。商业文档的示例包括现金、硬币以及其它货币或银行票据、支票、债券、股票证书等。

[0073] 在一些示例中,第一实体1402是药品、医疗装置或医疗保健器材的制造商,第二实体1404是分销商,并且第三实体1406是医疗保健提供方。对象可以是由第一实体1402制造并由第二实体1404分销至医疗保健机构的药品、医疗装置或医疗保健器材(或者药品、医疗装置或医疗保健器材的包装或其组件)。例如,第二实体1404和第三实体1406可以使用唯一

码,以认证医疗装置或医疗保健器材的来源、类型、预期接收者(例如,特定患者)或另一属性。作为示例,医疗装置可以是针对特定患者制造或分配的假体装置或植入物。

[0074] 在一些示例中,第一实体1402是容器(例如,小瓶、瓶子、箱、集装箱等)的制造商,第二实体1404将一些内容物放置在容器中并将这些容器委托给第三实体1406以供存储、分析、运输、加工或另一目的。对象可以是由第一实体1402制造并提供给第二实体1404的容器(或容器的一部分)。例如,第二实体1404和第三实体1406可以使用唯一码,以认证各单独容器的身份或内容物。作为示例,可以使用唯一码来认证个体患者的生物样品、处方药的类型或其它敏感内容物。作为另一示例,可以使用唯一码来验证容器的防篡改组件,例如以判断容器或其内容物是否已被篡改。

[0075] 在一些示例中,可以使用唯一码来验证对象被授权由特定实体或一组实体(例如,特定地理区域中的实体或具有适当凭证的实体)处理或使用。

[0076] 在1410处,第一实体1402制造对象。在一些实现中,另一实体(除图14所示的第一实体1402、第二实体1404或第三实体1406外)在1410处制造对象,然后将对象提供至第一实体1402。该对象可以由多个位置中的多个实体制造,并且在1410处进行的制造可以代表整个制造工作流程内的一个制造过程。

[0077] 在图14所示的示例中,在制造对象时,在对象中形成元素的悬浮。这里,可以在对象的二维表面上、在对象的三维体积内、或者在两者上形成元素的悬浮。在一些情况下,通过将元素分布在对象的表面(例如,外表面、内表面或这两者)上来在对象中形成悬浮。在一些情况下,通过将元素分布在对象的介质中(例如,在制造对象的材料中)来在对象中形成悬浮。例如,元素可以固定在悬浮中,使得元素相对于彼此并且相对于对象的介质保持静止。例如,悬浮可以是元素的静态空间分布,其中元素的相对位置、取向、大小、磁环境和其它性质可以保持固定。在一些实现中,只要对象的形状和结构保持不变,元素就固定在悬浮中;并且例如通过使对象变形或以其它方式改变,可以在悬浮中修改元素,以修改元素的相对位置、取向、大小、磁环境和其它性质。

[0078] 在一些示例中,元素是金刚石颗粒,并且在1410处制造对象时,在对象中形成金刚石颗粒的悬浮。金刚石颗粒的悬浮可以是图3所示的主体材料301中的类型或者另一类型的悬浮。金刚石颗粒的悬浮可以例如由使用包含金刚石颗粒的原材料的制造系统形成。例如,制造系统可以包括注射成型系统、增材制造系统、打印机、涂料应用系统、锯、车床、磨机和其制造系统。在一些情况下,制造系统还可以包括将金刚石颗粒混合到原材料中或者以其它方式将金刚石颗粒分布到原材料中的混合器或另一类型的系统。

[0079] 例如,可以通过将金刚石颗粒分布在对象的表面来形成金刚石颗粒的悬浮。例如,通过将金刚石颗粒混合到液体、气体或其它流体介质中并将液体、气体或其它流体介质施加到对象的表面,可以将金刚石颗粒分布在对象的表面。在一些情况下,可以在加压容器中将金刚石颗粒与气溶胶涂料混合,并且可以将气溶胶涂料喷涂到对象的表面(内部、外部或这两者)上。在一些情况下,可以将金刚石颗粒与刷涂、辊涂、喷涂或以其它方式应用到对象的表面(内部、外部或这两者)的乳胶基涂料、油基涂料或其它类型的涂料混合。在一些情况下,可以通过在半导体制造中使用的旋涂或浸涂工艺将金刚石颗粒分布在对象的表面。

[0080] 例如,通过将金刚石颗粒混合到保形涂层材料并将保形涂层材料应用到对象的表面,可以将金刚石颗粒分布在对象的表面。保形涂层材料可以包括丙烯酸、硅树脂、聚氨酯、

或者聚对二甲苯材料或通常施加至电子组件(例如,印刷电路板等)的类型的另一材料。可以将保形涂层材料喷涂、刷涂或以其它方式应用到对象的表面(内部、外部或这两者)。

[0081] 例如,通过将金刚石颗粒混合到(例如,打印机墨盒中的)调色剂或墨材料中并将调色剂或墨材料打印在对象上,可以使金刚石颗粒分布在对象的表面。调色剂或墨材料可以包括通常用在喷墨打印机、激光打印机等中的类型的材料。例如,利用传统打印机或另一类型的系统,可以将调色剂或墨材料打印在形成对象的全部或一部分的纸张、织物或其它材料上。

[0082] 例如,通过将金刚石颗粒分布在材料中并用该材料形成对象,可以形成金刚石颗粒的悬浮。例如,通过将金刚石颗粒混合到液体、气体或其它流体介质中并用该液体、气体或其它流体介质形成对象,可以将金刚石颗粒分布在材料中。例如,可以将金刚石颗粒与原材料(例如,液体或树脂热塑性材料、熔化的玻璃材料、熔化的金属材料等)混合,并且该原材料可以用在注射成型工艺或增材制造工艺中以形成对象。在典型的注射成型工艺中,以高压将加热后的原材料注射到由模具限定的腔体中,并且原材料符合模具,然后以腔体的形状冷却和硬化。在典型的增材制造工艺中,根据计算机模型将原材料沉积在连续的层中,并且构建这些层以形成对象。例如,可以利用传统的3D打印机或其它类型的系统来进行增材制造工艺。

[0083] 金刚石颗粒可以与原材料(例如,液体或树脂热塑性材料、熔化的玻璃材料、熔化的金属材料等)混合,并且可以冷却或以其它方式加工该原材料以形成在形成对象时依据的固体工件。例如,工件可以是塑料、金属或其它类型的固体工件,并且可以通过去除(例如,切割、填充、打磨、铣削、钻孔、冲压、机械加工等)工件的材料来形成对象。在一些情况下,例如,在减材制造工艺中,可以使用传统器材(例如,锯、锉刀、车床、铣床、钻头等)来加工工件。

[0084] 在一些情况下,制造工艺可以控制对象中的元素的密度、稀疏度或数量。例如,可以将对象制造成具有小于对象体积的阈值百分比(例如,小于20%、小于10%、小于1%等)的金刚石颗粒填充。在一些情况下,例如,以使得各个元素能够由成像系统识别的方式控制对象中的元素的密度(例如,质量密度、体积密度),使得对象的荧光图像包含稀疏的一群金刚石颗粒。

[0085] 在1412处,第一实体1402从对象的元素获得唯一码。例如,在元素是金刚石颗粒时,第一实体1402可以使用金刚石颗粒的悬浮来生成对象的唯一码。第一实体1402可以例如根据图15所示的示例过程1500或另一类型的过程来获得唯一码。在一些示例中,唯一码可以基于(例如,唯一码可以是、包括、可以源自于等)从对象提取的取向信息(例如,图12中所示的取向信息1206、图13所示的取向信息1306)或另一类型的元素信息(例如,磁环境信息、地形信息、位置信息等)。在一些实现中,通过提取元素信息的扫描器系统和从元素信息生成唯一码的计算机系统来获得唯一码。例如,在对象包括金刚石颗粒的悬浮时,元素信息可以描述悬浮中的各个金刚石颗粒的取向、位置、磁环境或大小,或者对象信息可以描述悬浮中的各个金刚石颗粒的这些性质的任何组合。

[0086] 在1414处,第二实体1404获得对象。第二实体1404可以从第一实体1402直接获得对象,或者通过中间实体间接获得对象。例如,对象可以由递送服务、海关或运输官员、供应链中的另一实体等处理。在一些情况下,对象可以在第一实体1402和第二实体1404之间在

数天、数月或数年的时间段内通过一个或多个中间所有者、受托人或其它实体。

[0087] 在1416处,第二实体1404从对象的元素获得唯一码。第二实体1404可以例如根据图15所示的示例过程1500或另一类型的过程来获得唯一码。在一些实现中,第二实体1404使用与第一实体1402用于获得唯一码相同的过程来获得唯一码。例如,第二实体可以访问相同类型的扫描器器材,并且可以通过第一实体1402和第二实体1404都知晓的协议来获得唯一码。

[0088] 在一些情况下,用于从对象获得唯一码的协议包括参数(例如,磁场强度、照射强度、扫描器设置或其它类型的参数),并且通过执行协议产生的唯一码取决于对象的性质和参数的值。在一些情况下,第一实体1402选择该第一实体(在1412处)用于提取唯一码的参数的值,并且第二实体1404使用相同的值(在1416处)来提取唯一码。例如,这些值可以与对象一起提供,与第一实体1402分开获得,从可信第三方接收到,从公共数据库获得,或者由第二实体1404以其它方式产生。在一些情况下,第二实体1404例如通过随机地选择值、通过使用预定义的值、或者以其它方式独立于第一实体(在1412处)为了获得唯一码所使用的值,来独立地选择该第二实体(在1416处)用于提取唯一码的参数的值。

[0089] 在一些实例中,第一实体1402和第二实体1404分别在1412和1416处获得相同的唯一码。例如,在对象的元素未被改变并且适当地执行提取协议时,第二实体1404(在1416处)所获得的唯一码可以与第一实体1402(在1412处)所获得的唯一码相同。在一些实例下,第一实体1402和第二实体1404分别在1412和1416处获得不同的唯一码。例如,在对象的元素已被改变、或者不适当地执行了提取协议时,第二实体1404(在1416处)所获得的唯一码可以不同于第一实体1402(在1412处)所获得的唯一码。

[0090] 在1418处,第二实体1404使用唯一码。在一些实现中,在用于认证对象、跟踪对象、验证对象的完整性的过程或者与对象有关的另一类型的过程中使用唯一码。作为示例,唯一码可以是图13中的用于认证独特物品1301的取向信息1306。在一些实现中,可以在与对象无关的过程中使用唯一码。在一些实例下,唯一码可用作质量度量、安全度量和库存管理工具。在一些情况下,唯一码可用于证明法规遵从性或用于其它用途。

[0091] 在一些实现中,第二实体1404与第一实体1402(或另一实体)进行通信以在1418处使用唯一码。在一些情况下,第一实体1402和第二实体1404例如通过通信信道或直接通信链路直接彼此通信。示例通信信道包括有线或无线连接(例如,无线电连接、光学或电气连接等)、有线或无线网络(例如,局域网(LAN)、广域网(WAN)、私有网络、公共网络(诸如因特网等)、对等网络、蜂窝网络、Wi-Fi网络等)、其它物理连接(例如,气动导管、声介质等)等。在一些情况下,第一实体1402和第二实体1404例如通过访问共享数据库或其它资源、通过中间实体、通过托管信道或其它方式,间接地彼此通信。在一些实现中,在1418处使用唯一码不要求第二实体1404与第一实体1402或任何其它实体通信。例如,可以在由第二实体1404在内部执行的过程(例如,安全过程或另一类型的过程)中使用唯一码。

[0092] 在一些实现中,在认证过程中使用唯一码。例如,第二实体1404可以执行图16所示的示例认证过程1600中的请求器1602的操作。在一些情况下,认证过程包括或被实现为挑战-响应过程,例如,图17所示的示例挑战-响应过程1700等。认证过程可用于防伪、完整性验证、身份验证、监管链验证或其它用途。认证过程可以产生表示对象的真实性的输出,例如作为二进制(“通过”或“失败”)或作为分级值(例如,作为百分比、可能性或概率)。

[0093] 对于防伪,例如,可以使用唯一码来认证对象,以判断对象的声称来源、等级、类型或质量是真正的(即,真实的)还是伪造的(即,假的)。例如,产品制造商可以认证产品组件,以判断产品组件是否是由特定组件制造商制造的。例如,零售商可以认证品牌产品,以判断品牌产品是否由所指示的品牌来源或授权制造商生产的。例如,银行可以认证货币项目,以判断货币项目是否是由特定金融机构或政府发行的。认证过程可用于其它类型的防伪。

[0094] 对于完整性验证,例如,可以使用唯一码来认证对象,以判断对象是保持完整(即,真实的)还是已被损害或被篡改(即,假的)。例如,分销商或最终用户可以认证产品,以判断产品印章是否被弄乱、组件是否被拆卸或更换(例如,安装螺钉是否被弄乱)或者对象是否被以其它方式篡改。例如,药房可以认证化合物,以判断包装或容器是否已被篡改。认证过程可用于其它类型的完整性验证。

[0095] 对于身份验证,例如,可以使用唯一码来认证对象,以判断对象是否与人或其它实体(例如,公司实体,政府实体等)的特定身份或标识符相关联。例如,医院可以认证处方药容器,以判断内容物是否与特定处方或患者相关联。例如,医疗保健提供方可以认证假体装置或植入物,以判断装置或植入物是否与特定患者或手术相关联。认证过程可用于其它类型的身份验证。

[0096] 对于监管链验证,可以使用唯一码来认证对象是否已拥有一个或多个实体。例如,企业实体可以验证敏感产品或信息的监管链,以在部署在安全的内部过程之前确保机密性。例如,执法实体可以验证物证的监管链,以确保调查的完整性。认证过程可用于其它类型的监管链验证。

[0097] 认证过程可以产生第二实体1404可以作用的结果。作为示例,如果认证过程(例如,利用二进制指示符、利用高于可接受阈值的分级等)表示对象是真品,则第二实体1404可以接受并部署该对象。例如,可以安装组件,可以管理药物,可以接受金融工具作为支付等。作为另一示例,如果认证过程(例如,利用二进制指示符、利用低于可接受阈值的分级等)表示对象是赝品,则第二实体1404可以拒绝或隔离该对象。例如,可以退回组件,可以处置药物,可以拒绝金融工具作为支付等。

[0098] 在一些实现中,在加密过程中使用唯一码。例如,可以基于唯一码生成密钥(例如,私钥、共享秘密等)或用于加密过程的另一值(例如,唯一码可以用作或用于导出密钥)。唯一码可用于消息认证(例如,签名、验证)、消息加密(例如,加密、解密),密钥推导(例如,产生会话密钥、临时密钥等)和其它密码应用。

[0099] 在一些实现中,例如,类似于通过加密密钥协商算法(例如,Diffie-Hellman、量子密钥分发(QKD)或其它算法)产生的共享秘密的类型,第一实体1402和第二实体1404可以使用唯一码作为共享秘密。例如,第二实体1404可以通过公共信道在加密通信会话中使用共享秘密,以将消息加密到第一实体1402或者从第一实体1402解密消息。例如,第二实体1404可以通过公共信道在认证通信会话中使用共享秘密,以将消息签名到第一实体1402或者验证来自第一实体1402的消息。

[0100] 在一些实现中,例如,第二实体1404可以使用唯一码作为私钥并生成相关公钥,以用在公钥基础结构(PKI)系统中。例如,第二实体1404可以使用私钥来对已由另一实体使用公钥加密后的消息进行解密。作为另一示例,另一实体可以使用公钥来验证已由第二实体1404使用私钥签名后的消息。示例PKI系统包括基于RSA的系统和椭圆曲线系统等。

[0101] 在一些实现中,对象被用作分类帐(例如,安全分类帐、公共分类帐、分布式分类帐或其它类型的分类帐)(或与分类帐结合使用),并且唯一码被用作(或用于生成)分类帐中的条目或更新。例如,利用第一实体1402(在1412处)获得的第一唯一码可以表示分类帐中的第一条目,并且利用第二实体1404(在1416处)获得的不同的第二唯一码可以表示分类帐中的不同的第二条目。在一些情况下,第二实体1404在1416处获得唯一码之前修改对象,这使得第二实体1404在1416处获得不同的第二唯一码。例如,第二实体1404可以改变对象的一个或多个元素的取向,使得从对象提取的取向信息产生不同的唯一码。

[0102] 在1420处,第三实体1406获得对象。第三实体1406可以从第二实体1404直接地获得对象,或者通过一个或多个中间实体间接地获得对象。

[0103] 在1422处,第三实体1406从对象的元素获得唯一码。例如,根据图15所示的示例过程1500或另一类型的过程,第三实体1406可以获得唯一码。在一些实现中,第三实体1406使用与第一实体1402或第二实体1404(或这两者)用于获得唯一码的相同过程来获得唯一码。在一些实例中,第一实体1402、第二实体1404和第三实体1406分别在1412、1416和1422处获得相同的唯一码。例如在对象的元素未被改变并且适当地执行提取协议时,利用第三实体1406(在1422处)获得的唯一码可以与利用第一实体1402(在1412处)和第二实体1404(在1416处)获得的唯一码相同。在一些实例中,第一实体、第二实体和第三实体中的一个或多个从其它实体获得不同的唯一码。

[0104] 在1424处,第三实体1406使用唯一码。第三实体1406(在1424处)可以以类似于第二实体1404(在1418处)如何使用在1416处获得的唯一码的方式使用在1422处获得的唯一码。在一些实现中,第三实体1406与第一实体1402或第二实体1404(或另一实体)通信以在1424处使用唯一码。例如,可以在第三实体1406和第一实体之间执行认证过程;可以在第三实体1406和第一实体1402之间直接地或者通过中间实体(例如,第二实体1404或另一实体)进行认证过程。在一些情况下,过程1400以类似的方式扩展到其他实体。

[0105] 图15是示意性示出用于生成对象的唯一码的示例过程1500的流程图。示例过程1500可以包括附加或不同的操作,并且这些操作可以按所示顺序或按另一顺序进行。在一些情况下,操作可以组合、并行进行、迭代或以其它方式重复执行、或者以另一方式进行。

[0106] 在一些情况下,利用例如图4所示的扫描器或者另一类型的扫描器系统等的扫描器系统来实现图15所示的操作中的一个或多个。扫描器系统可被配置为例如通过向样品施加刺激并记录样品对刺激的响应,来从样品提取信息。扫描器系统可以包括施加刺激或记录样本的响应(或这两者)的一个或多个探测器。例如,扫描器系统可以包括照射源(例如,激光器或其它光源)、光学组件(例如,透镜、镜、滤波器、放大器等)、光学传感器、照相机(例如,CMOS照相机、CCD照相机或另一类型的照相机)、信号发生器(例如,RF信号发生器、微波信号发生器等)、线圈和天线、磁体系统(例如,电磁铁、超导磁体等)以及其它组件,这些组件可以根据图14所示的示例或以其它方式配置。

[0107] 在扫描器系统被配置为检查金刚石颗粒的色心的示例中,扫描器系统包括一个或多个探测器,该一个或多个探测器被配置为例如通过向样品施加照射并且(例如,在外加静磁场、外加静电场等的范围内)检测对象的荧光响应,来获得样品的荧光图像。在一些示例中,扫描器系统还包括一个或多个探测器,该一个或多个探测器被配置为例如通过将样品定位在外加磁场中、将无线电或微波脉冲施加到样品并检测对象对脉冲的响应,来获得样

品的磁共振性质。在一些示例中,扫描器系统还包括在利用扫描器系统检查样本时样本驻留的样本区域。

[0108] 在一些情况下,利用计算机系统实现图15所示的操作中的一个或多个。例如,从样本提取信息的扫描器系统可以包括分析所提取的信息的处理器。附加地或可选地,可以利用另一计算机系统进行操作。例如,可以将扫描器系统所提取的信息通信至与该扫描器系统不同(并且在一些情况下远离该扫描器系统)的单独计算机系统。

[0109] 在1502处,接收到对象。例如,可以在扫描器系统的样本区域中接收到对象。在1502处接收到的对象是包括元素(例如,集成到对象的结构中或以其它方式分布在对象中的元素)的物理对象。在1502处接收到的对象可以是在图14的过程1400中涉及的类型。例如,对象可以是或包括独特标记物(UM)或包括元素的悬浮的另一项。

[0110] 在一些实现中,对象是所制造的系统或装置(例如,容器、文档、医疗装置等)。在一些实现中,对象是所制造的系统或装置的组件。例如,对象可以是容器(例如,处方药容器、生物样品容器、信封或其它文档容器、货运集装箱等)的组件(例如,标签、盖子、印章或其它组件)、文档(例如,货币、钞票或其它商业文档)上的打印区域、医疗装置(例如,假肢装置或植入物)的一部分、贴在零售商品或电子装置上的标签、等等。

[0111] 在一些实现中,对象是宏观对象,并且元素是对象的微结构或纳米结构。例如,元素可以是金刚石颗粒、磁性颗粒、纳米棒、诸如薄片或箔等的微观结构、表现出电子顺磁性的分子、具有有限电偶极矩的分子、或者悬浮在对象中的其它类型的结构。对象可以具有宏观大小,例如具有毫米、厘米或更大的最大大小;并且元素可以具有比对象小一个或多个数量级的大小,例如,在一些情况下,元素具有毫米、微米或纳米级的最大大小。在一些示例中,元素是固定在介质中的晶体颗粒。晶体颗粒可以是例如各自具有色心(例如,NV中心或其它类型的色心)的金刚石颗粒,并且介质可以是有机或无机材料。在一些情况下,晶体颗粒可以悬浮在硅、玻璃、热塑性塑料(例如,丙烯酸、丙烯腈丁二烯苯乙烯(ABS)、聚氯乙烯(PVC)、聚乙烯)、热固性聚合物(例如,环氧树脂和聚氨酯)或者其它类型的材料中。对象可以包括数百个、数千个、数百万个或更多的元素。元素可以分散在对象的全部或部分体积中,分散在对象的全部或部分表面上,或者以其它方式分布在对象中。

[0112] 在一些实现中,各元素具有限定元素的取向的(内部或外部)结构。例如,元素可以具有晶体结构,并且元素的取向可以由元素的晶体结构的特定轴(例如,对称轴)或平面限定。作为另一示例,元素可以具有长形结构,并且元素的取向可以由元素的长形形状的特定轴(例如,长轴)或平面限定。作为另一示例,元素可以具有内部特征或结构(例如,色心),并且元素的取向可由元素的特定轴(例如,NV轴)或者内部特征或结构的平面限定。

[0113] 在一些实现中,各元素相对于对象中的其它元素固定在对象中。例如,元素可以固定在对象中,使得元素的相对位置和取向保持固定,只要对象的形状和结构保持固定即可。因此,对象可以通过检测各个元素,以可重复和确定的方式固有地定义可以检测到的元素性质的分布。例如,元素的悬浮可以定义相对空间取向的分布、相对位置的分布、大小和形状等的分布。元素性质的分布可以具有在各对象中可以改变的数千个、数百万个或更多的独立自由度。

[0114] 在一些实现中,通过高度复杂的随机或准随机的过程(例如,在制造对象时发生的热力学过程)来控制元素性质中的一些或全部。因此,在另一对象中克隆或复制单个对象中

的元素性质的分布可能是困难的或不切实际的(或者甚至是不可能的)。因此,元素性质的分布针对各单独对象可以是唯一的,并且类似于指纹或签名,可以用作对象的唯一标识符。

[0115] 在1504处,从对象提取元素信息。例如,可以通过扫描器系统的一个或多个探测器的操作来从对象提取元素信息。元素信息可以包括或者元素信息可以基于由对象的元素定义的元素性质的分布。例如,元素信息可以描述相对空间取向的分布、相对位置的分布、大小和形状的分布或者这些的组合。

[0116] 在一些情况下,通过(例如,如针对图4所述)使用光学显微镜使对象成像并处理如此得到的图像来提取元素信息。在一些情况下,通过(例如,如针对图4所述)检测对象的磁共振性质并处理磁共振数据来提取元素信息。

[0117] 在一些情况下,元素信息通过扫描器系统进行的提取协议来提取,并且元素信息可以取决于元素性质和提取协议的参数。例如,提取协议的参数可以被提供作为向操作扫描器系统的探测器的控制器或控制过程(例如,图4中的主逻辑模块408)的输入。在一些情况下,从对象提取的元素信息不一定取决于提取协议的参数。例如,由于取向是固定的,因此识别相同元素(例如,所有元素或元素的相同子集)的取向的两个不同提取协议可以产生相同的取向信息。并且,可以在对象的全局旋转下可以是不变的标准化或预定义格式来定义元素信息。

[0118] 在一些实现中,提取元素信息包括从对象提取取向信息,其中取向信息指示对象的各个元素的相对空间取向。取向信息可被格式化为列表、数组或其它格式。在一些情况下,取向信息包括描述各个元素的相对空间取向的坐标变换。坐标变换可以是例如变换矩阵的列表、正交旋转(诸如欧拉分解等)的顺序集合或者另一形式的坐标变换。在元素是金刚石颗粒的示例中,取向信息可以是复合变换矩阵的列表(例如,各金刚石颗粒的复合变换矩阵),并且复合变换矩阵的列表可以是对对象的坐标系全局旋转不变的。

[0119] 在一些情况下,通过获得对施加到对象的照射的光学响应(例如,荧光响应或另一类型的光学响应)来提取取向信息和可能的其它元素信息(例如,位置信息、大小信息、形状信息)。在一些情况下,光学响应可以包括拉曼散射或另一非线性效应(例如,二次谐波产生、自发参数下转换等)。在一些示例中,荧光响应可以包括例如在635nm~800nm的范围或者由元素的色心或另一特征信号(斯托克斯和反斯托克斯移位或另一非线性过程)产生的另一波长内的电磁信号。可以基于元素的荧光响应来生成对象的荧光图像,并且可以从荧光图像确定相对空间取向。图5所示的图像500表示具有1位颜色深度的单色荧光图像的示例。可以基于对象中的荧光变化(例如,检测到的元素的响应于照射的变化或者施加到对象的场的变化的荧光变化)来确定取向信息。在另一示例中,可以基于非线性光学过程(例如,二次谐波产生(SHG))的取向依赖性来确定取向信息。

[0120] 在一些情况下,使用例如电子自旋共振(ESR)、核磁共振(NMR)、光学检测到的磁共振(ODMR)或另一类型的磁共振技术等的磁共振技术来提取取向信息和可能的其它元素信息(例如,磁环境信息)。例如,扫描器可以获得对施加到对象的振荡电磁场(例如,射频、微波频率等)的磁共振响应,并且计算机系统可以通过分析磁共振响应来确定相对空间取向。例如,可以通过以下来获得磁共振响应:将对象定位在外部磁场(例如,静态外部场)中,将振荡电磁场(例如,将无线电或微波频率脉冲)施加到外部磁场中的对象,并且光学地检测元素的响应于外部磁场的相对变化(例如,外部磁场的强度或取向的相对变化)、振荡电磁

场的相对变化(例如,振荡电磁场的振幅、频率或相位的相对变化)的磁共振变化。

[0121] 在一些实现中,可以独立于例如相对于扫描器系统配准对象来提取取向信息。在一些情况下,对象不包括除元素本身之外的配准标示或取向参考。在通过向对象施加照射来提取取向信息时,可以在无需参考照射的角度的情况下相对于彼此描述元素的取向。类似地,在通过磁共振技术提取取向信息时,可以在无需参考外加磁场的角度的情况下相对于彼此描述元素的取向。因此,取向信息可以是对对象的坐标系全局旋转不变的。

[0122] 在晶体颗粒是各自具有色心的金刚石颗粒时,可以通过检测色心的相对取向来提取取向信息。在一些情况下,可以通过处理对象的荧光图像、磁共振数据或其它测量值来检测相对取向。例如,可以使用坐标变换(例如,表示各金刚石颗粒的多个变换的复合变换矩阵(例如,如关于图6和7所述))来识别相对取向。金刚石颗粒的复合变换矩阵可以表示对象的坐标系和金刚石颗粒的坐标系之间的第一变换、以及金刚石颗粒的坐标系和金刚石颗粒中的色心的坐标系之间的第二变换。在一些示例中,各金刚石颗粒包括单个色心(例如,各单独金刚石颗粒包含单个NV中心)。在一些示例中,金刚石颗粒的一些或全部包括多个色心(例如,各单独金刚石颗粒包含两个或更多个NV中心)。在单个金刚石晶体包括多个NV中心时,金刚石晶格的四重对称意味着可以选择四个取向中的任何取向作为参考来描述颗粒的取向。

[0123] 在一些实现中,提取元素信息包括从对象提取位置信息,其中位置信息指示对象的各个元素的相对空间位置。位置信息可被格式化为列表、数组或其它格式。在一些情况下,位置信息包括描述各个元素的相对空间位置的坐标矢量的列表。在一些情况下,可以通过处理对象的荧光图像、磁共振数据或其它测量值来检测相对位置。例如,可以使用如关于图5所述或以另一方式识别相对位置。

[0124] 在一些实现中,提取元素信息包括从对象提取地形信息,其中地形信息指示对象的各个元素的相对空间地形(例如,相对大小,相对形状等)。地形信息可被格式化为列表、数组或其它格式。在一些情况下,地形信息包括描述(例如,沿着一个或多个坐标轴的)维度的坐标矢量的列表。在一些情况下,可以通过处理对象的荧光图像、磁共振数据或其它测量值来检测元素的地形。

[0125] 在一些实现中,提取元素信息包括从对象提取磁环境信息,其中磁环境信息指示对象的各个元素的磁环境。磁环境信息可被格式化为列表、数组或其它格式。在一些情况下,磁环境信息包括描述各元素所经历的(例如,沿着一个或多个坐标轴的)磁场强度的坐标矢量的列表。在一些情况下,可以通过处理对象的磁共振数据或其它测量值来检测元素的磁环境。

[0126] 元素信息可以指例如两个或三个空间维度中的元素的性质。例如,取向信息可以指示二维空间或三维空间中的相对空间取向;同样,地形和位置信息可以指示二维空间或三维空间中的相对位置、大小、形状等。在元素是固定在对象的另一介质中的晶体颗粒的示例中,元素信息可以指例如在两个或三个空间维度中的晶体颗粒的相对大小、形状、取向或位置、或者这些性质的组合。

[0127] 在1506处,从元素信息生成唯一码。例如,可以利用扫描器系统中的处理器、与扫描器系统分开的计算机系统或者它们的组合来生成唯一码。例如,另一计算机系统可以获得元素信息(取向信息、位置信息、地形信息、磁环境信息或这些信息的组合)并生成唯一

码。

[0128] 在一些实现中,根据扫描器系统从对象提取的取向信息生成唯一码,并且唯一码不依赖于对象和扫描器系统之间的任何配准或相对取向。例如,可以独立于对象和扫描器系统之间的相对取向来处理取向信息。在通过对对象施加照射来提取取向信息时,可以在不参考向对象施加照射的角度的情况下确定唯一码。类似地,在通过磁共振技术提取取向信息时,可以在不参考向对象施加外部(静态或振荡)磁场的角度的情况下确定唯一码。

[0129] 在一些实现中,根据仅表示对象中的元素的子集的元素信息生成唯一码。例如,对象可以包括元素超集,并且用于生成唯一码的元素信息可以仅表示元素子集(少于所有元素)。

[0130] 在一些情况下,在1504处提取的元素信息指示仅元素子集的性质,并且在1506处根据在1504处提取的所有元素信息生成唯一码。例如,元素子集可以是响应特定范围的场强度、频率、极化等的刺激的元素。作为示例,在元素是金刚石颗粒时,可以使用照相机仅观察具有对特定频带(例如,2.77~2.79千兆赫(GHz)或另一频带)的光学响应的金刚石颗粒。

[0131] 在一些情况下,在1504处提取的元素信息指示超集中的所有元素的性质,并且在1506处从在1504处提取的元素信息的子集生成唯一码。例如,可以从元素信息的完整集合中识别指示元素子集的相对空间取向的取向信息的子集,使得可以基于仅子集的相对空间取向来生成唯一码。元素子集可以是对象的特定区域中的元素、产生特定信号强度的元素、或另一元素子集。

[0132] 唯一码可以包括采用任何合适形式或格式的信息,并且可以通过以任何适当方式处理元素信息来生成。例如,唯一码可以是二进制或字母数字,或者唯一码可以包括其它类型的符号或值。唯一码可被格式化为单个值或值的集合(例如,列表、数组等)或另一格式。作为示例,在取向信息包括坐标变换的列表时,可以处理或重新格式化列表以定义唯一码。在一些情况下,将函数或变换应用于元素信息以生成唯一码。

[0133] 在示例过程1500中,在1506处生成的唯一码对于对象是唯一的。例如,在实际意义上,唯一码可以由足够大而使得没有两个对象将产生相同代码的相空间中的参数定义。例如,可以利用从对象提取的元素信息中的自由度的数量来定义相空间的大小。(通过相同工艺使用相同材料等所制造的)另一对象在相空间中占据相同位置的可能性可能是无限小的。在一些情况下,产生将在相空间中占据相同位置并产生相同代码的另一对象是不切实际的。

[0134] 在1508处,可以修改对象。例如,修改对象可以改变至少一些元素的相对空间取向或空间位置(或这两者)。例如,在修改对象1508之后或在其它实例中可以重复过程1500。在一些情况下,在过程1500的第一次迭代中,生成对象的第一唯一码;在过程1500的第二次迭代中,基于在改变相对空间取向之后从对象提取的取向信息,来针对同一对象生成不同的第二唯一码。在一些情况下,元素的相对空间取向可被用作与对象相关的信息的安全或公共分类帐。例如,(通过在1508处修改对象)改变空间取向可以与对分类帐的更新相关联。

[0135] 图16是示意性示出示例认证过程1600的流程图。示例过程1600可以包括包含由附加或不同的实体进行的操作的附加或不同的操作,并且这些操作可以按所示顺序或以其它顺序执行。在一些情况下,操作可以组合、并行进行、迭代或以其它方式重复、或者以另一方式进行。

[0136] 在一些情况下,利用一个或多个计算机系统实现图16所示的操作。图16示出请求器1602和认证器1604所进行的示例过程1600。请求器1602和认证器1604可以表示例如在单个计算机系统中、在不同的计算机系统中(例如,在不同的位置处、在不同的环境中等)、在分布式计算系统中或者在不同实体的过程中(例如,在制造过程、工业过程、供应链、分销渠道、财务过程、公司工作流程或另一类型的过程中)部署的计算机实现的模块。作为示例,请求器1602可以表示在图13的目的地1300处执行的过程,并且认证器1604可以表示在图13的认证器1350处执行的过程。作为另一示例,请求器1602可以表示在图14的第二实体1404处执行的过程,并且认证器1604可以表示在图14的第一实体1402处执行的过程。

[0137] 在过程1600期间,请求器1602和认证器1604彼此通信。在一些实现中,请求器1602和认证器1604例如通过通信信道或直接通信链路直接地彼此通信。在一些实现中,请求器1602和认证器1604例如通过访问共享数据库或以其它方式间接地彼此通信。

[0138] 图16所示的示例认证过程1600利用从物理对象提取的信息。在一些情况下,在图16的示例过程1600中涉及的对象可以是或包括上述类型的独特标记物(UM)、图14的过程1400中涉及的对象、图15的过程1500中涉及的对象或另一类型的对象。在一些实现中,所提取的信息包括指示对象的各个元素的性质的元素信息(例如,指示各个元素的相对空间取向的取向信息)。

[0139] 示例认证过程1600还可以利用对象标识符以及可能与物理对象有关的其它信息。对象标识符可以是例如对象的序列号、对象的零部件号、或者对象的来源、等级、类型或质量的标识。对象标识符可以是例如与对象相关联的人或其它实体的身份或标识符(例如,姓名、地址、电话号码、用户名、社会保障号等)。

[0140] 在过程1600之前或期间,根据从对象提取的元素信息生成认证码,并且认证码与对象的对象标识符相关联。可以以与在图15所示的过程1500中生成唯一码相同的方式生成认证码。例如,可以通过将对象标识符和认证码存储在安全认证数据库中或者以另一方式来使这两者相关联。例如,对象标识符可以是图12中的序列号1207,元素信息可以是图12中的取向信息1206,并且可以通过在图12的安全数据存储1208(或者图13的安全数据库1351)中链接对象标识符和元素信息来关联这两者。对象标识符和认证码可以以另一方式相关联。

[0141] 在一些实现中,将附加信息存储在安全认证数据库中或者以其它方式与对象标识符和认证码相关联。例如,可以使扫描器系统为了提取元素信息所使用的扫描器设置与对象标识符和认证码相关联。扫描器设置可以包括例如在对象上进行的提取协议中使用的参数值。

[0142] 在1610处,请求器1602获得对象数据。例如,对象数据可以包括基于请求器1602从对象提取的元素信息的认证码。如图15所示的过程1500那样或者以另一方式,认证码可以是或包括例如请求器1602从元素信息生成的唯一码。在1610处获得的对象数据还可以包括例如对象的序列号等的对象标识符。在1610处获得的对象数据还可以包括挑战-响应数据或其它类型的信息。

[0143] 在1612处,请求器1602向认证提供者发送认证请求。认证请求可以包括或基于包含例如认证码和对象标识符的对象数据。在一些情况下,认证请求包括附加信息。例如,认证请求可以指示请求器1602的扫描器系统用于提取元素信息的扫描器设置。

[0144] 在1614处,认证器1604评价认证请求。可以基于安全认证数据库或认证器1604可访问的另一类型的安全系统中的信息来评价认证请求。作为示例,认证器1604可以使用来自认证请求的对象标识符(并且在一些情况下为例如扫描器设置等的其它信息)来找到先前与对象标识符相关联的有效认证码。然后,认证器1604可以将有效认证码与认证请求中提供的认证码进行比较。

[0145] 在1616处,认证器1604向请求器1602发送认证响应。图16的认证响应包括指示在1614处进行的评价的结果的真实性数据。认证响应可以将结果指示为二进制值。例如,真实性数据可以指示比较产生了匹配(例如,数据库中的有效认证码与认证请求中提供的认证码完全匹配或在一定容差内),这可能意味着该对象是真品;或者真实性数据可以指示比较没有产生匹配(例如,数据库中的有效认证码与认证请求中提供的认证码不完全匹配或在一定容差内),这可能意味着该对象是赝品。认证响应可以将结果指示为分级值。例如,真实性数据可以指示有效认证码与认证请求中提供的认证码匹配的百分比或程度,并且请求器1602可以基于自身的标准(例如,参考一些容差或其它验收标准)来解释分级值。

[0146] 图17是示意性示出示例挑战-响应过程1700的流程图。示例过程1700可以包括包含由附加或不同的实体进行的操作的附加或不同的操作,并且这些操作可以按所示顺序或按另一顺序进行。在一些情况下,操作可以组合、并行进行、迭代或以其它方式重复、或者以另一方式进行。

[0147] 在一些情况下,利用一个或多个计算机系统实现图17所示的操作。图17示出请求器1702和验证器1704所进行的示例过程1700。与图16的请求器1602和认证器1604相似,例如,请求器1702和验证器1704可被实现为一个或多个计算机系统中的一个或多个计算机实现的模块。作为示例,请求器1702可以表示在图13中的目的地1300处执行的计算机实现的过程,并且验证器1704可以表示在图13中的认证器1350处执行的计算机实现的过程。作为另一示例,请求器1702可以表示在图14中的第二实体1404处执行的过程,并且验证器1704可以表示在图14中的第一实体1402处执行的过程。在过程1700期间请求器1702和验证器1704(直接地或间接地)彼此通信。

[0148] 图17所示的示例认证过程1700利用从物理对象提取的信息。在一些情况下,在图17的示例过程1700中涉及的对象可以是或包括上述类型的独特标记物(UM)、在图14的过程1400中涉及的对象、在图15的过程1500中涉及的对象或另一类型的对象。在一些实现中,所提取的信息包括指示对象的各个元素的性质的元素信息(例如,指示各个元素的相对空间取向的取向信息)。示例认证过程1700还可以利用对象标识符以及可能与物理对象有关的其它信息。

[0149] 挑战-响应过程1700可以作为认证过程(例如,认证对象)或用于其它目的而执行。在一些情况下,使用将对象部署为物理不可克隆功能(PUF)的挑战-响应过程1700。例如,在将特定刺激或挑战施加至对象时,该对象可以提供该对象特有的并且在无该对象的情况下难以或不切实际地(或甚至不可能)获得的可预测响应。对个体挑战的响应可能取决于例如难以或不切实际地(或甚至不可能)复制或分析方式确定的对象的高度复杂的内部结构。因此,对象在被部署为PUF时,在一些实例中可以服务与单向函数(例如,散列函数)相同的目的。

[0150] 在1710处,请求器1702获得挑战数据。例如,挑战数据可以指示请求器1702的扫描

器系统为了从对象提取元素信息而可以使用的提取协议。在一些情况下,挑战数据指示提取协议的扫描器设置。扫描器设置可以包括例如扫描器系统的参数的特定值以执行提取协议。在一些实现中,请求器1702从验证器1704或另一外部源获得挑战数据。在一些实现中,请求器1702例如通过随机地选择扫描器设置、通过选择预定义的一组扫描器设置或以其它方式来生成挑战数据。

[0151] 在1712处,请求器1702基于挑战数据来获得响应数据。可以通过根据挑战数据询问对象(例如,通过使用利用挑战数据指示的扫描器设置执行提取协议)来获得响应数据。响应数据可以包括根据使用挑战数据从对象提取的元素信息所生成的唯一码。可以如图15所示的过程1500那样或者以另一方式从对象提取元素信息。在1712处获得的响应数据还可以包括例如对象的序列号等的对象标识符。

[0152] 在1714处,请求器1702将响应数据发送至验证器1704。在一些情况下,请求器1702还将挑战数据发送至验证器1704。请求器1702还可以将对象标识符或其它信息发送至验证器1704。

[0153] 在1716处,验证器1704评价响应数据。可以基于安全认证数据库或验证器1704可访问的另一类型的安全系统中的信息来评价响应数据。作为示例,验证器1704可以使用挑战数据(并且在一些情况下为例如对象标识符等的其它信息)来找到先前从对象获得的有效响应。然后,验证器1704可以将(例如,来自安全数据库的)有效响应与响应数据中提供的响应进行比较。

[0154] 在一些情况下,验证器1704在1716处使用预定义的有效响应来评价响应数据。例如,验证器1704可以访问对象的挑战-响应库,其中挑战-响应库中的各有效响应与不同的挑战相关联。例如,通过基于一组不同的挑战询问对象或以其它方式,可以在执行挑战-响应过程1700之前定义挑战-响应库。在一些情况下,验证器1704基于在1710处获得的挑战数据来在挑战-响应过程1700期间生成有效响应。例如,验证器1704可以访问对象的完整元素信息,这可以使得验证器1704能够基于挑战数据计算有效响应。

[0155] 在1718处,验证器1704将有效性数据发送至请求器1702。图17的有效性数据指示在1716处进行的评价的结果。有效性数据可以将结果指示为二进制值。例如,有效性数据可以指示比较产生了匹配(例如,数据库中的有效响应与响应数据中提供的响应完全匹配或在某个容差内),这可能意味着响应有效;或者有效性数据可以指示比较没有产生匹配(例如,数据库中的有效响应与响应数据中提供的响应不精确匹配或没有在某个容差内),这可能意味着响应无效。有效性数据可以将结果指示为分级值(例如,有效响应与提供的响应匹配的百分比或程度),并且请求器1702可以基于自身的标准(例如,参考一些容差或其它验收标准)来解释分级值。

[0156] 本说明书所述的主题和操作中的一些可以在数字电子电路中、或者在(包括本说明书所公开的结构及其结构等同物的)计算机软件、固件或硬件中、或者在它们中的一个或多个的组合中实现。本说明书所述的主题的一些可被实现为编码在计算机存储介质上以由数据处理设备执行或者控制数据处理设备的操作的一个或多个计算机程序、即计算机程序指令的一个或多个模块。计算机存储介质可以是或者可以包括于计算机可读存储装置、计算机可读存储板、随机或串行存取存储器阵列或装置、或者它们中的一个或多个的组合。此外,尽管计算机存储介质不是传播信号,但计算机存储介质可以是在人工生成的传播信号

中编码的计算机程序指令的源或目的地。计算机存储介质还可以是或者包括于一个或多个单独的物理组件或介质(例如,多个CD、盘或其它存储装置)内。

[0157] 本说明书所描述的操作中的一些可被实现为由数据处理设备对一个或多个计算机可读存储装置上所存储的或者从其它源接收到的数据进行的操作。

[0158] 术语“数据处理设备”包括用于处理数据的所有类型的设备、装置和机器,包括例如可编程处理器、计算机、片上系统、或者多个可编程处理器、多个计算机、多个片上系统、或者前述的组合。该设备可以包括专用逻辑电路,例如FPGA(现场可编程门阵列)或ASIC(专用集成电路)。除硬件外,该设备还可以包括为所讨论的计算机程序创建执行环境的代码,例如构成处理器固件、协议栈、数据库管理系统、操作系统、跨平台运行时环境、虚拟机或它们中的一个或多个的组合的代码。

[0159] 可以以包括编译语言或解释语言、声明语言或过程语言的编程语言的任何形式来编写计算机程序(还已知为程序、软件、软件应用程序、脚本或代码),并且可以以包括适合用在计算环境中的组件、子例程、对象或其它单元作为单机程序或作为模块的任何形式来运用该计算机程序。计算机程序可以但并非必须与文件系统中的文件相对应。可以将程序存储于如下文件中:保持其它程序或数据的文件的一部分(例如,在标记语言文档中存储的一个或多个脚本)、程序专用的单个文件、或者多个协同文件(例如,存储一个或多个模块、子程序或部分代码的文件)。可以使计算机程序在位于一个站点或分布在多个站点之间并且经由通信网络互连的一个计算机或多个计算机上执行。

[0160] 本说明书中描述的过程和逻辑流程中的一些可以由执行一个或多个计算机程序的一个或多个可编程处理器进行,以通过对输入数据进行操作并生成输出来进行动作。过程和逻辑流程也可以由例如FPGA(现场可编程门阵列)或ASIC(专用集成电路)的专用逻辑电路实现,并且设备也可被实现为该专用逻辑电路。

[0161] 适合计算机程序的执行的处理器例如包括通用微处理器和专用微处理器这两者、以及任意种类的数字计算机的处理器。通常,处理器将从只读存储器或随机存取存储器或者这两者接收指令和数据。计算机的元件可以包括用于根据指令进行动作的处理器以及用于存储指令和数据的一个或多个存储器装置。通常,计算机还可以包括例如磁盘、磁光盘或光盘的用于存储数据的一个或多个大容量存储装置,或者在操作上连接以与该一个或多个大容量存储装置进行数据的接收或传送或者接收和传送这两者。然而,计算机并非必须具有这些装置。此外,计算机可以嵌入例如以下的另一装置中:电话、电子器具、移动音频或视频播放器、游戏控制台、全球定位系统(GPS)接收器或便携式存储装置(例如,通用串行总线(USB)闪速驱动器)。适合存储计算机程序指令和数据的装置包括所有形式的非易失性存储器、介质和存储器装置,例如包含以下:半导体存储器装置(例如,EPROM、EEPROM和闪速存储器装置等);磁盘(例如,内部硬盘和可移除盘等);磁光盘;以及CD-ROM盘和DVD-ROM盘。在一些情况下,处理器和存储器可以由专用逻辑电路来补充或者并入专用逻辑电路内。

[0162] 为了提供与用户的交互,操作可以在计算机上实现,其中该计算机具有用于向用户显示信息的显示装置(例如,监视器或另一类型的显示装置)、以及用户可以使用其向计算机提供输入的键盘和指向装置(例如,鼠标、追踪球、输入板、触敏屏或另一类型的指向装置)。其它种类的装置也可以用于提供与用户的交互;例如,被提供至用户的反馈可以是任何形式的感官反馈,例如,视觉反馈、听觉反馈或触觉反馈;并且可以以任何形式接收来自

用户的输入,包括声音、语音或触觉输入。另外,计算机可以通过向用户所使用的装置发送文档并且从该装置接收文档来与用户进行交互;例如,通过响应于从用户的客户端装置上的网络浏览器接收到的请求向该网络浏览器发送网页,来与用户进行交互。

[0163] 计算机系统可以包括单个计算装置,或者在彼此附近或通常彼此远离地操作并且通常通过通信网络交互的多个计算机。通信网络的示例包括局域网(“LAN”)和广域网(“WAN”)、互连网络(例如,因特网)和对等网络(例如,点对点网络)。客户端和服务器的关系可以通过在各个计算机上运行并且彼此具有客户端-服务器关系的计算机程序而产生。

[0164] 在一般方面,使用元素信息来生成代码。在一些示例中,元素信息可以包括取向信息,并且可能地包括描述金刚石颗粒或其它类型的元素的其它信息。

[0165] 在第一示例中,接收到包括多个元素的对象。通过检测元素的扫描器系统从对象提取取向信息。取向信息指示各个元素的相对空间取向。基于取向信息来针对对象生成唯一码。

[0166] 第一示例的实现可以包括以下特征中的一个或多个。提取取向信息可以包括获得对施加到对象的照射的光学响应。提取取向信息可以包括:获得对象的荧光图像;以及根据所述荧光图像确定各个元素的相对空间取向。获得对照射的光学响应可以包括检测元素的响应于照射的变化的荧光变化,并且可以基于所检测到的荧光变化来确定相对空间取向。根据取向信息生成的唯一码可以独立于照射施加到对象的角度(例如,在该角度的变化下是不变的)。

[0167] 第一示例的实现可以包括以下特征中的一个或多个。提取取向信息可以包括:获得对施加到对象的振荡(例如,射频、微波等)电磁场的磁共振响应;以及基于磁共振响应来确定相对空间取向。获得磁共振响应可以包括:将对象定位在外部磁场中;将振荡电磁场施加到外部磁场中的对象;以及光学地检测元素的响应于外部磁场的相对变化(例如,场强度或取向的变化)、振荡电磁场的相对变化(例如,信号振幅、频率或相位的相对变化)、或者这两者的相对变化的磁共振变化。根据取向信息生成的唯一码可以独立于振荡电磁场和外部磁场施加到对象的角度(例如,在该角度的变化下是不变的)。

[0168] 第一示例的实现可以包括以下特征中的一个或多个。对象可以包括元素的超集,并且可以基于包括少于超集中的所有元素的仅元素子集的相对空间取向来生成唯一码。从对象提取的取向信息可以指示仅元素子集的相对空间取向。从对象提取的取向信息可以指示超集中的所有元素的相对空间取向,并且可以识别指示子集的相对空间取向的取向信息的子集。

[0169] 第一示例的实现可以包括以下特征中的一个或多个。可以独立于对象相对于扫描器系统的配准来提取取向信息。取向信息可以指示元素在二维坐标空间或三维坐标空间中的相对空间取向。取向信息可以是以对象的坐标系全局旋转不变的格式指示相对空间取向。

[0170] 第一示例的实现可以包括以下特征中的一个或多个。取向信息可以包括描述各个元素的相对空间取向的坐标变换(例如,变换矩阵)的列表。该列表可以包括各元素的复合变换矩阵。复合变换矩阵的列表可以是对对象的坐标系全局旋转不变的。在元素是金刚石颗粒的情况下,各元素的复合变换矩阵可以表示:对象的坐标系和金刚石颗粒的坐标系之

间的第一变换;以及金刚石颗粒的坐标系和金刚石颗粒中的色心的坐标系之间的第二变换。

[0171] 第一示例的实现可以包括以下特征中的一个或多个。元素可以是晶体颗粒,并且对象可以包括固定在介质中的晶体颗粒。晶体颗粒可以是各自具有色心的金刚石颗粒,并且提取取向信息可以包括检测色心的相对取向。

[0172] 第一示例的实现可以包括以下特征中的一个或多个。可以从对象提取指示各个元素的相对空间位置的位置信息。可以从对象提取表示各个元素的相对空间地形的地形信息。可以从对象提取指示各个元素的磁环境的磁环境信息。可以根据位置信息、地形信息、磁环境信息和取向信息的任何组合生成唯一码。

[0173] 第一示例的实现可以包括以下特征中的一个或多个。唯一码可以是第一唯一码,并且可以通过修改对象来改变至少一些元素的相对空间取向。可以基于在改变相对空间取向之后从对象提取的取向信息来生成对象的不同的第二唯一码。例如,可以使用相对空间取向作为与对象有关的信息的分类帐。

[0174] 第一示例的实现可以包括以下特征中的一个或多个。扫描器系统可以包括样品区域、探测器和处理器。样本区域可被配置为接收对象。探测器可被配置为通过检测元素来从对象提取取向信息。处理器可被配置为基于取向信息来生成对象的唯一码。探测器可以包括光学成像系统(例如,荧光成像系统),该光学成像系统被配置为通过向对象施加照射并获得对照射的光学响应(例如,荧光响应)来提取取向信息。在一些情况下,光学成像系统可被配置为基于拉曼散射或另一非线性效应(例如,二次谐波产生、自发参量下转换等)来获得光学响应。探测器可以包括磁共振系统,该磁共振系统被配置为通过向对象施加场(例如,振荡电磁场和外部磁场)并获得对场的磁共振响应来提取取向信息。

[0175] 在第二示例中,获得指示对象的各个元素的相对空间取向的取向信息。根据取向信息生成对象的唯一码。

[0176] 第二示例的实现可以包括以下特征中的一个或多个。可以将唯一码用在挑战-响应协议中。可以基于挑战-响应协议的挑战数据来提取取向信息,可以使用唯一码来生成挑战-响应协议的响应数据,并且可以将响应数据发送给认证器。

[0177] 第二示例的实现可以包括以下特征中的一个或多个。可以将唯一码用在认证过程中。可以执行认证过程以认证对象的来源。可以执行认证过程以认证对象的完整性。可以执行认证过程以认证对象的监管链。

[0178] 第二示例的实现可以包括以下特征中的一个或多个。可以将唯一码用在加密过程中。可以使用唯一码来获得加密协议、数字签名协议或另一类型的加密过程的秘密密钥。

[0179] 第二示例的实现可以包括以下特征中的一个或多个。对象可以包括元素的超集,并且可以基于包括少于超集中的所有元素的仅元素子集的相对空间取向来生成唯一码。取向信息可以指示元素在二维坐标空间或三维坐标空间中的相对空间取向。取向信息可以是以对象的坐标系全局旋转不变的格式指示相对空间取向。

[0180] 第二示例的实现可以包括以下特征中的一个或多个。取向信息可以包括描述各个元素的相对空间取向的坐标变换(例如,变换矩阵)的列表。该列表可以包括各元素的复合变换矩阵。复合变换矩阵的列表可以是对对象的坐标系全局旋转不变的。在元素是金刚石颗粒的情况下,各元素的复合变换矩阵可以表示:对象的坐标系和金刚石颗粒的坐标系之

间的第一变换；以及金刚石颗粒的坐标系和金刚石颗粒中的色心的坐标系之间的第二变换。

[0181] 在第三示例中，在对象中形成元素的悬浮，并且使用元素的悬浮来生成对象的唯一码。元素的悬浮可以是例如金刚石颗粒的悬浮。

[0182] 第三示例的实现可以包括以下特征中的一个或多个。可以通过将金刚石颗粒分布在对象的表面来形成悬浮。将金刚石颗粒分布在对象的表面可以包括将包含金刚石颗粒的涂料应用到对象的表面。将金刚石颗粒分布在对象的表面可以包括将包含金刚石颗粒的保形涂层材料应用到对象的表面。

[0183] 第三示例的实现可以包括以下特征中的一个或多个。可以通过将金刚石颗粒分布在材料中并用包含金刚石颗粒的材料形成对象来形成悬浮。用材料形成对象可以包括通过注射成型工艺形成对象。用材料形成对象可以包括通过增材制造工艺形成对象。用材料形成对象可以包括通过打印工艺形成对象。用材料形成对象可以包括用材料形成工件并从工件移除材料。

[0184] 第三示例的实现可以包括以下特征中的一个或多个。将对象从发送实体发送至接收实体，并且在发送实体和接收实体之间执行的认证过程中使用唯一码。使用金刚石颗粒的悬浮作为物理不可克隆功能 (PUF)、与对象有关的信息的分类帐或其它方式。

[0185] 第三示例的实现可以包括以下特征中的一个或多个。制造系统被配置为在对象中形成金刚石颗粒的悬浮。扫描器系统被配置为从对象提取颗粒信息，并且颗粒信息指示悬浮中的各个金刚石颗粒的性质。计算机系统被配置为基于颗粒信息生成对象的唯一码。

[0186] 在第四示例中，接收到指示对象的各个元素的相对空间取向的取向信息。根据取向信息生成认证码。认证码与对象的对象标识符相关联。

[0187] 第四示例的实现可以包括以下特征中的一个或多个。对象可以包括应用于物品的独特标记物，并且对象标识符可以是物品的序列号。可以分发物品，并且可以将认证码和序列号存储在安全认证数据库中。可以通过扫描器系统的操作从独特标记物提取取向信息，并且可以将扫描器系统为了提取取向信息所使用的扫描器设置存储在安全认证数据库中。独特标记物可以使得物品的接收方能够对物品进行认证。

[0188] 在第五示例中，进行认证过程。认证过程包括：接收对象的对象标识符；接收对象的认证码，该认证码基于所检测到的对象的各个元素的相对取向；以及基于认证码和对象标识符来认证对象。

[0189] 第五示例的实现可以包括以下特征中的一个或多个。对象可以包括应用于物品的独特标记物，并且对象标识符可以包括物品的序列号。认证对象可以包括将认证码和对象标识符通信至认证器。认证对象可以包括基于安全认证数据库中的信息来评价认证码。认证对象可以包括执行认证过程以认证对象的来源、认证对象的完整性、或者认证对象的监管链。

[0190] 在第六示例中，进行挑战-响应协议。获得挑战-响应协议的挑战数据。基于挑战数据，通过用于检测对象的各个元素的相对空间取向的扫描器系统的操作来从对象提取取向信息。挑战数据包括扫描器系统为了检测相对空间取向所使用的参数。基于取向信息，针对挑战-响应协议生成响应数据。

[0191] 第六示例的实现可以包括以下特征中的一个或多个。可以将响应数据发送至验证

器以验证挑战-响应协议的响应数据。可以从验证器接收到基于挑战数据和响应数据的挑战-响应协议的结果。获得挑战数据可以包括从验证器接收挑战数据。获得挑战数据可以包括在扫描器系统处生成挑战数据。

[0192] 在第七示例中,进行挑战-响应协议。获得挑战-响应协议的挑战数据和响应数据。挑战数据包括用于从对象提取取向信息的参数,并且响应数据基于使用该参数(例如,通过扫描器系统)从对象提取的取向信息。取向信息指示对象的各个元素的相对空间取向。使用挑战数据和响应数据来判断响应数据是否表示对挑战数据的有效响应。

[0193] 第七示例的实现可以包括以下特征中的一个或多个。判断响应数据是否表示对挑战数据的有效响应可以包括基于安全认证数据库中的有效信息来评价取向信息。可以基于挑战数据和对象的对象标识符来从安全认证数据库获得有效信息。验证器可以从远程扫描器系统接收挑战数据和响应数据,并且验证器可以将响应数据是否表示有效响应的指示发送至远程扫描器系统。

[0194] 第四示例、第五示例、第六示例和第七示例的实现可以包括以下特征中的一个或多个。元素可以是各自具有色心的金刚石颗粒,并且可以通过检测色心的相对取向来提取取向信息。提取取向信息可以包括获得对施加到金刚石颗粒的照射的光学响应(例如,荧光响应)。可以通过金刚石颗粒的光学检测到的磁共振来提取取向信息。可以在认证过程中使用认证码和对象标识符来认证对象。

[0195] 在一些实现中,一种系统包括:数据处理设备;以及计算机可读介质,其存储指令,所述指令在由所述数据处理设备执行的情况下能够操作,以进行以上示例的一个或多个操作。在一些实现中,计算机可读介质存储指令,所述指令在由所述数据处理设备执行的情况下能够操作,以进行以上示例的一个或多个操作。

[0196] 尽管本说明书包含许多细节,但这些不应当被理解为对可能要求保护的内容的范围的限制,而应被理解为对特定示例特有的特征的描述。还可以组合在分开实现的情况下在本说明书中所描述的或者在附图中示出的特定特征。相反,在单一实现的情况下所描述的或所示的各种特征还可以在多个实现中单独或以任意适当的子组合来实现。

[0197] 同样,尽管按特定顺序在附图中示出了这些操作,但这不应当被理解为为了实现期望结果就需按所示特定顺序或顺次进行这些操作、或者进行所有例示操作。在特定情形下,多任务和并行处理可能是有利的。此外,以上所述的实现中的各种系统组件的分离不应当被理解为所有实现中均需要这些分离,并且应当理解,所述的程序组件和系统通常可以集成到单个软件产品中或者封装到多个软件产品中。

[0198] 已经描述了许多实施例。然而,应该理解,可以进行各种修改。因此,其它实施例也在所附权利要求书的范围内。

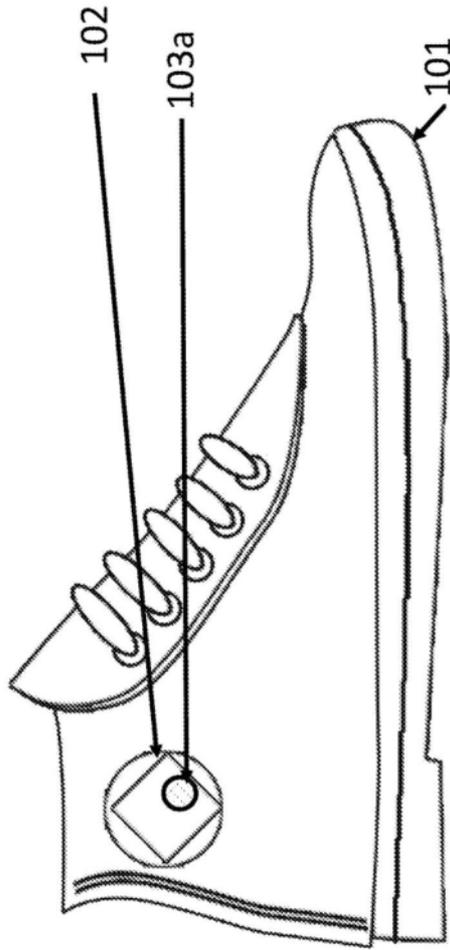


图1A

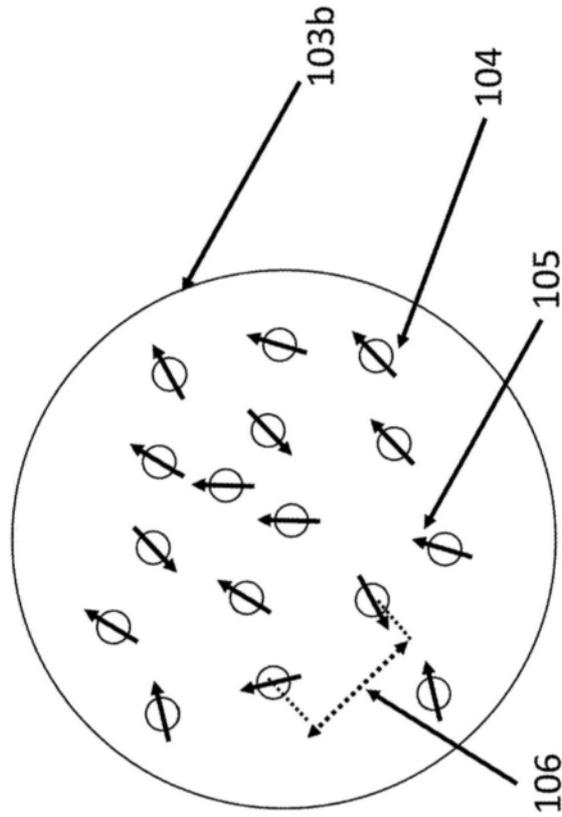


图1B

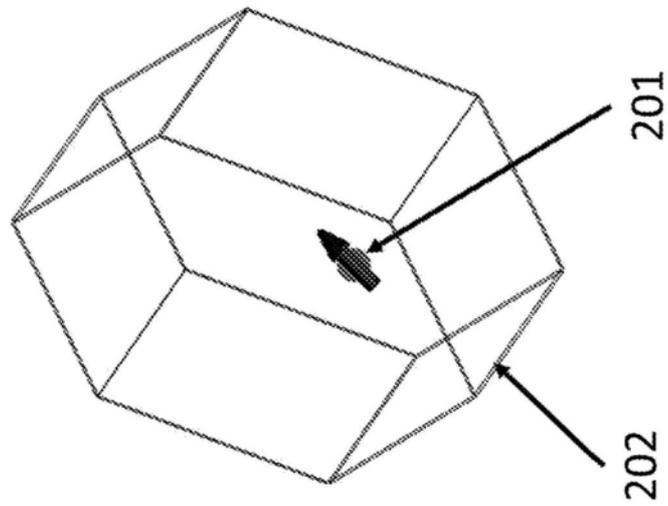


图2A

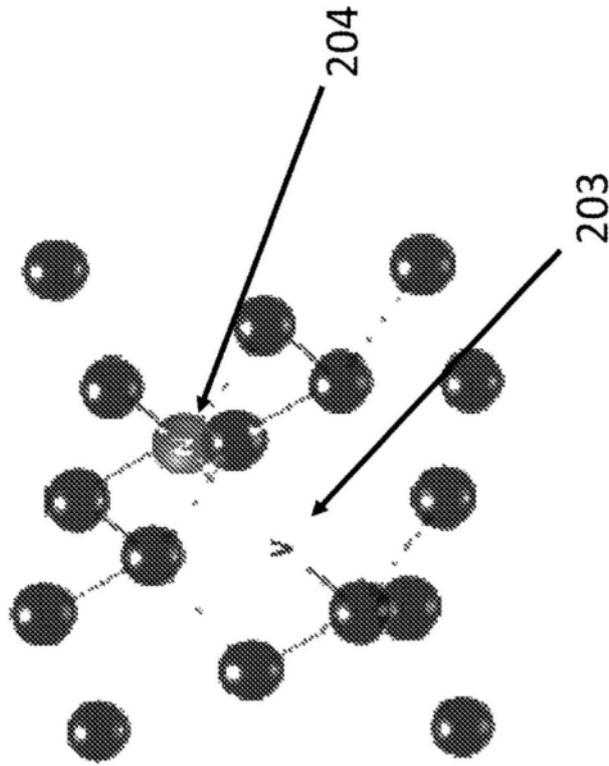


图2B

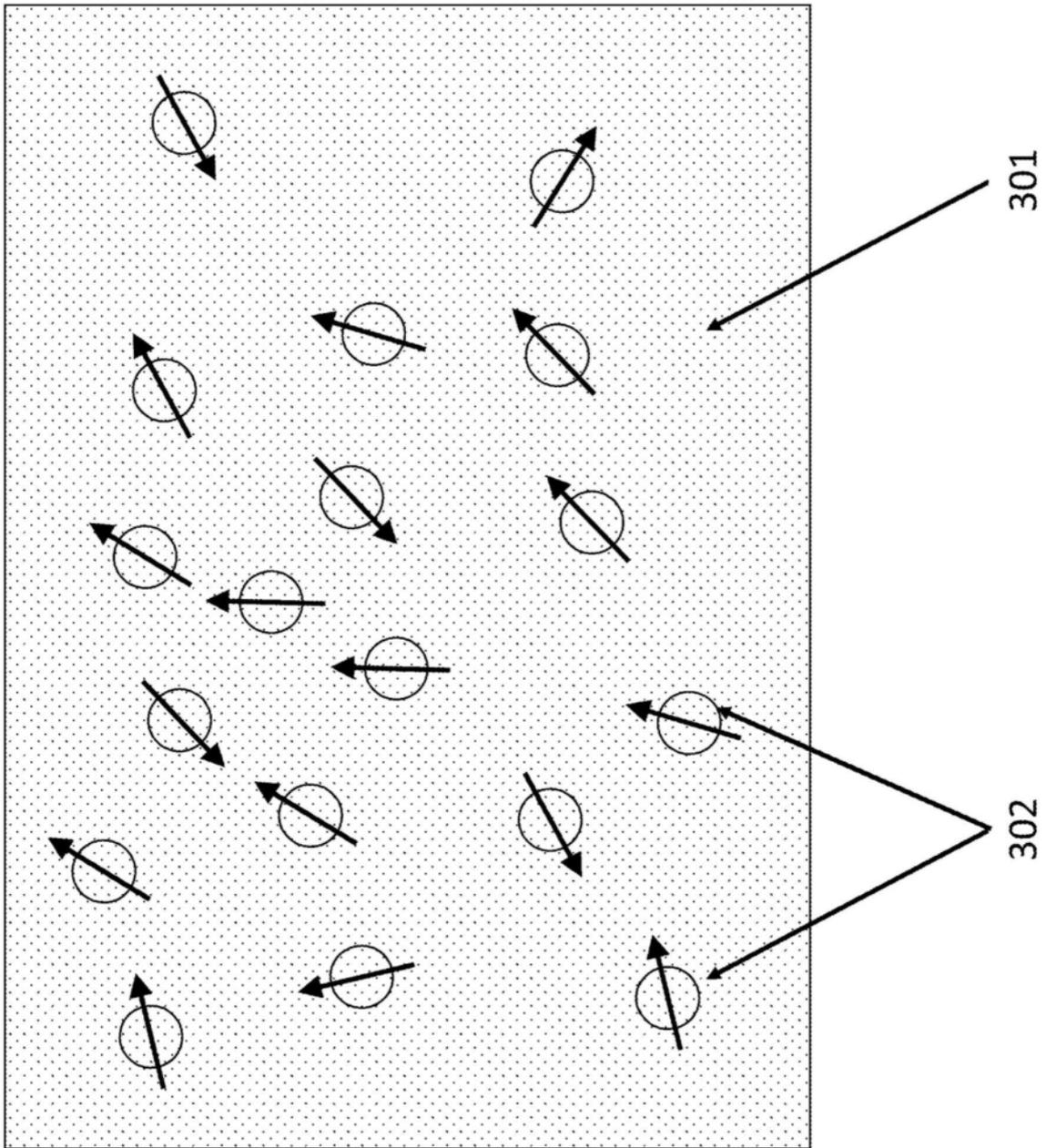


图3

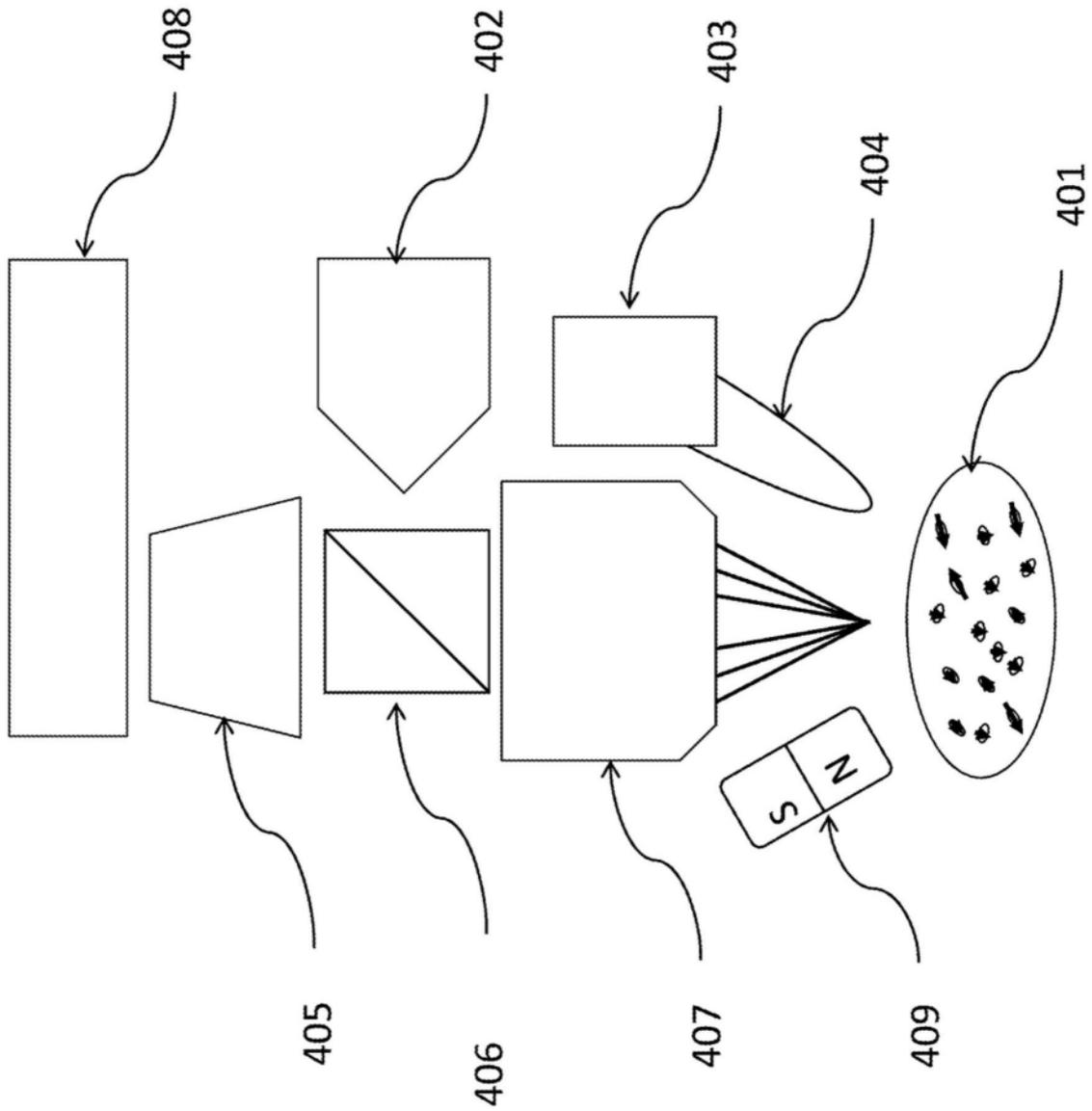


图4

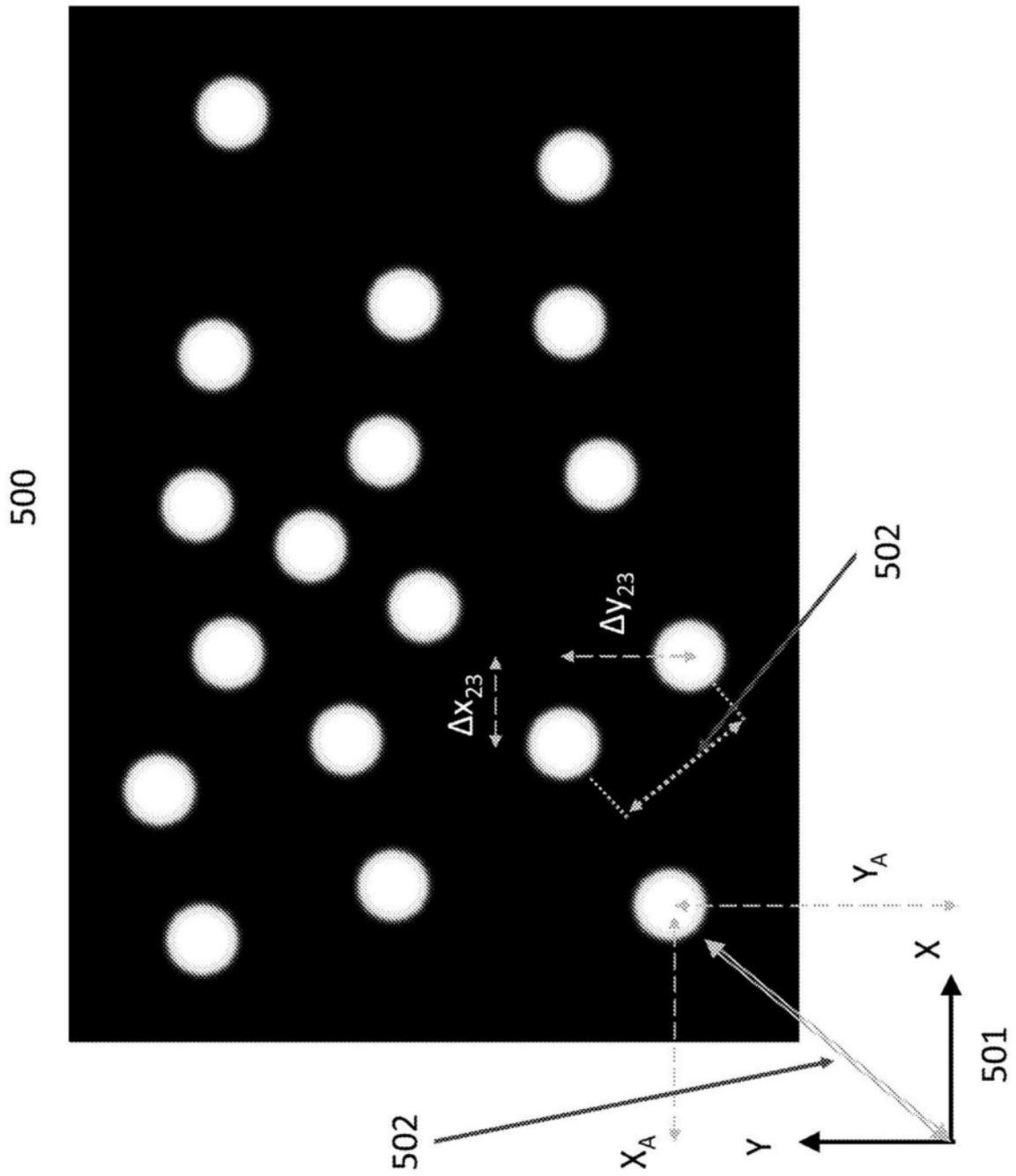


图5

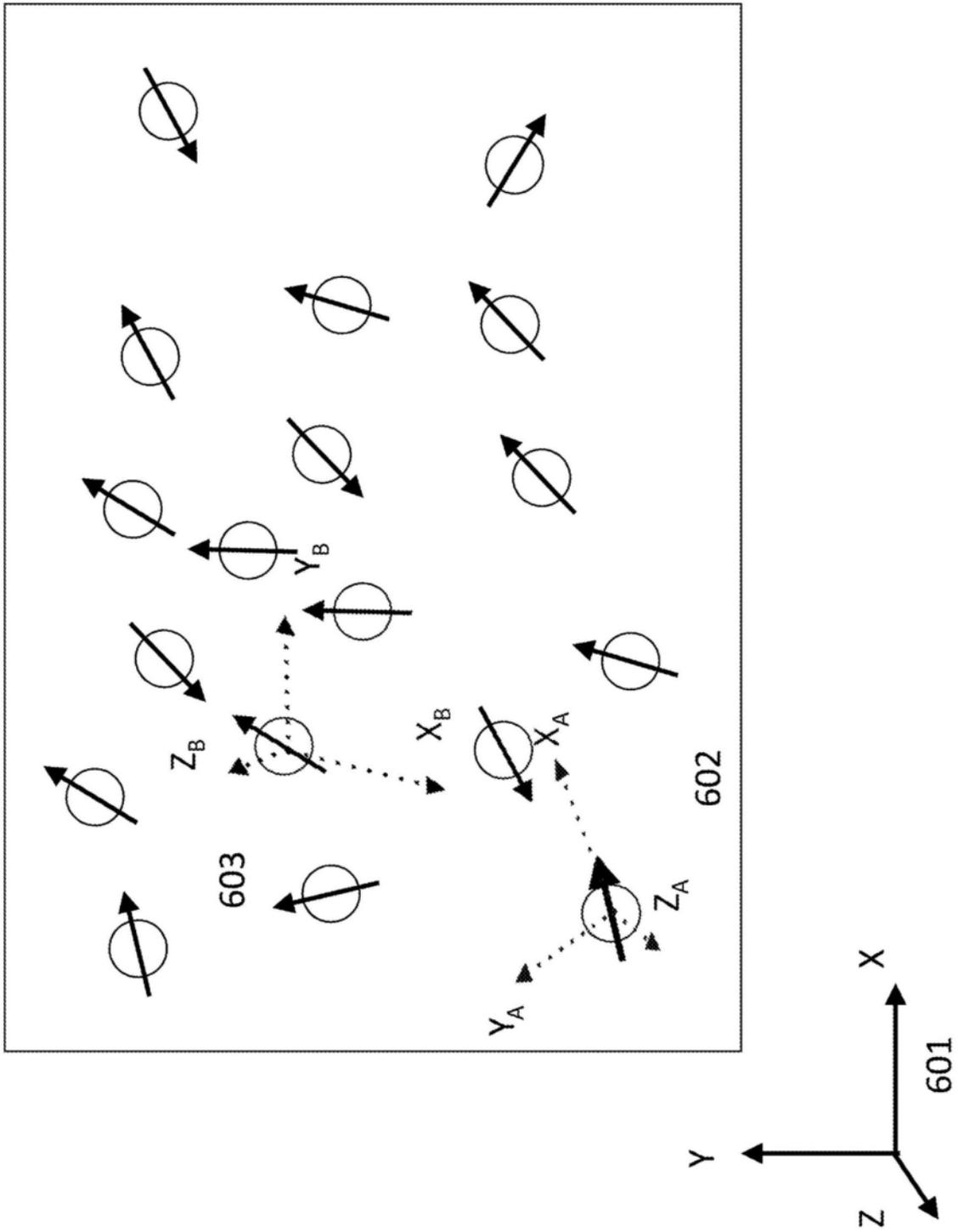
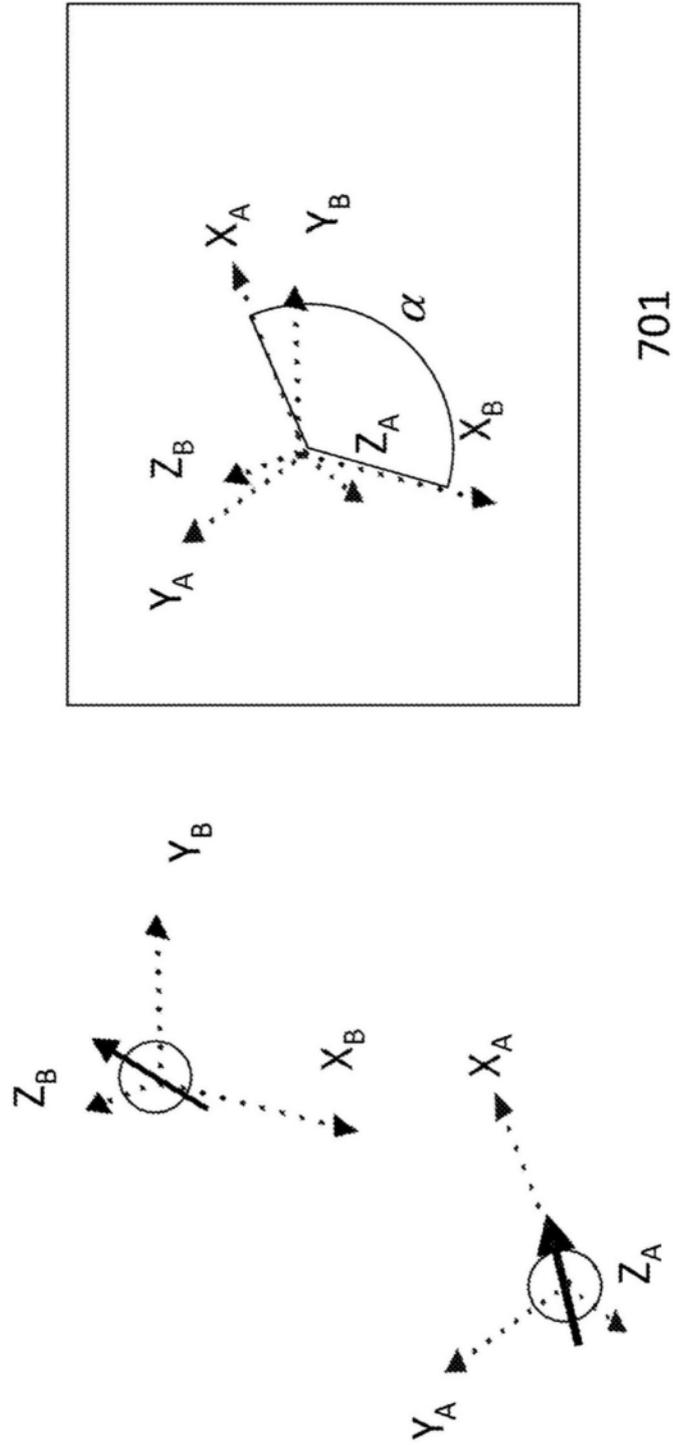


图6



701

图7

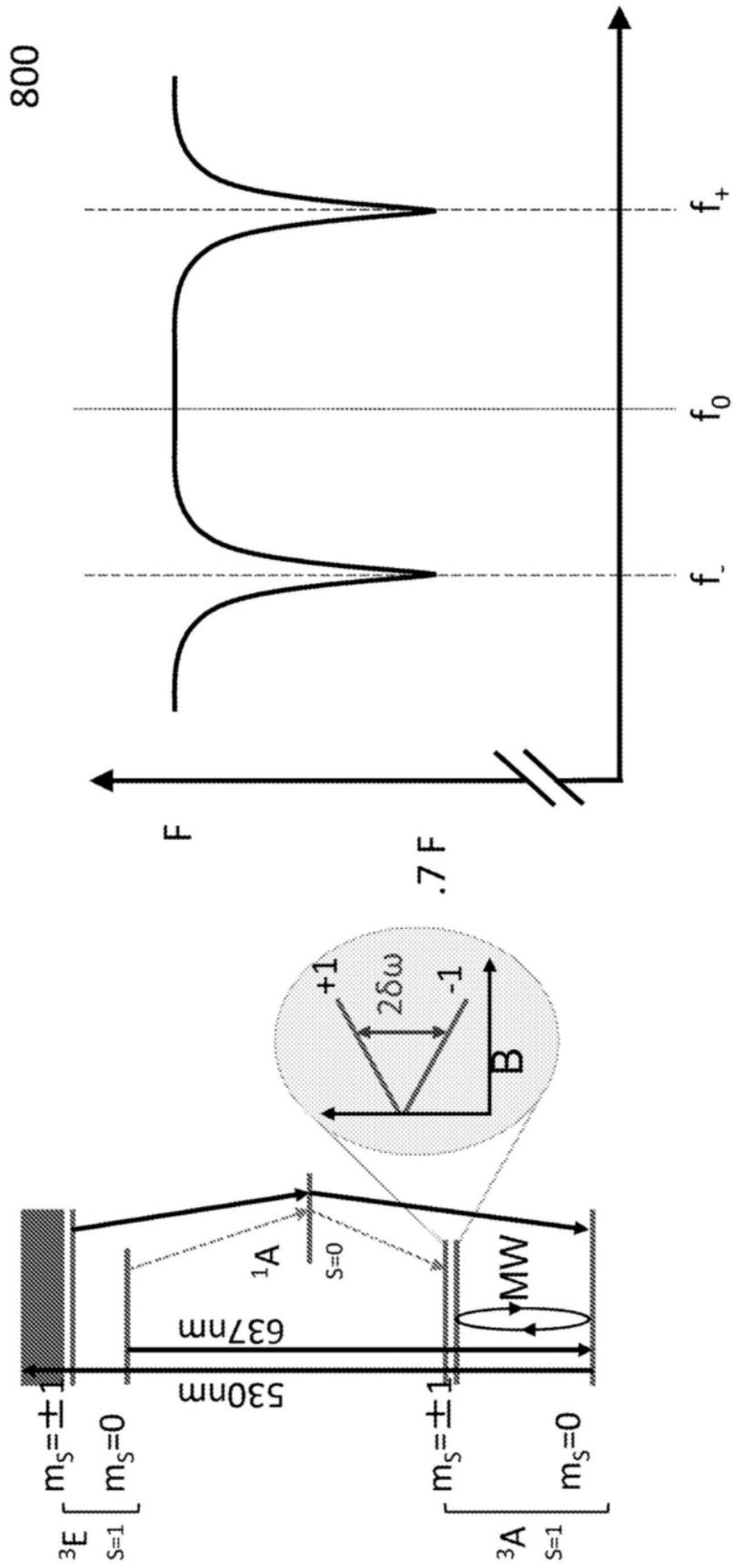


图8

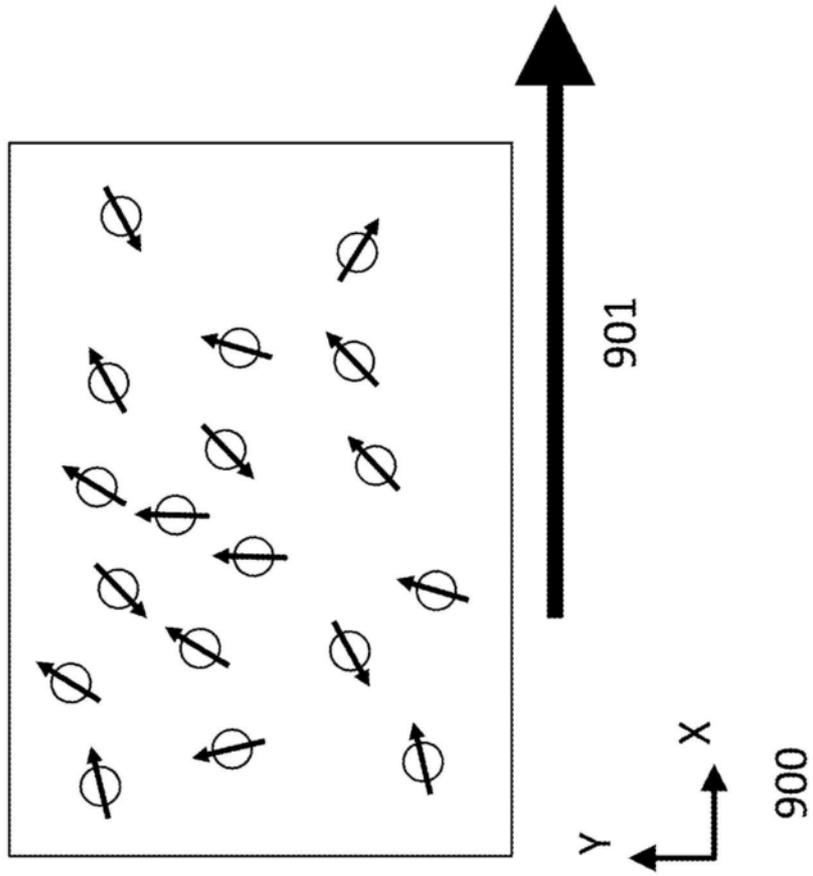


图9A

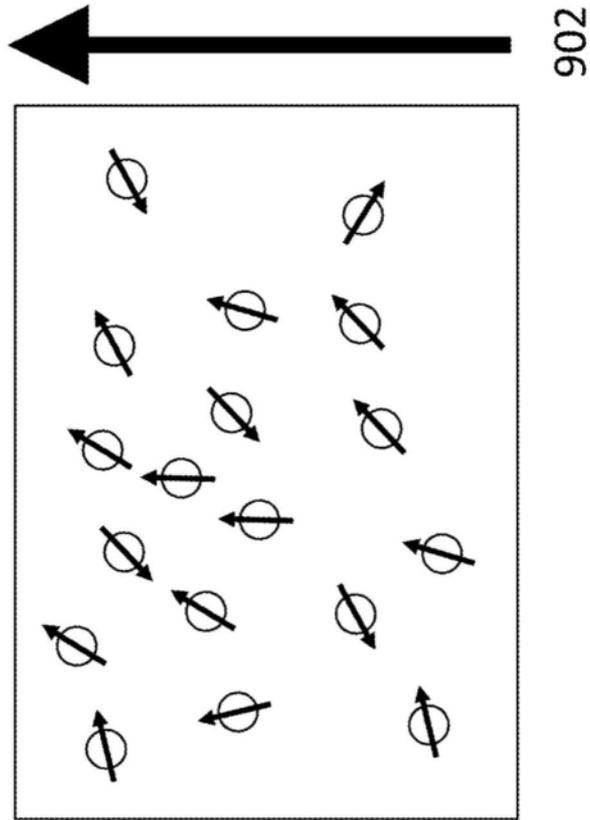


图9B

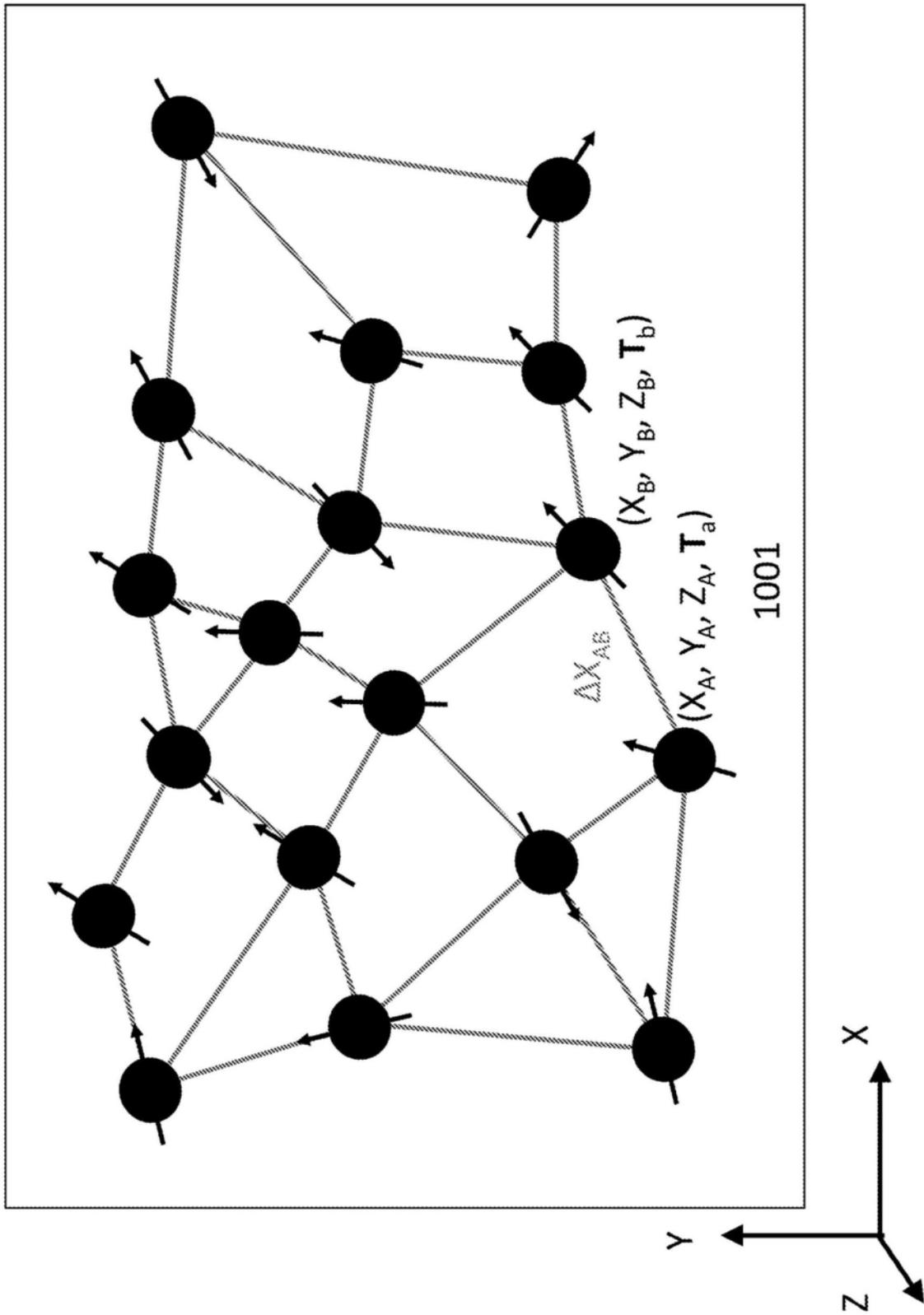
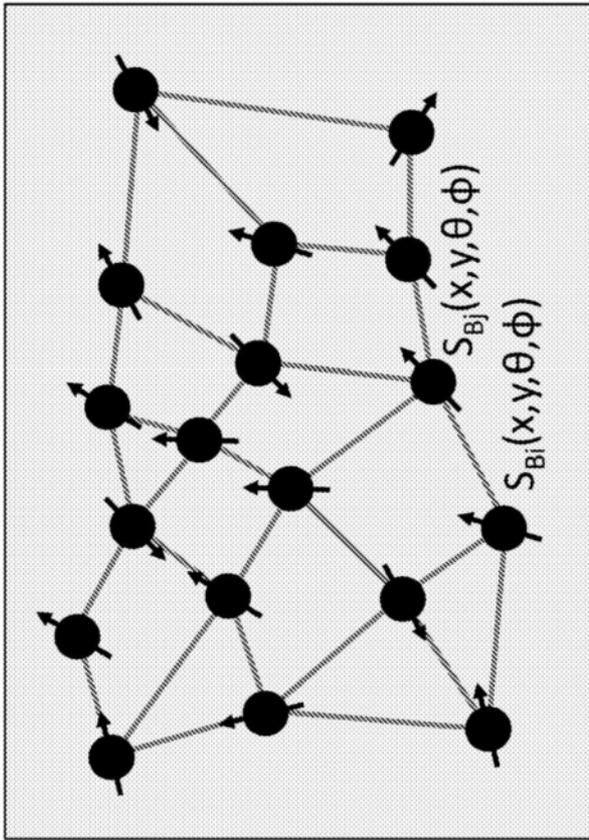
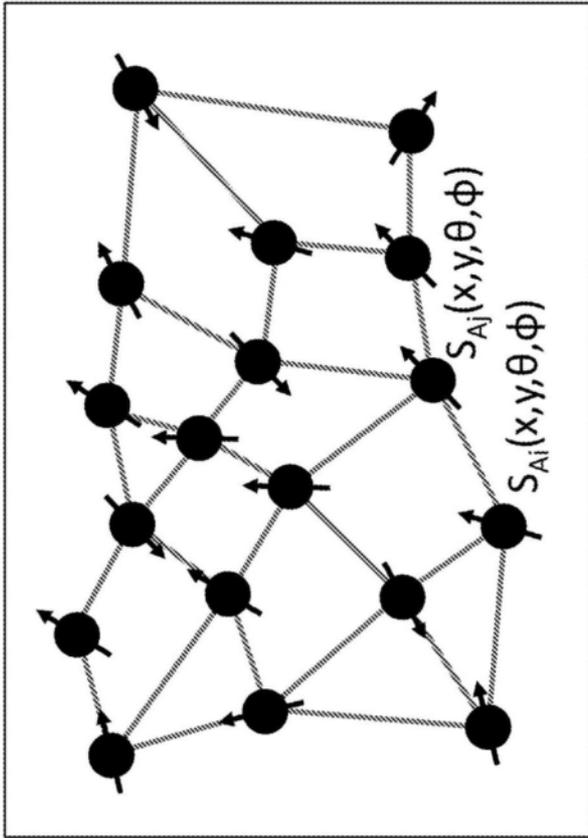


图10



1102



1101

$$| S_{Ai}(x,y,\theta,\phi) - S_{Bi}(x,y,\theta,\phi) | < \epsilon$$

1103

图 11B

图 11A

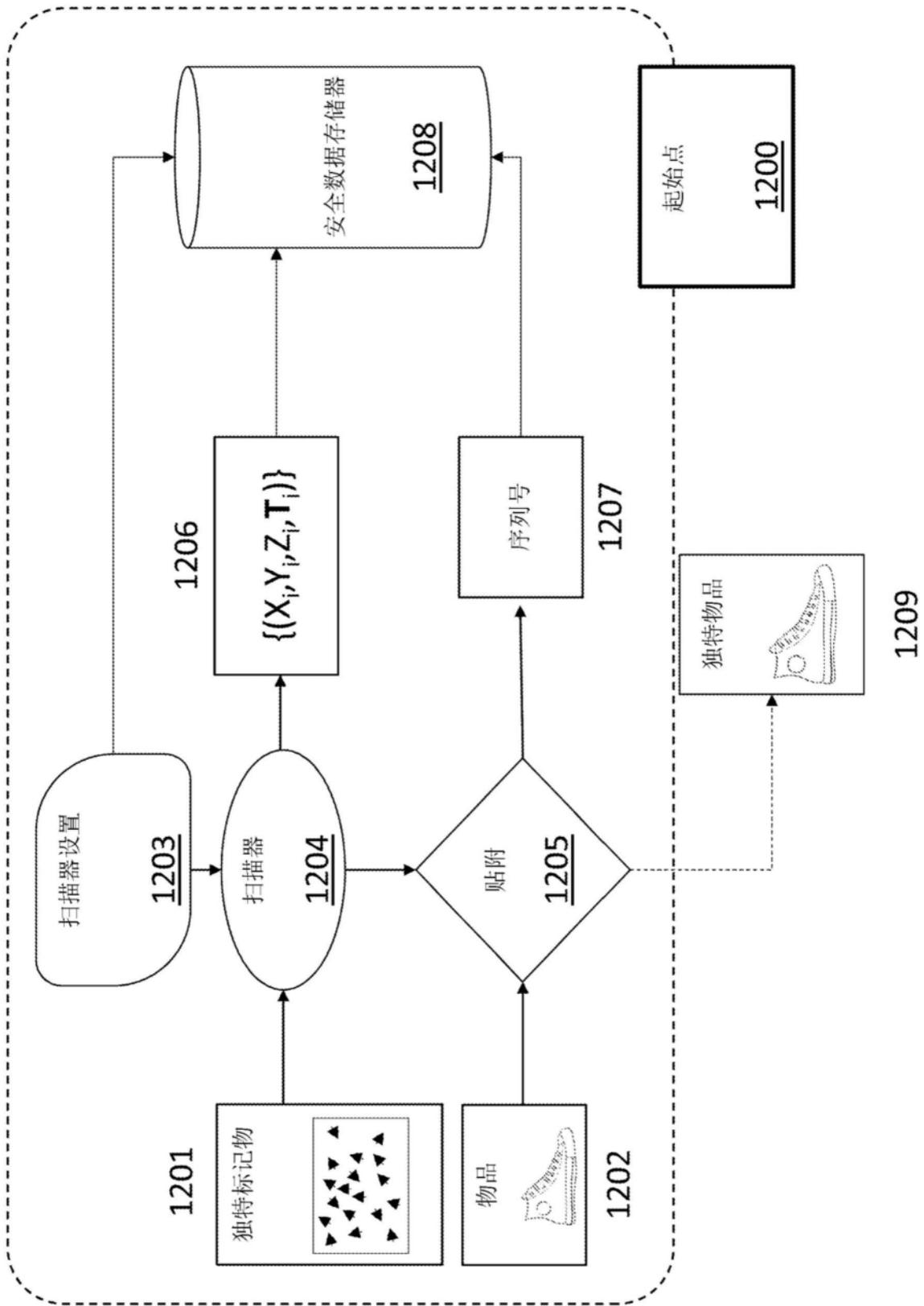


图12

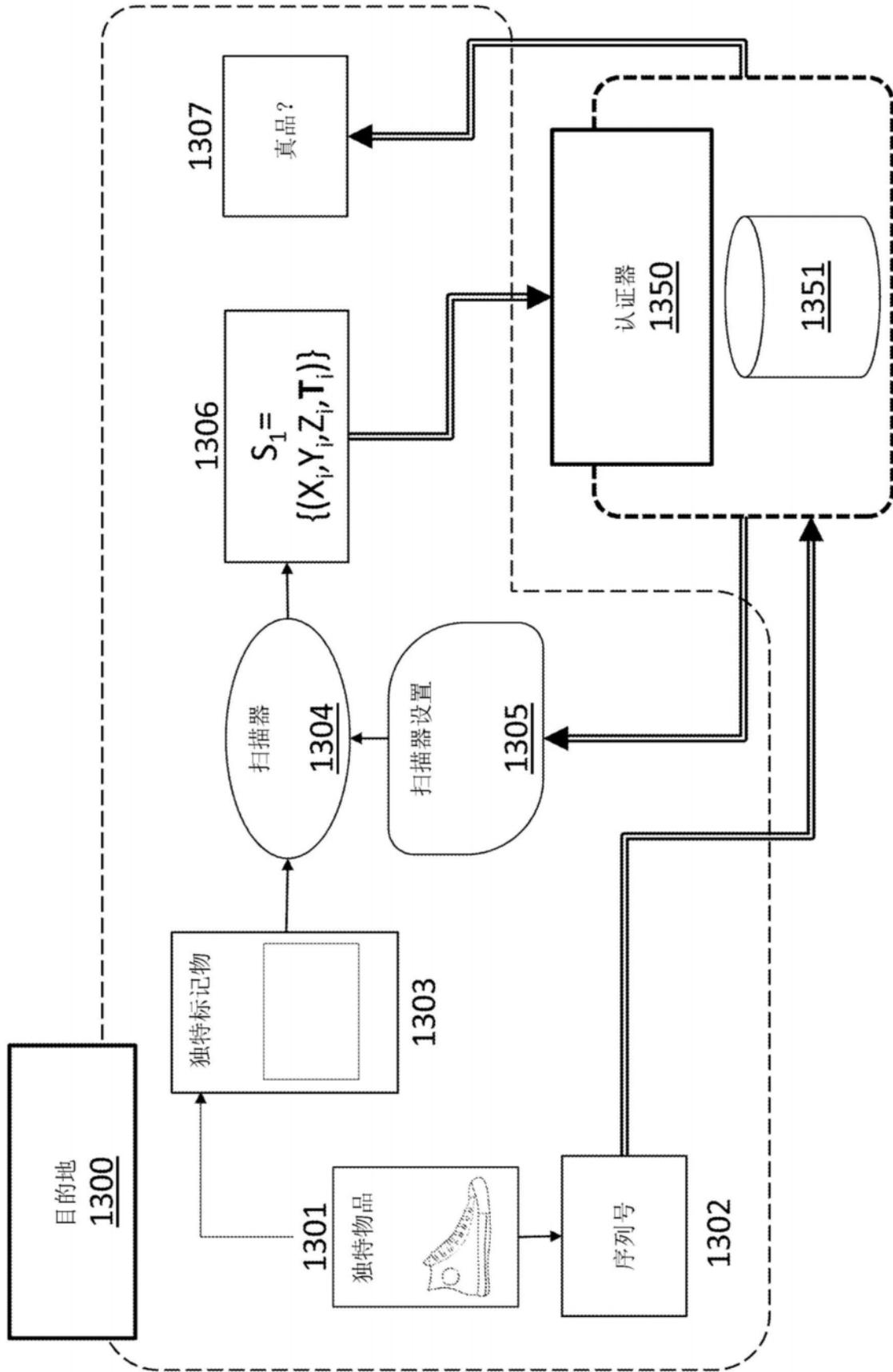


图13

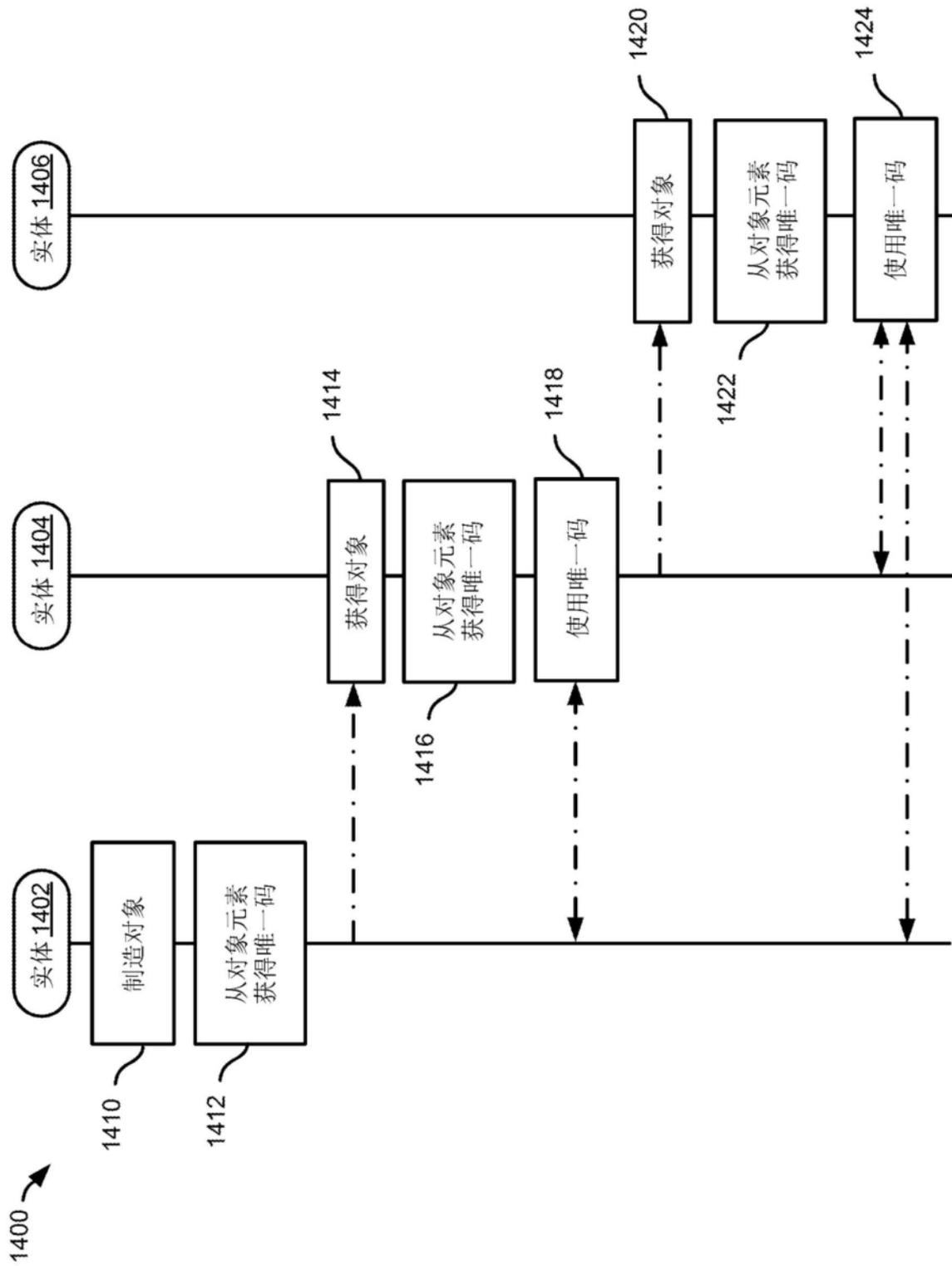


图14

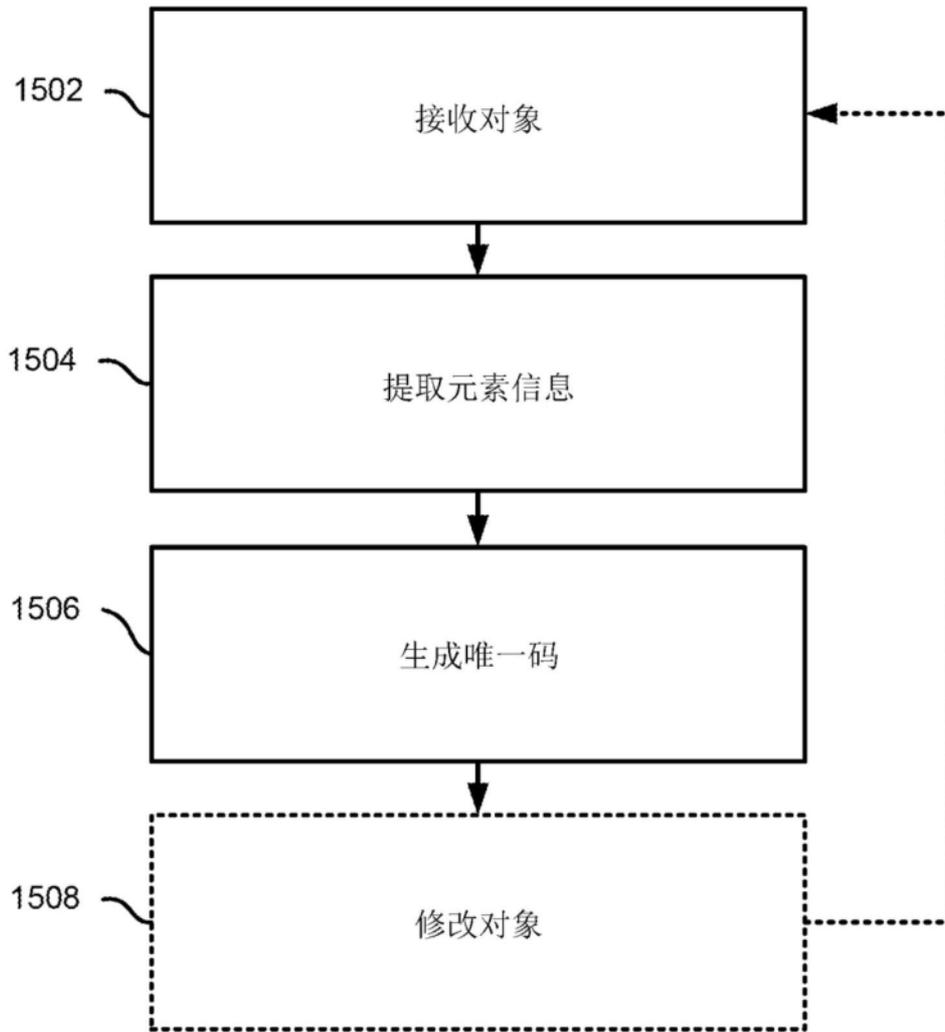


图15

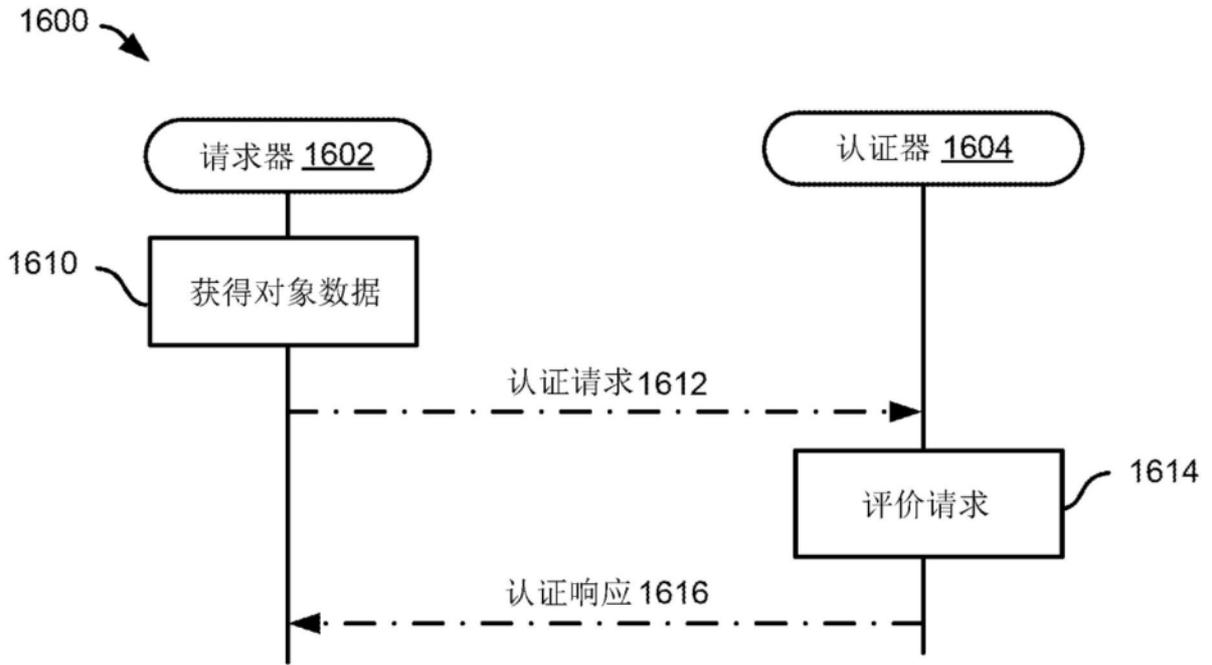


图16

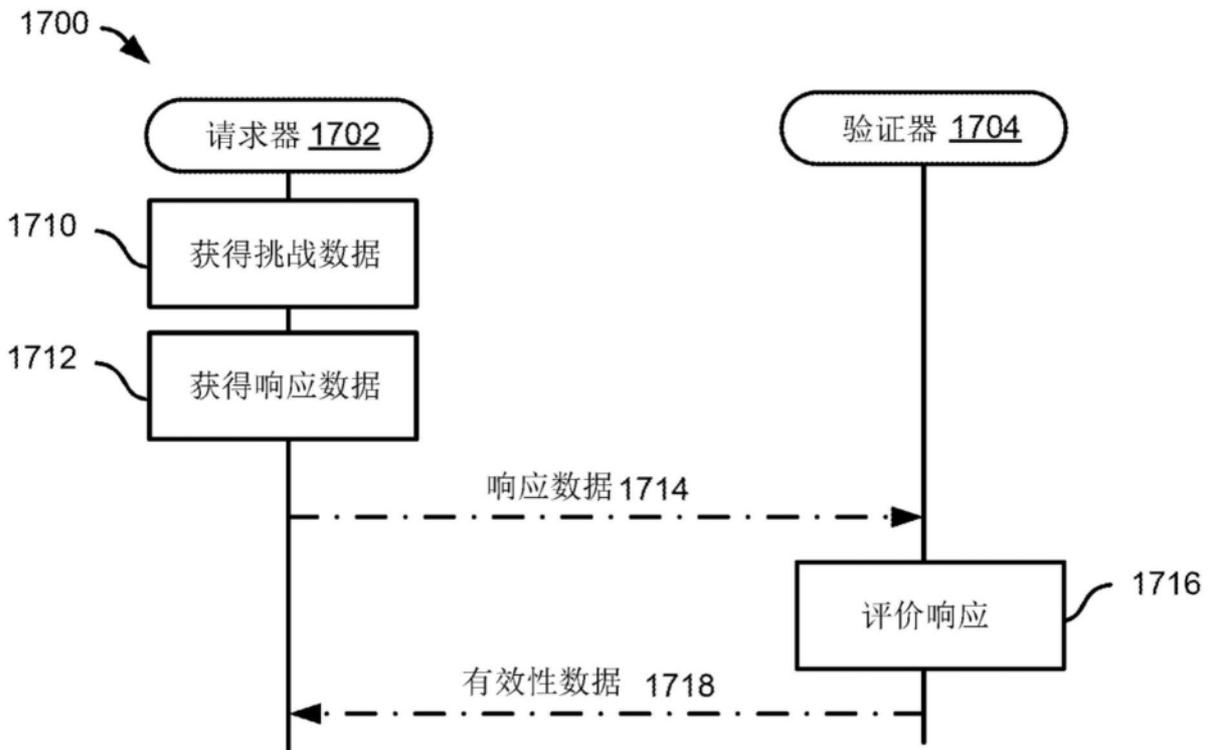


图17