

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 19/00 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200580022317.4

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101006454A

[22] 申请日 2005.1.24

[21] 申请号 200580022317.4

[30] 优先权

[32] 2004.5.18 [33] AU [31] 2004902623

[86] 国际申请 PCT/AU2005/000065 2005.1.24

[87] 国际公布 WO2005/111920 英 2005.11.24

[85] 进入国家阶段日期 2006.12.30

[71] 申请人 西尔弗布鲁克研究有限公司

地址 澳大利亚新南威尔士

[72] 发明人 卡·西尔弗布鲁克 保罗·拉普斯頓

[74] 专利代理机构 北京集佳知识产权代理有限公司

代理人 杨生平 杨红梅

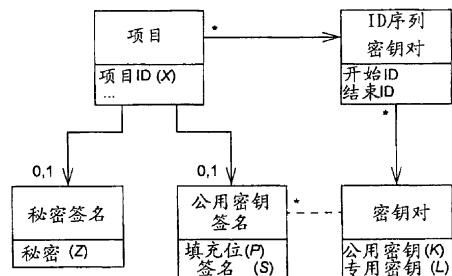
权利要求书 113 页 说明书 129 页 附图 37 页

[54] 发明名称

利用以许多数据部分编码的签名验证对象

[57] 摘要

编码数据布置在表面之上或者之内，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。



1. 一种设置在表面之上或者之内的编码数据，该编码数据包括一些编码数据部分，每个编码数据部分对如下进行编码：

身份；以及

至少部分签名，该签名是所述身份的至少部分的数字签名。

2. 根据权利要求 1 所述的编码数据，其中该签名是至少部分身份和至少部分预定填充位的数字签名。

3. 根据权利要求 2 所述的编码数据，其中该填充位与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：

预定数；以及

随机数。

4. 根据权利要求 1 所述的编码数据，其中每个数据部分至少对如下之一进行编码：

各签名单段；以及

在表面上的编码数据部分的位置。

5. 根据权利要求 1 所述的装置，其中每个编码数据部分对整个签名编码。

6. 根据权利要求 1 所述的装置，其中由多个签名部分构成整个签名，而且其中每个编码数据部分对相应的签名部分进行编码。

7. 根据权利要求 1 所述的编码数据，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

8. 根据权利要求 1 所述的编码数据，其中该编码数据对于目视基本上不可见。

9. 根据权利要求 8 所述的编码数据，其中至少利用如下之一，在表面上印刷该编码数据：

不可见油墨；以及

红外吸收油墨。

10. 根据权利要求 1 所述的编码数据，其中基本上与可见的人可读

信息重合设置该编码数据。

11. 根据权利要求 1 所述的编码数据，其中至少一些编码数据部分对指示如下至少之一的数据进行编码：

各数据部分的区位；

相应数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的身份；以及

所指示的地址的诸单元。

12. 根据权利要求 1 所述的编码数据，其中该编码数据包括至少如下之一：

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

13. 根据权利要求 1 所述的编码数据，其中该数字签名包括如下至少之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

14. 根据权利要求 1 所述的编码数据，其中至少一个编码数据部分进一步对至少数据对象片段进行编码。

15. 根据权利要求 14 所述的编码数据，其中数据对象包括至少如下

之一：

数字签名；
多用途因特网邮件扩展(MIME)数据；
文本数据；
图像数据；
声频数据；
视频数据；
应用数据；
联系数据；
业务名片数据；以及
目录数据。

16. 根据权利要求 1 所述的编码数据，其中该表面与对象相关，该对象包括至少如下之一：

制造项目；
药品项目；
钞票；
支票；
信用卡或者借记卡；
可赎回票、凭单或者息票；
彩票或者即刻兑奖票；以及
身份证件或者诸如驾驶证或者护照的身份证件。

17. 根据权利要求 1 所述的编码数据，其中该身份包括至少如下之一：

至少如下之一的身份：
用于限定该表面的对象；
该表面；
该表面上的区域；以及
与该表面相关的对象；

电子产品代码 (EPC);
国家药品代码 (NDC) 号;
药品项目序列号;
钞票属性，包括至少如下之一：
 货币;
 发行国家;
 面额;
 券面;
 印刷工厂；以及
 序列号;
支票属性，包括至少如下之一：
 货币;
 发行机构;
 账号;
 序列号;
 到期日;
 支票值；以及
 限额;
卡属性，包括至少如下之一：
 卡类型;
 发行机构;
 账号;
 发行日期;
 到期日；以及
 限额。

18. 根据权利要求 1 所述的编码数据，其中该编码数据适合被感测装置感测，以确定身份以及至少部分签名。
19. 根据权利要求 1 所述的编码数据，其中根据至少一种 n 重旋转

对称布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈相隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局区别开的旋转指示数据。

20. 根据权利要求 1 所述的编码数据，其中根据至少一种具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局对包括 n 个符号的 m 整数倍序列的取向指示数据进行编码，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向每个上来解码诸符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且它指示该布局的旋转程度。

21. 根据权利要求 1 所述的编码数据，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

22. 一种与表面相关的对象，该表面具有布置在其内或者其上、根据权利要求 1 的编码数据，该编码数据对该对象的身份进行编码。

23. 根据权利要求 1 所述的编码数据，其中该编码数据包括多个编码数据部分，每个编码数据部分对至少一数据对象片段编码，该数据部分如此排列，使得利用多个编码数据部分来对整个数据对象编码至少一次。

24. 根据权利要求 1 所述的编码数据，其中将该编码数据布置在对象表面之内或者之上。

25. 根据权利要求 1 所述的编码数据，该编码数据被用于验证对象的方法中，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，至少确定至少一被确定的签名部分；

将确定被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

26. 根据权利要求 1 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

27. 根据权利要求 1 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名片段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名片段；

利用该多个签名片段，确定被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与所产生的身份进行比较；以及

利用该比较结果，验证该对象。

28. 根据权利要求 1 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据；

根据感测的编码数据，确定：

该对象的身份；以及
多个签名片段，该签名是至少部分身份的数字签名；
利用该多个签名片段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与所产生的身份进行比较；以及
利用该比较结果，验证该对象。

29. 根据权利要求 1 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：

接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：

该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定被确定的签名；
将被确定的签名与该至少一个收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

30. 根据权利要求 1 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，每个编码数据部分对下述进行编码：

该对象的身份；以及
签名单段，该签名是至少部分身份的数字签名；
该方法包括，在处理器内：
接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

31. 根据权利要求 1 所述的编码数据，用于验证对象的装置使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：

传感器，用于感测编码数据，该编码数据对下述进行编码：
该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；以及
处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部
分；

利用该感测的身份和该至少一个感测的签名部分，验证该对象。

32. 一种布置在表面之上或者之内的编码数据，该编码数据包括许
多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少如下的数字签名：
部分身份；以及
部分预定填充位。

33. 根据权利要求 32 所述的编码数据，其中该填充位与该身份相关，
而且对于该身份是唯一的，该填充位是至少如下之一：

预定数；以及
随机数。

34. 根据权利要求 32 所述的编码数据，其中每个数据部分对签名单
段进行编码。

35. 根据权利要求 32 所述的编码数据，其中在多个数据部分内编码
整个签名。

36. 根据权利要求 32 所述的编码数据，其中该编码数据包括多个布

局，每个布局限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

37. 根据权利要求 32 所述的编码数据，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

38. 根据权利要求 32 所述的编码数据，其中该编码数据对于目视基本上不可见。

39. 根据权利要求 38 所述的编码数据，其中至少利用如下之一，在表面上印刷该编码数据：

不可见油墨；以及

红外吸收油墨。

40. 根据权利要求 32 所述的编码数据，其中基本上与可见的人可读信息重合设置该编码数据。

41. 根据权利要求 32 所述的编码数据，其中至少一些编码数据部分对指示如下至少之一的数据进行编码：

相应数据部分的区位；

相应数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的身份；以及

所指示的区位的诸单元。

42. 根据权利要求 32 所述的编码数据，其中该编码数据包括至少如下之一：

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

43. 根据权利要求 32 所述的编码数据，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

44. 根据权利要求 32 所述的编码数据，其中该身份包括至少如下之一的身份：

用于限定该表面的对象；
该表面；
该表面上的区域；以及
与该表面相关的对象。

45. 根据权利要求 32 所述的编码数据，其中至少一个编码数据部分进一步对至少数据对象片段进行编码。

46. 根据权利要求 45 所述的编码数据，其中数据对象包括至少如下之一：

数字签名；
多用途因特网邮件扩展(MIME)数据；
文本数据；
图像数据；
声频数据；
视频数据；
应用数据；
联系数据；
业务名片数据；以及
目录数据。

47. 根据权利要求 32 所述的编码数据，其中该表面与对象相关，该

对象包括至少如下之一：

制造项目；

药品项目；

钞票；

支票；

信用卡或者借记卡；

可赎回票、凭单或者息票；

彩票或者即刻兑奖票；以及

身份证件或者诸如驾驶证或者护照的身份证件。

48. 根据权利要求 32 所述的编码数据，其中该身份包括至少如下之一：

电子产品代码 (EPC)；

国家药品代码 (NDC) 号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

49. 根据权利要求 32 所述的编码数据，其中该编码数据适合被感测装置感测，以确定身份以及至少部分的签名。

50. 根据权利要求 32 所述的编码数据，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他的子布局区别的旋转指示数据。

51. 根据权利要求 32 所述的编码数据，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上对诸符号解码产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且它指示该布局的旋转程度。

52. 一种与表面相关的对象，该表面具有布置在其内或者其上、根据权利要求 32 的编码数据，该编码数据对该对象的身份进行编码。

53. 根据权利要求 32 所述的编码数据，该编码数据布置在表面之上或者之内，该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数

据部分。

54. 根据权利要求 32 所述的编码数据，其中将该编码数据布置在对象表面之上或者之内。

55. 根据权利要求 32 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

56. 根据权利要求 32 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

57. 根据权利要求 32 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，

该指示数据指示：

该对象的身份；以及
多个签名人段，该签名是至少部分身份的数字签名；
利用该指示数据，确定该身份和多个签名人段；
利用该多个签名人段，确定被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与所产生的身份进行比较；以及
利用该比较结果，验证该对象。

58. 根据权利要求 32 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据；
根据感测的编码数据，确定：
该对象的身份；以及
多个签名人段，该签名是至少部分身份的数字签名；
利用该多个签名人段，确定被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

59. 根据权利要求 32 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：

接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定被确定的签名；

将被确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

60. 根据权利要求 32 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；

将被确定的身份与收到的身份进行比较；以及

利用该比较结果，验证该对象。

61. 根据权利要求 32 所述的编码数据，用于验证对象的装置使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：

传感器，用于感测编码数据，该编码数据编码：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；以及

处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用感测的身份和至少一个感测的签名部分，验证该对象。

62. 一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

至少部分身份；以及
至少数据对象片段；
以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

63. 根据权利要求 62 所述的编码数据，其中该数据对象包括至少部分签名，该签名是至少部分身份的数字签名。

64. 根据权利要求 63 所述的编码数据，其中该签名是至少部分身份和至少部分预定填充位的数字签名。

65. 根据权利要求 64 所述的编码数据，其中该填充位与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：

预定数；以及
随机数。

66. 根据权利要求 62 所述的编码数据，其中每个数据部分对整个签名编码，该签名是至少部分身份的数字签名。

67. 根据权利要求 62 所述的编码数据，其中该编码数据由多个签名部分构成，该签名是至少部分身份的数字签名，而且其中以多个数据部分来编码整个签名的方式，每个编码数据部分编码相应的签名部分。

68. 根据权利要求 62 所述的编码数据，其中在多个数据部分内来编码该数据对象。

69. 根据权利要求 62 所述的编码数据，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分数据对象的第二符号的位置。

70. 根据权利要求 62 所述的编码数据，其中该编码数据对于目视基本上不可见。

71. 根据权利要求 70 所述的编码数据，其中利用至少如下之一，在表面上印刷该编码数据：

不可见油墨；以及
红外吸收油墨。

72. 根据权利要求 62 所述的编码数据，其中基本上与可见的人可读信息重合设置该编码数据。

73. 根据权利要求 73 所述的编码数据，其中至少一些编码数据部分来编码指示至少如下之一的数据：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

数据对象的大小；

数据对象片段的身份；以及

被指示区位的诸单元。

74. 根据权利要求 62 所述的编码数据，其中该编码数据包括至少如下之一：

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

75. 根据权利要求 66 所述的编码数据，其中该签名包括至少如下之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

76. 根据权利要求 62 所述的编码数据，其中数据对象包括至少如下之一：

多用途因特网邮件扩展(MIME)数据；
文本数据；
图像数据；
声频数据；
视频数据；
应用数据；
联系数据；
业务名片数据；以及
目录数据。

77. 根据权利要求 62 所述的编码数据，其中该表面与对象相关，该对象包括至少如下之一：

制造项目；
药品项目；
钞票；
支票；
信用卡或者借记卡；
可赎回票、凭单或者息票；
彩票或者即刻兑奖票；以及
身份证件或者诸如驾驶证或者护照的身份证件。

78. 根据权利要求 62 所述的编码数据，其中该身份包括至少如下之一：

至少如下之一的身份：
用于限定该表面的对象；
该表面；
该表面上的区域；以及
与该表面相关的对象；
电子产品代码 (EPC)；
国家药品代码 (NDC) 号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

79. 根据权利要求 62 所述的编码数据，其中该编码数据适合被感测装置感测，以确定至少如下之一：

身份；

编码数据部分在该表面上的位置；以及

数据对象。

80. 根据权利要求 62 所述的编码数据，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他另一个子布局区别开的旋转指示数据。

81. 根据权利要求 62 所述的编码数据，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码诸符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

82. 根据权利要求 62 所述的编码数据，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

83. 一种与表面相关的对象，该表面具有布置在其内或者其上、根据权利要求 62 的编码数据，该编码数据编码该对象的身份和与该对象相关的数据对象。

84. 根据权利要求 62 所述的编码数据，每个编码数据部分进一步编码至少部分签名，该签名是至少部分身份的数字签名。

85. 根据权利要求 62 所述的编码数据，每个编码数据部分进一步编码至少部分签名，该签名是至少如下之一的数字签名：

部分身份；以及

部分预定填充位。

86. 根据权利要求 62 所述的编码数据，编码数据布置在对象表面之内或者之上，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

87. 根据权利要求 62 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

88. 根据权利要求 62 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

89. 根据权利要求 62 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名片段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名片段；

利用该多个签名片段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

90. 根据权利要求 62 所述的编码数据，在验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：

感测该编码数据；

根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

91. 根据权利要求 62 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：

接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用收到的身份和保密密钥，确定一被确定的签名；

将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

92. 根据权利要求 62 所述的编码数据，在使用处理器验证对象的方法中使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，每个编码数据部分进一步编码签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；

将被确定的身份与收到的身份进行比较；以及

利用该比较结果，验证该对象。

93. 根据权利要求 62 所述的编码数据，用于验证对象的装置使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：

传感器，用于感测编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；以及

处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用感测的身份和该至少一个感测的签名部分，验证该对象。

94. 一种具有表面的对象，该表面具有布置在其上或者其内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

95. 根据权利要求 94 所述的对象，其中该签名是至少部分身份和至少部分预定填充位的数字签名。

96. 根据权利要求 94 所述的对象，其中该填充位与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：

预定数；以及

随机数。

97. 根据权利要求 94 所述的对象，其中每个数据部分编码签名片段。

98. 根据权利要求 97 所述的对象，其中在多个数据部分内编码整个签名。

99. 根据权利要求 94 所述的对象，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

100. 根据权利要求 94 所述的对象，其中该编码数据对于目视基本上不可见。

101. 根据权利要求 100 所述的对象，其中至少利用如下之一，在表面上印刷该编码数据：

不可见油墨；以及

红外吸收油墨。

102. 根据权利要求 94 所述的对象，其中基本上与可见的人可读信息重合设置该编码数据。

103. 根据权利要求 94 所述的对象，其中至少一些编码数据部分编码至少表示如下之一的数据：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的身份；以及

被指示区位的诸单元。

104. 根据权利要求 94 所述的对象，其中该编码数据包括至少如下之一：

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及
循环冗余校验（CRC）数据。

105. 根据权利要求 94 所述的对象，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键
控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

106. 根据权利要求 94 所述的对象，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

107. 根据权利要求 94 所述的对象，其中至少一个编码数据部分进一步对至少数据对象片段进行编码。

108. 根据权利要求 107 所述的对象，其中数据对象包括至少如下之一：

数字签名；
多用途因特网邮件扩展(MIME)数据；
文本数据；
图像数据；
声频数据；
视频数据；
应用数据；
联系数据；

业务名片数据；以及
目录数据。

109. 根据权利要求 94 所述的对象，其中该对象包括至少如下之一：
制造项目；
药品项目；
钞票；
支票；
信用卡或者借记卡；
可赎回票、凭单或者息票；
彩票或者即刻兑奖票；以及
身份证件或者诸如驾驶证或者护照的身份证件。

110. 根据权利要求 94 所述的对象，其中该身份包括至少如下之一：
电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：

货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；
到期日；

支票值；以及
限额；以及
卡属性，包括至少如下之一：
卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

111. 根据权利要求 94 所述的对象，其中该编码数据适合被感测装置感测，以确定身份以及至少部分签名。

112. 根据权利要求 94 所述的对象，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他的子布局区别开的旋转指示数据。

113. 根据权利要求 94 所述的对象，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

114. 根据权利要求 94 所述的对象，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

115. 根据权利要求 94 所述的对象，其中以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

116. 根据权利要求 94 所述的对象，在验证该对象的方法中使用该对象，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上

或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

117. 根据权利要求 94 所述的对象，在验证该对象的方法中使用该对象，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

118. 根据权利要求 94 所述的对象，在验证对象的方法中使用该对象，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名单段；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

119. 根据权利要求 94 所述的对象，在验证该对象的方法中使用该对象，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；

根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

120. 根据权利要求 94 所述的对象，在使用处理器验证该对象的方法中使用该对象，该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用收到的身份和保密密钥，确定一被确定的签名；

将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

121. 根据权利要求 94 所述的对象，在使用处理器验证该对象的方法中使用该对象，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

122. 根据权利要求 94 所述的对象，用于验证该对象的装置使用该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：
身份；以及

至少一部分签名，该签名是至少部分身份的数字签名；以及
处理器，用于：
利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用感测的身份和至少一个感测的签名部分，验证该对象。

123. 一种用于验证对象的方法，该方法包括，在计算机系统中：
从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：
该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和收到的签名部分；
利用收到的身份，确定至少一被确定的签名部分；
将被确定的签名部分与收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

124. 根据权利要求 123 所述的方法，其中该方法包括，在计算机系统中：

产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

125. 根据权利要求 124 所述的方法，其中该方法包括，在计算机系统中，将该验证数据传送到感测装置。

126. 根据权利要求 123 所述的方法，其中该指示数据进一步表示签名部分的身份，而且其中该方法包括，在计算机系统中：

利用该指示数据，确定收到的签名部分身份；

利用收到的身份，确定一被确定的签名；以及

利用该被确定的签名和收到的签名部分身份，确定一被确定的签名部分。

127. 根据权利要求 123 所述的方法，其中该方法包括，在计算机系统中，利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；

专用密钥；

公用密钥；

一个或者多个数字签名部分；以及

数字签名。

128. 根据权利要求 127 所述的方法，其中该存储数据存储在数据库中，而且利用如下至少之一索引该存储数据：

该身份；以及

一范围的身份。

129. 根据权利要求 127 所述的方法，其中该方法包括，在计算机系统中，利用该存储数据和收到的身份，产生确定的签名部分。

130. 根据权利要求 127 所述的方法，其中该方法包括，在计算机系统中：

利用该存储数据和收到的身份，产生确定的签名；

选择确定的签名的一部分；以及

将选择的签名部分与收到的签名部分进行比较。

131. 根据权利要求 130 所述的方法，其中该方法包括，在计算机系统中：

利用指示数据确定收到的签名部分身份；

利用收到的签名部分身份，选择部分确定的签名。

132. 根据权利要求 123 所述的方法，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在计算机系统中：

利用收到的身份，确定预定填充位；以及

利用该预定填充位和收到的身份，确定一被确定的签名部分。

133. 根据权利要求 123 所述的方法，其中计算机系统构成该感测装置的部分。

134. 根据权利要求 123 所述的方法，其中编码数据包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：

至少部分身份；

至少部分签名；以及

编码数据部分在该表面上的位置。

135. 根据权利要求 134 所述的方法，其中每个编码数据部分编码整个签名。

136. 根据权利要求 134 所述的方法，其中整个签名由多个签名部分构成，而且其中每个编码数据部分编码相应的签名部分。

137. 根据权利要求 134 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名部分的大小；

签名部分的身份；

被指示区位的诸单元；
冗余数据；
允许纠错的数据；
里德-索罗门数据；以及
循环冗余校验（CRC）数据。

138. 根据权利要求 123 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

139. 根据权利要求 123 所述的方法，其中该身份包括至少如下之一：至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域；
电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：
货币；
发行国家；
面额；
券面；
印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

140. 根据权利要求 123 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局区别开的旋转指示数据。

141. 根据权利要求 123 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码诸符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

142. 一种用于验证对象的方法，该方法包括，在感测装置内：

感测设置在与该对象相关的表面之上或者之内的编码数据；

利用感测的编码数据，确定指示如下所述的指示数据：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；以及

将该指示数据传送到计算机系统，该计算机系统响应该指示数据，以：

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

143. 根据权利要求 142 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分编码该身份以及至少部分签名，该方法包括至少感测一个数据部分。

144. 根据权利要求 142 所述的方法，其中该方法包括，在感测装置内：

接收表示该验证是成功还是失败的验证数据；以及

将该验证是成功还是失败的指示提供给用户。

145. 根据权利要求 142 所述的方法，其中在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：

感测许多编码部分；以及

产生指示整个签名的指示数据。

146. 根据权利要求 142 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

147. 根据权利要求 142 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

148. 根据权利要求 142 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

149. 根据权利要求 142 所述的方法，其中计算机系统构成该感测装

置的部分。

150. 根据权利要求 142 所述的方法，其中该方法包括，在该感测装置内，通过至少如下之一，与该计算机系统通信：

通信网；
因特网；
移动电话网；以及
无线连接。

151. 根据权利要求 142 所述的方法，其中该方法包括，在该感测装置内，产生至少指示如下之一的指示：

各数据部分的区位；
各数据部分在表面上的位置；
数据部分的大小；
签名的大小；
签名单段的身份；
被指示区位的诸单元；
冗余数据；
允许纠错的数据；
里德-索罗门数据；以及
循环冗余校验（CRC）数据。

152. 根据权利要求 142 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

153. 根据权利要求 142 所述的方法，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

154. 根据权利要求 142 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：
货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；
到期日；
支票值；以及
限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；

发行日期；
到期日；以及
限额。

155. 根据权利要求 142 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局区别开的旋转指示数据。

156. 根据权利要求 142 所述的方法，其中至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码诸符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

157. 根据权利要求 123 所述的方法，其中设置在与该对象相关的表面之上或者之内的编码数据包括许多编码数据部分，每个编码数据部分对如下进行编码：

身份；以及
至少部分签名，该签名是至少部分身份的数字签名。

158. 根据权利要求 123 所述的方法，其中设置在与该对象相关的表面之上或者之内的编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少如下的数字签名：
部分身份；以及
部分预定填充位。

159. 根据权利要求 123 所述的方法，其中设置在与该对象相关的表面之上或者之内的编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少数据对象片段；
以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

160. 根据权利要求 123 所述的方法，其中该方法进一步包括：
感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：

该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用感测的编码数据，确定感测的身份和感测的签名部分；
利用感测的身份，确定至少一被确定的签名部分；
将被确定的签名部分与感测的签名部分进行比较；以及
利用该比较结果，验证该对象。

161. 根据权利要求 123 所述的方法，该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及
多个签名片段，该签名是至少部分身份的数字签名；
利用该指示数据，确定该身份和多个签名片段；
利用多个签名片段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

162. 根据权利要求 123 所述的方法，该方法进一步包括：
感测设置在与该对象相关的表面之上或者之内的编码数据；
根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；
利用该多个签名单段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

163. 根据权利要求 123 所述的方法，其中利用处理器验证该对象，
该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的
编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定一被确定的签名；
将确定的签名与该至少一个收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

164. 根据权利要求 123 所述的方法，其中利用处理器验证该对象，
该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及
签名单段，该签名是至少部分身份的数字签名；
该方法包括，在处理器内：
接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该
指示数据指示：
该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

165. 根据权利要求 123 所述的方法，其中该方法包括，在计算机系统中，通过至少如下之一，与感测装置通信：

通信网；

因特网；

移动电话网；以及

无线连接。

166. 一种用于验证对象的方法，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；以及

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

167. 根据权利要求 166 所述的方法，其中该方法包括产生表示该验证是否成功还是失败的表示。

168. 根据权利要求 166 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分至少表示如下之一：

至少部分身份；

至少一个签名部分；以及

编码数据在该表面上的位置，

其中该方法包括感测至少一个编码数据部分。

169. 根据权利要求 166 所述的方法，其中编码数据进一步指示签名部分的身份，而且其中该方法包括：

确定感测的签名部分的签名部分身份；

利用感测的身份，确定一被确定的签名；以及

利用感测的签名部分的签名部分身份且根据确定的签名来选择

确定的签名部分。

170. 根据权利要求 166 所述的方法，其中该方法包括利用感测的身份从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

- 与该签名相关的填充位；
- 专用密钥；
- 公用密钥；
- 一个或者多个数字签名部分；以及
- 数字签名。

171. 根据权利要求 170 所述的方法，其中至少利用如下之一索引该存储数据：

- 该身份；以及
- 一范围的身份。

172. 根据权利要求 170 所述的方法，其中该方法包括，利用该存储数据和感测的身份，确定该被确定的签名部分。

173. 根据权利要求 170 所述的方法，其中该方法包括从远程数据库检索存储数据。

174. 根据权利要求 166 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名部分的第二符号的位置。

175. 根据权利要求 166 所述的方法，其中整个签名由多个签名部分构成，而且其中以多个数据部分编码整个签名的方式，每个编码数据部分编码各签名部分。

176. 根据权利要求 166 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

177. 根据权利要求 166 所述的方法，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括：

利用身份，确定预定填充位；以及

利用该预定填充位和确定的签名，产生该被产生的身份。

178. 根据权利要求 166 所述的方法，其中在感测装置内执行该方法，该感测装置具有：

图像传感器，用于感测编码数据；以及

处理器，用于验证该对象。

179. 根据权利要求 166 所述的方法，其中指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名部分的大小；

签名部分的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

180. 根据权利要求 166 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及

利用 RSA 加密产生的密码文本。

181. 根据权利要求 166 所述的方法，其中该身份包括至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域。

182. 根据权利要求 166 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；

国家药品代码（NDC）号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；
发行日期；
到期日；以及
限额。

183. 根据权利要求 166 所述的方法，其中至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与另一个子布局互相区别开的旋转指示数据。

184. 根据权利要求 166 所述的方法，其中至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

185. 根据权利要求 168 所述的方法，其中每个编码数据部分对整个签名编码。

186. 根据权利要求 174 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

187. 根据权利要求 166 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少部分身份的数字签名。

188. 根据权利要求 166 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少如下的数字签名：
部分身份；以及
部分预定填充位。

189. 根据权利要求 166 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

190. 根据权利要求 166 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

191. 根据权利要求 166 所述的方法，该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

192. 根据权利要求 166 所述的方法，该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名片段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名片段；

利用多个签名单段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

193. 根据权利要求 166 所述的方法，其中该方法进一步包括，在计算机系统中：

感测设置在与该对象相关的表面之上或者之内的编码数据；
根据感测的编码数据，确定：
该对象的身份；以及
多个签名单段，该签名是至少部分身份的数字签名；
利用该多个签名单段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

194. 根据权利要求 166 所述的方法，其中处理器用于验证该对象的方法中，该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定一被确定的签名；
将确定的签名与该至少一个收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

195. 根据权利要求 166 所述的方法，其中利用处理器验证该对象，该对象与在其上或者其内布置了该编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；
该方法包括，在处理器内：
接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：
该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

196. 根据权利要求 166 所述的方法，其中由一装置利用该方法验证该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：

身份；以及
至少一部分签名，该签名是至少部分身份的数字签名；
处理器，用于：
利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；
利用感测的身份和至少一个感测的签名部分，验证该对象。

197. 一种用于验证对象的方法，该方法包括，在计算机系统中：
从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；
利用该指示数据，确定该身份和多个签名单段；
利用多个签名单段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

198. 根据权利要求 197 所述的方法，其中该方法包括，在计算机系
统中：

产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

199. 根据权利要求 198 所述的方法，其中该方法包括，在计算机系
统中，将该验证数据传送到感测装置。

200. 根据权利要求 197 所述的方法，其中该指示数据进一步表示多
个签名单段中每个签名单段的身份，而且其中该方法包括，在计算机系统
中：

利用该指示数据，确定多个签名单段中每个签名单段的签名单段身
份；以及

利用被确定的签名单段身份，确定该被确定的签名。

201. 根据权利要求 197 所述的方法，其中该方法包括，在计算机系
统中，利用收到的身份，从数据存储装置中检索存储数据，该存储数据包
括至少如下之一：

与该签名相关的填充位；
专用密钥；以及
公用密钥；以及

利用该存储数据和该被确定的签名，产生该被产生的身份。

202. 根据权利要求 201 所述的方法，其中至少利用如下之一索引该
存储数据：

该身份；以及
一范围的身份。

203. 根据权利要求 201 所述的方法，其中该方法包括，在计算机系
统中，从远程数据库中检索该存储数据。

204. 根据权利要求 197 所述的方法，其中该签名是至少部分身份和

至少部分预定填充位的数字签名，而且其中该方法包括，在计算机系统中：

利用收到的身份，确定预定填充位；以及

利用该预定填充位和该被确定的签名，产生该被产生的身份。

205. 根据权利要求 197 所述的方法，其中多个签名字段指示整个签名。

206. 根据权利要求 197 所述的方法，其中计算机系统构成该感测装置的部分。

207. 根据权利要求 197 所述的方法，其中该方法包括，在计算机系统中，通过至少如下之一，与该感测装置通信：

通信网；

因特网；

移动电话网；以及

无线连接。

208. 根据权利要求 197 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的大小；

签名单段的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

209. 根据权利要求 197 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

210. 根据权利要求 197 所述的方法，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

211. 根据权利要求 197 所述的方法，其中该身份包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：

货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

212. 根据权利要求 197 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与另一个子布局互相区别开的旋转指示数据。

213. 根据权利要求 197 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

214. 一种用于验证对象的方法，该方法包括，在感测装置内：

感测设置在与该对象相关的表面上的编码数据；

根据感测的编码数据，确定指示下述的指示数据：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

将该指示数据送到计算机系统，该计算机系统响应该指示数据，以：

利用该指示数据，确定该身份和多个签名单段；

利用多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

215. 根据权利要求 214 所述的方法，其中该方法包括，在该感测装置中：

接收表示该验证是成功还是失败的验证数据；以及
将该该验证是成功还是失败的表示送到用户。

216. 根据权利要求 214 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少签名单段；

其中该方法包括，在该感测装置内，感测多个编码数据部分，从而确定指示数据。

217. 根据权利要求 215 所述的方法，其中每个编码数据部分编码签名单段身份，而且其中该方法包括，在该感测装置内：

确定每个确定的签名单段的身份；以及
利用确定的签名单段身份、确定的签名，产生该指示数据。

218. 根据权利要求 214 所述的方法，其中多个签名单段指示整个签名。

219. 根据权利要求 214 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名单段的第二符号的位置。

220. 根据权利要求 217 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

221. 根据权利要求 214 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在该感测装置内，利用红外检测器感测该编码数据。

222. 根据权利要求 214 所述的方法，其中计算机系统构成该感测装

置的部分。

223. 根据权利要求 214 所述的方法，其中该方法包括，在该感测装置内，通过至少如下之一，与该计算机系统通信：

通信网；
因特网；
移动电话网；以及
无线连接。

224. 根据权利要求 214 所述的方法，其中该方法包括，在该感测装置内，产生至少指示如下之一的指示：

各数据部分的区位；
各数据部分在表面上的位置；
数据部分的大小；
签名的大小；
签名单段的大小；
签名单段的身份；
被指示区位的诸单元；
冗余数据；
允许纠错的数据；
里德-索罗门数据；以及
循环冗余校验（CRC）数据。

225. 根据权利要求 214 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

226. 根据权利要求 214 所述的方法，其中该身份包括至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域。

227. 根据权利要求 214 所述的方法，其中该身份包括至少如下之一：

电子产品代码 (EPC)；

国家药品代码 (NDC) 号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；
发行日期；
到期日；以及
限额。

228. 根据权利要求 214 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与另一个子布局互相区别开的旋转指示数据。

229. 根据权利要求 214 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

230. 根据权利要求 197 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少部分身份的数字签名。

231. 根据权利要求 197 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少如下的数字签名：
部分身份；以及
部分预定填充位。

232. 根据权利要求 197 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

233. 根据权利要求 197 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

234. 根据权利要求 197 所述的方法，其中该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

235. 根据权利要求 197 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

236. 根据权利要求 197 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；

根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

237. 根据权利要求 197 所述的方法，其中利用处理器验证该对象，该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用收到的身份和保密密钥，确定一被确定的签名；

将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

238. 根据权利要求 197 所述的方法，其中利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；

将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

239. 根据权利要求 197 所述的方法，其中由一装置利用该方法验证
该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数
据，该编码数据编码：

身份；以及

至少一部分签名，该签名是至少部分身份的数字签名；

处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部
分；

利用感测的身份和至少一个感测的签名部分，验证该对象。

240. 一种用于验证对象的方法，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；

利用感测的编码数据确定：

该对象的身份；

多个签名片段，该签名是至少部分身份的数字签名；

利用多个签名片段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

241. 根据权利要求 240 所述的方法，其中该方法包括，产生表示该
验证是成功还是失败的表示。

242. 根据权利要求 240 所述的方法，其中该编码数据包括多个编码
数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少签名片段；

其中该方法包括感测多个编码数据部分，从而确定多个签名片段。

243. 根据权利要求 242 所述的方法，其中每个编码数据部分编码签名片段身份，而且其中该方法包括：

确定每个确定的签名片段的签名片段身份；以及
利用确定的签名片段身份，确定该被确定的签名。

244. 根据权利要求 240 所述的方法，其中该编码数据包括多个布局，
每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一
部分签名片段的第二符号的位置。

245. 根据权利要求 244 所述的方法，其中该编码数据包括多个标签，
每个编码数据部分至少由一个标签构成。

246. 根据权利要求 240 所述的方法，其中利用不可见油墨和红外吸
收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括利
用红外检测器感测该编码数据。

247. 根据权利要求 240 所述的方法，其中多个签名片段指示整个签
名。

248. 根据权利要求 240 所述的方法，其中该方法包括：

利用该身份，从数据存储装置中检索存储数据，该存储数据包括至少
如下之一：

与该签名相关的填充位；

专用密钥；以及

公用密钥；以及

利用该存储数据和确定的签名，产生该被产生的身份。

249. 根据权利要求 248 所述的方法，其中至少利用如下之一索引该
存储数据：

该身份；以及

一范围的身份。

250. 根据权利要求 248 所述的方法，其中该方法包括，从远程数据
库中检索该存储数据。

251. 根据权利要求 240 所述的方法，其中该签名是至少部分身份和

至少部分预定填充位的数字签名，而且其中该方法包括：

利用该身份确定该预定填充位；以及

利用该预定填充位和确定的签名，产生该被产生的身份。

252. 根据权利要求 197 所述的方法，其中该方法包括，在感测装置中：

利用传感器感测该编码数据；

利用处理器：

根据感测的编码数据，确定：

该对象的身份；

多个签名单段，该签名是至少部分身份的数字签名；

利用多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生该被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

253. 根据权利要求 240 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的大小；

签名单段的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

254. 根据权利要求 240 所述的方法，其中该数字签名包括至少如下

之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；以及

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

255. 根据权利要求 240 所述的方法，其中该身份包括至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域。

256. 根据权利要求 240 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；

国家药品代码（NDC）号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；
到期日；
支票值；以及
限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

257. 根据权利要求 240 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与另一个子布局互相区别开的旋转指示数据。

258. 根据权利要求 240 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

259. 根据权利要求 240 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少部分身份的数字签名。

260. 根据权利要求 240 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少如下的数字签名：

部分身份；以及

部分预定填充位。

261. 根据权利要求 240 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

262. 根据权利要求 240 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

263. 根据权利要求 240 所述的方法，其中该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

264. 根据权利要求 240 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；
利用感测的编码数据，确定感测的身份和感测的签名部分；
利用感测的身份，确定至少一被确定的签名部分；
将被确定的签名部分与感测的签名部分进行比较；以及
利用该比较结果，验证该对象。

265. 根据权利要求 240 所述的方法，该方法包括，在计算机系统中：
从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；
利用该指示数据，确定该身份和多个签名单段；
利用该多个签名单段，确定一被确定的签名部分；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

266. 根据权利要求 240 所述的方法，其中利用处理器验证该对象，该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定一被确定的签名；
将确定的签名与该至少一个收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

267. 根据权利要求 240 所述的方法，其中利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：
该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；
该方法包括，在处理器内：
接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：
该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

268. 根据权利要求 240 所述的方法，其中由一装置利用该方法验证该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：
身份；以及
至少一部分签名，该签名是至少部分身份的数字签名；
处理器，用于：
利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；
利用感测的身份和至少一个感测的签名部分，验证该对象。

269. 一种利用处理器验证对象的方法，该方法包括，在处理器中：
接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和至少一个收到的签名部分；
利用收到的身份和保密密钥，确定一被确定的签名；
将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

270. 根据权利要求 269 所述的方法，其中该方法包括，在处理器中：
产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

271. 根据权利要求 270 所述的方法，其中该方法包括，在处理器中，
将该验证数据传送到感测装置。

272. 根据权利要求 269 所述的方法，其中该指示数据进一步表示签名部分的身份，而且其中该方法包括，在处理器中：
利用该指示数据，确定收到的的签名部分身份；
利用收到的身份，选择确定的签名的部分；以及
通过将被确定的签名部分与至少一个收到的签名部分进行比较，验证该对象。

273. 根据权利要求 269 所述的方法，其中该方法包括，在处理器中，
利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；
专用密钥；
公用密钥；
一个或者多个数字签名部分；以及
数字签名。

274. 根据权利要求 273 所述的方法，其中该方法包括，在处理器中，
利用该存储数据和收到的身份，产生确定的签名部分。

275. 根据权利要求 269 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

276. 根据权利要求 269 所述的方法，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在处理器中：
利用收到的身份，确定预定填充位；以及

利用该预定填充位和收到的身份，确定该被确定的签名部分。

277. 根据权利要求 269 所述的方法，其中该处理器构成感测装置的一部分，而且其中该方法包括从该感测装置内的传感器接收该指示数据。

278. 根据权利要求 269 所述的方法，其中该处理器与产生该指示数据的感测装置通信，而且其中该方法包括，从该感测装置接收该指示数据。

279. 根据权利要求 278 所述的方法，其中该方法包括，在处理器中，通过至少如下之一，与该感测装置通信：

通信网；

因特网；

移动电话网；以及

无线连接。

280. 根据权利要求 269 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名部分的大小；

签名部分的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

281. 根据权利要求 269 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；以及

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

282. 根据权利要求 269 所述的方法，其中该身份包括至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域。

283. 根据权利要求 269 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；

国家药品代码（NDC）号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

284. 根据权利要求 269 所述的方法，其中通过与第二处理器通信，该处理器确定该被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

285. 根据权利要求 269 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

286. 根据权利要求 269 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

287. 一种利用处理器验证对象的方法，该方法包括，在感测装置内：

感测设置在与该对象相关的表面之上或者之内的编码数据；

根据感测的编码数据，确定指示如下所述的指示数据：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

将该指示数据送到处理器，该处理器响应该指示数据，以：

利用该身份和保密密钥，产生签名；

将确定的签名与该至少部分签名进行比较；以及
利用该比较结果，验证该对象。

288. 一种用于验证对象的处理器，该对象与其上或者其内设置了编
码数据的表面相关，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名，

其中该处理器

接收指示数据，响应感测到该编码数据，产生该指示数据，

该指示数据指示该身份和至少部分签名；

利用该指示数据，确定该身份和至少部分签名；

利用确定的身份和保密密钥，产生确定的签名；

将确定的签名与该至少部分签名进行比较；

利用该比较结果，验证对象。

289. 根据权利要求 269 所述的方法，其中该编码数据包括多个布局，
每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一
个签名部分的第二符号的位置。

290. 根据权利要求 289 所述的方法，其中该编码数据包括多个标签，
每个编码数据部分至少由一个标签构成。

291. 根据权利要求 273 所述的方法，其中至少利用如下之一索引该
存储数据：

该身份；以及

一范围的身份。

292. 根据权利要求 273 所述的方法，其中该方法包括，在处理器中，
从远程数据库中检索该存储数据。

293. 根据权利要求 291 所述的方法，其中该编码数据包括许多编码
数据部分，每个编码数据部分编码该身份以及至少部分签名，该方法包括
至少感测一个数据部分。

294. 根据权利要求 287 所述的方法，其中该方法包括，在感测装置

内：

接收表示该验证是成功还是失败的验证数据；以及
将该验证是成功还是失败的指示提供给用户。

295. 根据权利要求 287 所述的方法，其中在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：

感测许多编码部分；以及
产生指示整个签名的指示数据。

296. 根据权利要求 287 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

297. 根据权利要求 287 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

298. 根据权利要求 287 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

299. 根据权利要求 287 所述的方法，其中该处理器构成该感测装置的部分。

300. 根据权利要求 287 所述的方法，其中该方法包括，在该感测装置内，通过至少如下之一，与该处理器通信：

通信网；
因特网；
移动电话网；以及
无线连接。

301. 根据权利要求 287 所述的方法，其中该方法包括，在该感测装置内，产生至少指示如下之一的指示：

各数据部分的区位；
各数据部分在表面上的位置；
数据部分的大小；

签名的大小；
签名单段的身份；
被指示区位的诸单元；
冗余数据；
允许纠错的数据；
里德-索罗门数据；以及
循环冗余校验（CRC）数据。

302. 根据权利要求 287 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

303. 根据权利要求 287 所述的方法，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

304. 根据权利要求 287 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：
货币；
发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

305. 根据权利要求 287 所述的方法，其中通过与第二处理器通信，该处理器确定该被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

306. 根据权利要求 287 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局区别的旋转指示数据。

307. 根据权利要求 287 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个

符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

308. 根据权利要求 288 所述的处理器，其中该处理器：

产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

309. 根据权利要求 288 所述的处理器，其中该处理器将该验证数据传送到感测装置。

310. 根据权利要求 288 所述的处理器，其中该指示数据进一步表示签名部分的身份，而且其中该处理器：

利用该指示数据，确定收到的签名部分身份；
利用收到的身份，选择确定的签名的部分；以及
通过将被确定的签名部分与该至少一个收到的签名部分进行比较，验证该对象。

311. 根据权利要求 288 所述的处理器，其中利用收到的身份，该处理器从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；
专用密钥；
公用密钥；
一个或者多个数字签名部分；以及
数字签名。

312. 根据权利要求 288 所述的处理器，其中至少利用如下之一索引该存储数据：

该身份；以及
一范围的身份。

313. 根据权利要求 288 所述的处理器，其中利用该存储数据和收到

的身份，该处理器产生确定的签名部分。

314. 根据权利要求 288 所述的处理器，其中该处理器从远程数据库中检索该存储数据。

315. 根据权利要求 288 所述的处理器，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该处理器：

利用收到的身份，确定预定填充位；以及

利用该预定填充位和收到的身份，确定该被确定的签名部分。

316. 根据权利要求 288 所述的处理器，其中该处理器构成该感测装置的部分。

317. 根据权利要求 288 所述的处理器，其中该处理器与产生指示数据的感测装置通信，而且其中该处理器从该感测装置接收该指示数据。

318. 根据权利要求 288 所述的处理器，其中通过至少如下之一，该处理器与该感测装置通信：

通信网；

因特网；

移动电话网；以及

无线连接。

319. 根据权利要求 288 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名部分的大小；

签名部分的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及
循环冗余校验（CRC）数据。

320. 根据权利要求 288 所述的处理器，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

321. 根据权利要求 288 所述的处理器，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

322. 根据权利要求 288 所述的处理器，其中该身份包括至少如下之一：

电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：
货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；
到期日；
支票值；以及
限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

323. 根据权利要求 288 所述的处理器，其中通过与第二处理器通信，该处理器确定该被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

324. 根据权利要求 288 所述的处理器，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

325. 根据权利要求 288 所述的处理器，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

326. 根据权利要求 269 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

327. 根据权利要求 269 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少如下的数字签名：

部分身份；以及

部分预定填充位。

328. 根据权利要求 269 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

329. 根据权利要求 269 所述的方法，其中该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

330. 根据权利要求 269 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用感测的编码数据，确定感测的身份和感测的签名部分；

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

331. 根据权利要求 269 所述的方法，该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名单段；

利用多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

332. 根据权利要求 269 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；

根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

333. 根据权利要求 269 所述的方法，其中利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；

将被确定的身份与收到的身份进行比较；以及

利用该比较结果，验证该对象。

334. 根据权利要求 269 所述的方法，其中由一装置利用该方法验证该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：

身份；以及

至少一部分签名，该签名是至少部分身份的数字签名；

处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用感测的身份和至少一个感测的签名部分，验证该对象。

335. 一种利用处理器验证对象的方法，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名，

该方法包括，在该处理器内：

从感测装置接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定身份；

将被确定的身份与收到的身份进行比较；以及

利用该比较结果，验证该对象。

336. 根据权利要求 335 所述的方法，其中该方法包括，在处理器中：

产生表示该验证是成功还是失败的验证数据；以及

将该验证数据传送到用户。

337. 根据权利要求 336 所述的方法，其中该方法包括，在处理器中，将该验证数据传送到感测装置。

338. 根据权利要求 335 所述的方法，其中该指示数据进一步表示每个签名单段的身份，而且其中该方法包括，在处理器中：

利用该指示数据，对每个收到的签名单段确定收到的签名单段身份；

利用每个收到的签名单段的收到的签名单段身份，确定一被确定的签名；以及

利用确定的签名和保密密钥，确定一被确定的身份。

339. 根据权利要求 335 所述的方法，其中该方法包括，在处理器中，利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；

专用密钥；

公用密钥；

一个或者多个数字签名部分；以及

数字签名。

340. 根据权利要求 339 所述的方法，其中该方法包括，在处理器中，利用该存储数据和收到的签名单段，确定一被确定的身份。

341. 根据权利要求 335 所述的方法，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

342. 根据权利要求 335 所述的方法，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在处理器中：

利用收到的身份，确定预定填充位；以及

利用该预定填充位和收到的签名单段，确定该被确定的身份。

343. 根据权利要求 335 所述的方法，其中该处理器构成感测装置的一部分，而且其中该方法包括从该感测装置内的传感器接收该指示数据。

344. 根据权利要求 335 所述的方法，其中该处理器与产生该指示数据的感测装置通信，而且其中该方法包括，从该感测装置接收该指示数据。

345. 根据权利要求 345 所述的方法，其中该指示数据进一步指示至少如下之一：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的大小；

签名单段的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

346. 根据权利要求 335 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

347. 根据权利要求 335 所述的方法，其中该身份包括至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域。

348. 根据权利要求 335 所述的方法，其中该身份包括至少如下之一：电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：

货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

349. 根据权利要求 335 所述的方法，其中该指示数据指示整个签名。

350. 根据权利要求 335 所述的方法，其中通过与第二处理器通信，该处理器确定该被确定的身份，该第二处理器利用收到的签名单段和保密密钥产生确定的身份。

351. 根据权利要求 335 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

352. 根据权利要求 335 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

353. 一种利用处理器验证对象的方法，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名，
该方法包括，在感测装置中：
感测多个编码数据部分；
利用感测的编码数据部分，确定指示数据，该指示数据指示：
该对象的身份；以及
多个签名单段；
将该指示数据送到该处理器，响应该指示数据，该处理器：
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；以及
利用该比较结果，验证该对象。

354. 一种用于验证对象的处理器，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：
该对象的身份；以及
签名单段，该签名表示至少部分身份的数字签名，
其中该处理器：
从感测装置接收指示数据，响应于感测多个编码数据部分，该感测装置产生该指示数据，该指示数据指示：
该对象的身份；以及
多个签名单段；
利用该指示数据，确定收到的身份和多个收到的签名单段；
利用该多个签名单段和保密密钥，确定一被确定的身份；
将被确定的身份与收到的身份进行比较；
利用该比较结果，验证对象。

355. 根据权利要求 339 所述的方法，其中至少利用如下之一索引该存储数据：
该身份；以及

一范围的身份。

356. 根据权利要求 335 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名单段的第二符号的位置。

357. 根据权利要求 339 所述的方法，其中该方法包括在该处理器中从远程数据库中检索该存储数据。

358. 根据权利要求 341 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

359. 根据权利要求 345 所述的方法，其中该方法包括，在该处理器内，通过至少如下之一，与感测装置通信：

通信网；

因特网；

移动电话网；以及

无线连接。

360. 根据权利要求 353 所述的方法，其中该方法包括，在感测装置内：

接收表示该验证是成功还是失败的验证数据；以及

将该验证是成功还是失败的指示提供给用户。

361. 根据权利要求 353 所述的方法，其中在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：

感测许多编码部分；以及

产生指示整个签名的指示数据。

362. 根据权利要求 358 所述的方法，其中该编码数据包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名单段的第二符号的位置。

363. 根据权利要求 358 所述的方法，其中该编码数据包括多个标签，每个编码数据部分至少由一个标签构成。

364. 根据权利要求 358 所述的方法，其中利用不可见油墨和红外吸

收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

365. 根据权利要求 358 所述的方法，其中该处理器构成该感测装置的部分。

366. 根据权利要求 358 所述的方法，其中该方法包括，在该感测装置内，通过至少如下之一，与该处理器通信：

通信网；

因特网；

移动电话网；以及

无线连接。

367. 根据权利要求 358 所述的方法，其中该方法包括，在该感测装置内，产生至少指示如下之一的指示：

各数据部分的区位；

各数据部分在表面上的位置；

数据部分的大小；

签名的大小；

签名单段的身份；

被指示区位的诸单元；

冗余数据；

允许纠错的数据；

里德-索罗门数据；以及

循环冗余校验（CRC）数据。

368. 根据权利要求 358 所述的方法，其中该数字签名包括至少如下之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；以及

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

369. 根据权利要求 358 所述的方法，其中该身份包括至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域。

370. 根据权利要求 358 所述的方法，其中该身份包括至少如下之一：

电子产品代码（EPC）；

国家药品代码（NDC）号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

371. 根据权利要求 358 所述的方法，其中通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

372. 根据权利要求 358 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

373. 根据权利要求 358 所述的方法，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

374. 根据权利要求 373 所述的处理器，其中该处理器：
产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

375. 根据权利要求 373 所述的处理器，其中该处理器将该验证数据传送到感测装置。

376. 根据权利要求 373 所述的处理器，其中该指示数据进一步表示每个签名单段的身份，而且其中该处理器：

利用该指示数据，确定用于每个收到的签名单段的收到签名单段身份；

利用该用于每个收到的签名单段的收到签名单段身份，确定一被确定的签名；以及

利用确定的签名和保密密钥，确定该被确定的身份。

377. 根据权利要求 373 所述的处理器，其中利用收到的身份，该处理器从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；

专用密钥；

公用密钥；

一个或者多个数字签名部分；以及

数字签名。

378. 根据权利要求 377 所述的处理器，其中至少利用如下之一索引该存储数据：

该身份；以及

一范围的身份。

379. 根据权利要求 377 所述的处理器，其中利用该存储数据和收到的签名单段，该处理器确定一被确定的身份。

380. 根据权利要求 3377 所述的处理器，其中该处理器从远程数据库中检索该存储数据。

381. 根据权利要求 373 所述的处理器，其中该签名是至少部分身份和至少部分预定填充位的数字签名，而且其中该处理器：

利用收到的身份，确定预定填充位；以及

利用该预定填充位和收到的签名单段，确定该被确定的身份。

382. 根据权利要求 373 所述的处理器，其中该处理器构成该感测装置的部分。

383. 根据权利要求 373 所述的处理器，其中该处理器与产生指示数据的感测装置通信，而且其中该处理器从该感测装置接收该指示数据。

384. 根据权利要求 383 所述的处理器，其中通过至少如下之一，该

处理器与该感测装置通信：

 通信网；
 因特网；
 移动电话网；以及
 无线连接。

385. 根据权利要求 373 所述的方法，其中该指示数据进一步指示至少如下之一：

 各数据部分的区位；
 各数据部分在表面上的位置；
 数据部分的大小；
 签名的大小；
 签名单段的大小；
 签名单段的身份；
 被指示区位的诸单元；
 冗余数据；
 允许纠错的数据；
 里德-索罗门数据；以及
 循环冗余校验（CRC）数据。

386. 根据权利要求 373 所述的处理器，其中该数字签名包括至少如下之一：

 与身份有关的随机数；
 至少该身份的键控散列；
 利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
 通过对至少该身份进行加密产生的密码文本；
 通过对至少该身份和随机数进行加密产生的密码文本；以及
 利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

387. 根据权利要求 373 所述的处理器，其中该身份包括至少如下之

一的身份：

该对象；

该表面；以及

该表面上的区域。

388. 根据权利要求 373 所述的处理器，其中该身份包括至少如下之一：

电子产品代码 (EPC)；

国家药品代码 (NDC) 号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；

发行国家；

面额；

券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；
到期日；以及
限额。

389. 根据权利要求 373 所述的处理器，其中通过与第二处理器通信，该处理器确定一被确定的身份，该第二处理器利用收到的签名单段和保密密钥产生确定的身份。

390. 根据权利要求 373 所述的处理器，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

391. 根据权利要求 373 所述的处理器，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

392. 根据权利要求 335 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少部分身份的数字签名。

393. 根据权利要求 335 所述的方法，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少部分签名，该签名是至少如下的数字签名：
部分身份；以及
部分预定填充位。

394. 根据权利要求 335 所述的方法，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及
至少数据对象片段；
以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

395. 根据权利要求 335 所述的方法，其中该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；
利用该指示数据，确定收到的身份和收到的签名部分；
利用收到的身份，确定至少一被确定的签名部分；
将被确定的签名部分与收到的签名部分进行比较；以及
利用该比较结果，验证该对象。

396. 根据权利要求 335 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；

该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用感测的编码数据，确定感测的身份和感测的签名部分；
利用感测的身份，确定至少一被确定的签名部分；
将被确定的签名部分与感测的签名部分进行比较；以及
利用该比较结果，验证该对象。

397. 根据权利要求 335 所述的方法，该方法进一步包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该指示数据，确定该身份和多个签名单段；

利用多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

398. 根据权利要求 335 所述的方法，该方法进一步包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；

根据感测的编码数据，确定：

该对象的身份；以及

多个签名单段，该签名是至少部分身份的数字签名；

利用该多个签名单段，确定一被确定的签名；

利用被确定的签名和密钥，产生一被产生的身份；

将该身份与被产生的身份进行比较；以及

利用该比较结果，验证该对象。

399. 根据权利要求 335 所述的方法，其中利用处理器验证该对象，

该方法包括，在处理器内：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用该收到的身份和保密密钥，确定一被确定的签名；

将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

400. 根据权利要求 335 所述的方法，其中由一装置利用该方法验证该对象，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：

身份；以及

至少一部分签名，该签名是至少部分身份的数字签名；
处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用感测的身份和至少一个感测的签名部分，验证该对象。

401. 一种用于验证对象的装置，该装置包括：

传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：

身份；以及

至少一部分签名，该签名是至少部分身份的数字签名；以及
处理器，用于：

利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；

利用确定的身份和至少一个感测的签名部分，验证该对象。

402. 根据权利要求 401 所述的装置，其中该装置包括指示器，用于指示该验证是成功还是失败。

403. 根据权利要求 401 所述的装置，其中该处理器用于：

利用感测的身份，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

404. 根据权利要求 401 所述的装置，其中该处理器用于：

利用感测的身份和密钥，确定至少一被确定的签名部分；

将被确定的签名部分与感测的签名部分进行比较；以及

利用该比较结果，验证该对象。

405. 根据权利要求 401 所述的装置，其中该处理器用于：

利用感测的编码数据，确定多个感测的签名部分；

利用感测的签名部分，确定一被确定的签名；

利用确定的签名部分和密钥，确定一被确定的身份；

将感测的身份与确定的身份进行比较；以及

利用该比较结果，验证该对象。

406. 根据权利要求 401 所述的装置，其中该装置包括数据存储装置，而且其中该处理器：

利用感测的身份，检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；

专用密钥；

公用密钥；

一个或者多个数字签名部分；以及

数字签名；

利用该存储数据，验证该对象。

407. 根据权利要求 406 所述的装置，其中该数据存储装置是远程数据库。

408. 根据权利要求 401 所述的装置，其中该处理器利用感测的编码数据确定多个用于表示整个签名的签名部分。

409. 根据权利要求 401 所述的装置，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该传感器是至少如下之一：

红外检测器；以及

激光扫描仪。

410. 根据权利要求 401 所述的装置，其中该装置是至少如下之一：

文件扫描仪；

现金出纳机；

Netpage 笔；

钞票扫描仪；
手持扫描仪；
具有内置扫描仪的移动电话；
自动柜员机；以及
自动售货机。

411. 根据权利要求 401 所述的装置，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及
利用 RSA 加密产生的密码文本。

412. 根据权利要求 401 所述的装置，其中该身份包括至少如下之一：

至少如下之一的身份：

该对象；
该表面；以及
该表面上的区域；以及
电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：

货币；
发行国家；
面额；
券面；

印刷工厂；以及

序列号；

支票属性，包括至少如下之一：

货币；

发行机构；

账号；

序列号；

到期日；

支票值；以及

限额；

卡属性，包括至少如下之一：

卡类型；

发行机构；

账号；

发行日期；

到期日；以及

限额。

413. 根据权利要求 401 所述的装置，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

414. 根据权利要求 401 所述的装置，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

415. 根据权利要求 401 所述的装置，其中该处理器：

产生表示感测的身份和至少一个感测的签名部分的指示数据；以及将该指示数据传送到计算机系统，响应该指示数据，该计算机系统：利用该指示数据，确定一被确定的身份和确定的签名部分；以及利用确定的身份和确定的签名部分，验证该对象。

416. 根据权利要求 401 所述的装置，其中该编码数据包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：
至少部分身份；
至少部分签名；以及
编码数据部分在该表面上的位置。

417. 根据权利要求 416 所述的装置，其中每个编码数据部分编码整个签名。

418. 根据权利要求 416 所述的装置，其中整个签名由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

419. 一种用于验证对象的装置，该装置包括：
传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：
身份；以及
至少部分签名，该签名是至少部分身份的数字签名；以及
处理器，用于利用感测的编码数据，确定指示数据，该指示数据指示：
该身份；
至少一个签名部分；
通信系统，用于将该指示数据传送到计算机系统，该计算机系统响应该指示数据验证该对象。

420. 一种用于验证对象的计算机系统，该计算机系统用于：
从装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：
该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用收到的身份和至少一个收到的签名部分，验证该对象。

421. 根据权利要求 415 所述的装置，其中该装置通过至少如下之一与该计算机系统通信：

通信网；

因特网；

移动电话网；以及

无线连接。

422. 根据权利要求 416 所述的计算机系统，其中该计算机系统用于：

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

423. 根据权利要求 418 所述的计算机系统，其中该计算机系统用于：

利用收到的身份和密钥，确定至少一被确定的签名部分；

将确定的签名与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

424. 根据权利要求 418 所述的计算机系统，该计算机系统用于：

利用该指示数据，确定多个收到的签名部分；

利用收到的签名部分，确定一被确定的签名；

利用被确定的签名和密钥，确定一被确定的身份；

将收到的身份与确定的身份进行比较；以及

利用该比较结果，验证该对象。

425. 根据权利要求 415 所述的装置，其中该装置包括指示器，用于指示该验证是成功还是失败。

426. 根据权利要求 415 所述的装置，其中利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该传感器是至少如下之一：

红外检测器；以及

激光扫描仪。

427. 根据权利要求 415 所述的装置，其中该装置是至少如下之一：

文件扫描仪；

现金出纳机；

Netpage 笔；

钞票扫描仪；

手持扫描仪；

具有内置扫描仪的移动电话；

自动柜员机；以及

自动售货机。

428. 根据权利要求 415 所述的装置，其中该数字签名包括至少如下之一：

与身份有关的随机数；

至少该身份的键控散列；

利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；

通过对至少该身份进行加密产生的密码文本；

通过对至少该身份和随机数进行加密产生的密码文本；以及

利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

429. 根据权利要求 415 所述的装置，其中该身份包括至少如下之一：至少如下之一的身份：

该对象；

该表面；以及

该表面上的区域；以及

电子产品代码（EPC）；

国家药品代码（NDC）号；

药品项目序列号；

钞票属性，包括至少如下之一：

货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；
到期日；
支票值；以及
限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

430. 根据权利要求 415 所述的装置，其中该处理器利用感测的编码数据确定指示数据，该指示数据指示多个签名部分，该签名部分代表整个签名。

431. 根据权利要求 415 所述的装置，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

432. 根据权利要求 415 所述的装置，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

433. 根据权利要求 417 所述的计算机系统，其中该计算机系统：
产生表示该验证是成功还是失败的验证数据；以及
将该验证数据传送到用户。

434. 根据权利要求 418 所述的计算机系统，其中该计算机系统包括数据存储装置，而且其中该计算机系统：

利用感测的身份，检索指示该数字签名的存储数据，该存储数据包括至少如下之一：

与该签名相关的填充位；
专用密钥；
公用密钥；
一个或者多个数字签名部分；以及
数字签名；
利用该存储数据，验证该对象。

435. 根据权利要求 428 所述的计算机系统，其中该数据存储装置是远程数据库。

436. 根据权利要求 418 所述的计算机，其中该计算机系统利用感测的编码数据确定多个用于代表整个签名的签名部分。

437. 根据权利要求 418 所述的计算机系统，其中该计算机系统将验证数据传送到该装置。

438. 根据权利要求 418 所述的方法，其中该计算机系统通过至少如下之一与该装置通信：

通信网；

因特网；
移动电话网；以及
无线连接。

439. 根据权利要求 418 所述的计算机系统，其中该数字签名包括至少如下之一：

与身份有关的随机数；
至少该身份的键控散列；
利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；
通过对至少该身份进行加密产生的密码文本；
通过对至少该身份和随机数进行加密产生的密码文本；以及
利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

440. 根据权利要求 418 所述的计算机系统，其中该身份包括至少如下之一：

至少如下之一的身份：
该对象；
该表面；以及
该表面上的区域；以及
电子产品代码（EPC）；
国家药品代码（NDC）号；
药品项目序列号；
钞票属性，包括至少如下之一：
货币；
发行国家；
面额；
券面；
印刷工厂；以及
序列号；

支票属性，包括至少如下之一：

货币；
发行机构；
账号；
序列号；
到期日；
支票值；以及
限额；

卡属性，包括至少如下之一：

卡类型；
发行机构；
账号；
发行日期；
到期日；以及
限额。

441. 根据权利要求 418 所述的计算机系统，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

442. 根据权利要求 418 所述的计算机系统，其中根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

443. 根据权利要求 401 所述的装置，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少部分身份的数字签名。

444. 根据权利要求 401 所述的装置，其中该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少部分签名，该签名是至少如下的数字签名：

部分身份；以及

部分预定填充位。

445. 根据权利要求 401 所述的装置，其中该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：

身份；以及

至少数据对象片段；

以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

446. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方法，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分片段，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和收到的签名部分；

利用收到的身份，确定至少一被确定的签名部分；

将被确定的签名部分与收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

447. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方法，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：

该对象的身份；以及
至少部分签名，该签名是至少部分身份的数字签名；
利用感测的编码数据，确定感测的身份和感测的签名部分；
利用感测的身份，确定至少一被确定的签名部分；
将被确定的签名部分与感测的签名部分进行比较；以及
利用该比较结果，验证该对象。

448. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方法，该方法包括，在计算机系统中：

从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及
多个签名片段，该签名是至少部分身份的数字签名；
利用该指示数据，确定该身份和多个签名片段；
利用多个签名片段，确定一被确定的签名；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与该被产生的身份进行比较；以及
利用该比较结果，验证该对象。

449. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方法，该方法包括：

感测设置在与该对象相关的表面之上或者之内的编码数据；
利用感测的编码数据，确定：
该对象的身份；以及
多个签名片段，该签名是至少部分身份的数字签名；
利用该多个签名片段，确定一被确定的身份；
利用被确定的签名和密钥，产生一被产生的身份；
将该身份与被产生的身份进行比较；以及
利用该比较结果，验证该对象。

450. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方

法，该方法包括，在处理器中：

接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：

该对象的身份；以及

至少部分签名，该签名是至少部分身份的数字签名；

利用该指示数据，确定收到的身份和至少一个收到的签名部分；

利用收到的身份和保密密钥，确定一被确定的签名；

将确定的签名与该至少一个收到的签名部分进行比较；以及

利用该比较结果，验证该对象。

451. 根据权利要求 401 所述的装置，其中该装置用于验证对象的方法，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：

该对象的身份；以及

签名单段，该签名是至少部分身份的数字签名；

该方法包括，在处理器内：

接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：

该对象的身份；以及

多个签名单段；

利用该指示数据，确定收到的身份和多个收到的签名单段；

利用该多个签名单段和保密密钥，确定一被确定的身份；

将被确定的身份与收到的身份进行比较；以及

利用该比较结果，验证该对象。

452. 一种用于核实对象的方法，其中该方法包括，在计算机系统中：

接收核实请求，该请求的至少部分地指示：

该对象的身份；

至少一个签名单段，该签名是至少部分身份的数字签名；

利用该核实请求，确定一被确定的身份；

利用确定的身份，从数据库中，确定至少一个与该核实有关的判据；将收到的核实请求与该至少一个判据进行比较；以及如果满足该至少一个判据，则该对象将被核实。

453. 根据权利要求 452 所述的方法，其中该至少一个判据与至少如下之一的限制有关：

收到的核实请求的数目；
收到核实请求的速率；以及
收到核实请求的时间。

454. 根据权利要求 453 所述的方法，其中根据至少如下之一确定该限制：

该对象的身份；
该签名；
该签名单段；
核实请求信源；以及
该对象。

455. 根据权利要求 453 所述的方法，其中该限制与签名单段的大小成比例。

456. 根据权利要求 453 所述的方法，其中该方法包括，在计算机系统中：

利用该核实请求，确定：
请求历史，表示先前收到的核实请求的数目；以及
对应的限制；

利用该核实请求和该请求历史，确定请求数量；以及
如果该请求数量不超过相应限制，则该对象将被核实。

457. 根据权利要求 456 所述的方法，其中该方法包括，在计算机系统中，响应核实请求，更新该请求历史。

458. 根据权利要求 456 所述的方法，其中该请求历史指示收到核实请求的时间。

459. 根据权利要求 456 所述的方法，其中该请求历史与如下相关：
该对象的身份；
该签名；
该签名单段；
核实请求信源；以及
该对象。

460. 根据权利要求 452 所述的方法，其中该方法包括，在计算机系统中，通过利用该对象的身份和至少一个签名单段对该对象进行验证来核实该对象。

461. 根据权利要求 452 所述的方法，其中该核实请求至少部分地指示该签名单段的身份。

462. 根据权利要求 452 所述的方法，其中该对象与其上或者其内设置了编码数据的表面相关，该编码数据包括许多编码数据部分，每个编码数据部分指示至少该身份和签名单段，而且其中响应于感测至少一个编码数据部分，感测装置产生该核实请求。

463. 根据权利要求 462 所述的方法，其中该核实请求至少部分地指示签名单段的身份，该片段身份基于至少如下之一：

在至少一个感测的编码数据部分内编码的数；以及
该至少一个感测的编码数据部分在该表面上的位置。

464. 根据权利要求 452 所述的方法，其中该方法包括，在计算机系统中，在核实失败后，仅将收到的核实请求与该至少一个判据进行比较。

465. 一种用于核实对象的方法，其中该方法包括，在计算机系统中，接收核实请求，该核实请求至少部分地指示：
该对象的身份；
并置的：

签名单段，该签名是至少部分身份的数字签名；以及
随机签名；
利用该核实请求，确定一被确定的身份；

利用该并置，确定签名单段；以及
利用确定的身份和签名单段，核实该对象。

466. 根据权利要求 465 所述的方法，其中该方法包括，在计算机系统中，利用确定的身份，确定密钥；

利用确定的身份和该密钥，产生一被产生的签名；

将产生的签名与该并置进行比较，从而识别和验证该签名单段。

467. 一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：

身份；

签名单段，该签名是至少部分身份的数字签名；以及

随机签名；

468. 一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分至少部分地指示：

身份；

至少部分签名，该签名是至少部分身份的数字签名；以及
该编码数据在该表面上的位置。

469. 根据权利要求 468 所述的编码数据，其中每个编码数据部分至少部分地指示数据部分身份，对于每个编码数据部分，该数据部分身份是唯一的，该数据部分身份指示该位置。

470. 根据权利要求 469 所述的编码数据，其中利用某种布局将该编码数据布置在该表面之上或者之内，对于每个数据部分身份，该布局指示对应编码数据部分的位置。

471. 根据权利要求 470 所述的编码数据，其中利用 RSA 加密，产生该签名。

利用以许多数据部分编码的签名验证对象

技术领域

本发明宽泛地涉及用于利用设置在产品或安全文档表面上或表面内的机器可读标签来保护该产品和安全文档的方法和装置。

共同未决申请

下面的申请已由本申请人与本申请同时提交：

HYN HYP

这些共同未决申请的公开内容通过引用结合于此。上述申请通过其提交案卷号标识，一旦分配了对应的申请号，该提交案卷号将被该申请号所取代。

交叉引用

涉及本发明的各种方法、系统和装置都公开在下列由本申请人或本发明的受让人提交的美国未决申请和已授权专利中。将所有这些美国共同未决申请和已授权专利的公开内容通过引用结合于此。

6,795,215	10/884,881	PEC01NP	09/575,109	10/296,535	09/575,110	6,805,419
09/607,985	6,398,332	6,394,573	6,622,923	6,747,760	10/189,459	10/943,941
10/949,294	10/727,181	10/727,162	10/727,163	10/727,245	10/727,204	10/727,233
10/727,280	10/727,157	10/727,178	10/727,210	10/727,257	10/727,238	10/727,251
10/727,159	10/727,180	10/727,179	10/727,192	10/727,274	10/727,164	10/727,161
10/727,198	10/727,158	10/754,536	10/754,938	10/727,227	10/727,160	10/934,720
10/854,521	10/854,522	10/854,488	10/854,487	10/854,503	10/854,504	10/854,509
10/854,510	10/854,496	10/854,497	10/854,495	10/854,498	10/854,511	10/854,512
10/854,525	10/854,526	10/854,516	10/854,508	10/854,507	10/854,515	10/854,506
10/854,505	10/854,493	10/854,494	10/854,489	10/854,490	10/854,492	10/854,491
10/854,528	10/854,523	10/854,527	10/854,524	10/854,520	10/854,514	10/854,519
PLT036US	10/854,499	10/854,501	10/854,500	10/854,502	10/854,518	10/854,517
10/934,628	10/728,804	10/728,952	10/728,806	10/728,834	10/729,790	10/728,884
10/728,970	10/728,784	10/728,783	10/728,925	10/728,842	10/728,803	10/728,780
10/728,779	10/773,189	10/773,204	10/773,198	10/773,199	10/773,190	10/773,201
10/773,191	10/773,183	10/773,195	10/773,196	10/773,186	10/773,200	10/773,185

10/773,192	10/773,197	10/773,203	10/773,187	10/773,202	10/773,188	10/773,194
10/773,193	10/773,184	6,746,105	6,623,101	6,406,129	6,505,916	6,457,809
6,550,895	6,457,812	6,428,133	09/575,141	10/407,212	10/815,625	10/815,624
10/815,628	09/517,539	6566,858	09/112,762	6,331,946	6,246,970	6,442,525
09/517,384	09/505,951	6,374,354	09/517,608	09/505,147	6,757,832	6,334,190
6,745,331	09/517,541	10/203,559	10/203,540	10/203,564	10/636,263	10/63,6283
10/866,608	10/902,889	10/902,883	10/940,653	10/942,858	10/409,876	10/409,848
10/409,845	09/575,197	09/575,195	09/575,159	09/575,132	09/575,123	6,825,945
09/575,130	09/575,165	6,813,039	09/693,415	09/575,118	6,824,044	09/608,970
09/575,131	09/575,116	6,816,274	NPA019NUS	09/575,139	09/575,186	6,681,045
6,678,499	6,679,420	09/663,599	09/607,852	6,728,000	09/693,219	09/575,145
09/607,656	6,813,558	6,766,942	09/693,515	09/663,701	09/575,192	6,720,985
09/609,303	09/610,095	09/609,596	09/693,705	09/693,647	09/721,895	09/721,894
09/607,843	09/693,690	09/607,605	09/608,178	09/609,553	09/609,233	09/609,149
09/608,022	09/575,181	09/722,174	09/721,896	10/291,522	6,718,061	10/291,523
10/291,471	10/291,470	6,825,956	10/291,481	10/291,509	10/291,825	10/291,519
10/291,575	10/291,557	10/291,661	10/291,558	10/291,587	10/291,818	10/291,576
6,829,387	6,714,678	6,644,545	6,609,653	6,651,879	10/291,555	10/291,510
10/291,592	10/291,542	10/291,820	10/291,516	10/291,363	10/291,487	10/291,520
10/291,521	10/291,556	10/291,821	10/291,525	10/291,586	10/291,822	10/291,524
10/291,553	10/291,511	10/291,585	10/291,374	10/685,523	10/685,583	10/685,455
10/685,584	10/757,600	10/804,034	10/793,933	10/853,356	10/831,232	10/884,882
10/943,875	10/943,938	10/943,874	10/943,872	10/944,044	10/943,942	10/944,043
10/949,293	10/943,877	10/965,913	10/954,170	NPA174US	NPA175US	NPA176US
NPA177US	NPA178US	NPA179US	NPA181US	NPA182US	NPA183US	NPA184US
NPA185US	NPA186US	NPA187US	NPA188US	09/575,193	09/575,156	09/609,232
09/607,844	6,457,883	09/693,593	10/743,671	NPB010US	09/928,055	09/927,684
09/928,108	09/927,685	09/927,809	09/575,183	6,789,194	09/575,150	6,789,191
10/900,129	10/900,127	10/913,328	10/913,350	NPK010US	NPK011US	6,644,642
6,502,614	6,622,999	6,669,385	6,827,116	10/933,285	NPM016US	6,549,935
NPN004US	09/575,187	6,727,996	6,591,884	6,439,706	6,760,119	09/575,198
09/722,148	09/722,146	6,826,547	6,290,349	6,428,155	6,785,016	6,831,682
6,741,871	09/722,171	09/721,858	09/722,142	10/171,987	10/202,021	10/291,724
10/291,512	10/291,554	10/659,027	10/659,026	10/831,242	10/884,885	10/884,883
10/901,154	10/932,044	NPP051US	NPP052US	NPP053US	10/965,733	10/965,933
NPP058US	NPP060US	NPP061US	NPP062US	10/659,027	09/693,301	09/575,174
6,822,639	6,474,888	6,627,870	6,724,374	6,788,982	09/722,141	6,788,293

09/722,147	6,737,591	09/722,172	09/693,514	6,792,165	09/722,088	6,795,593
10/291,823	6,768,821	10/291,366	10/291,503	6,797,895	10/274,817	10/782,894
10/782,895	10/778,056	10/778,058	10/778,060	10/778,059	10/778,063	10/778,062
10/778,061	10/778,057	10/846,895	10/917,468	10/917,467	10/917,466	10/917,465
10/917,356	10/948,169	10/948,253	10/948,157	10/917,436	10/943,856	10/919,379
10/943,843	10/943,878	10/943,849	NPS086US	09/575,154	09/575,129	6,830,196
09/575,188	09/721,862	10/473,747	10/120,441	10/291,577	10/291,718	6,789,731
10/291,543	6,766,944	6,766,945	10/291,715	10/291,559	10/291,660	10/409,864
10/309,358	10/410,484	10/884,884	10/853,379	10/786,631	10/853,782	10/893,372
10/893,381	10/893,382	10/893,383	10/893,384	NPT046US	NPT047US	NPT048US
NPT049US	NPT050US	NPW001US	10/492,152	NPW003US	NPW004US	10/492,154
NPW007US	10/683,151	10/683,040	NPW012US	10/919,260	NPW013US	10/919,261
10/778,090	09/575,189	09/575,162	09/575,172	09/575,170	09/575,171	09/575,161
10/291,716	10/291,547	10/291,538	6,786,397	10/291,827	10/291,548	10/291,714
10/291,544.	10/291,541	10/291,584	10/291,579	10/291,824	10/291,713	10/291,545
10/291,546	10/917,355	10/913,340	10/940,668	NPX041US	6,593,166	10/428,823
10/849,931	10/815,621	10/815,612	10/815,630	10/815,637	10/815,638	10/815,640
10/815,642	10/815,643	10/815,644	10/815,618	10/815,639	10/815,635	10/815,647
10/815,634	10/815,632	10/815,631	10/815,648	10/815,614	10/815,645	10/815,646
10/815,617	10/815,620	10/815,615	10/815,613	10/815,633	10/815,619	10/815,616
10/815,614	10/815,636	10/815,649	10/815,609	10/815,627	10/815,626	10/815,610
10/815,611	10/815,623	10/815,622	10/815,629			

某些申请通过案卷号列出，这些案卷号将会在知道了申请号之后由申请号所代替。

背景技术

当前，主要有两种技术提供用于进行唯一产品项目识别的可替选方法，例如，EPC，即：

- 2D 光学条形码，以及
- RFID

2D 光学条形码包括可以沿二维存储约 2,000 字节数据的复合图像。统一代码协会 (Uniform Code Council) 和欧洲商品编号 (EAN) 国际组织已经对

大量 2D 条形码进行了标准化，它们比现有 EPC 具有大得多的数据容量。

现在，2D 光学条形码广泛用于全球制药业。在美国，食品及药物管理局（FDA）已经批准对在其管辖范围内制造的所有药品上使用 2D 光学条形码，以识别生产线。它们被接受的主要优点是，制造它们价廉。

2D 光学条形码的主要缺点是，通常因为标记破损难以读取它们，而且需要直接利用“瞄准线”扫描。此外，2D 光学条形码不美观，因此有损产品的包装。对于通常采用小包装，但是要求较大条形码的药品，这种问题严重，较大的条形码可能影响该包装上的实质内容。

对于 RFID 标签，也可以提供以 EPC 方式编码的唯一产品项目识别。然而，也存在 RFID 标签不适合某些产品的缺陷。

首先，生产 RFID 标签的成本高。其次，存在金属、液体和其它电磁频率（EMF）信号可能干扰 RFID 标签扫描仪，因此，严重危及 RFID 系统的可靠性和完整性。第三，可以远程读取标签，而无需知道标签持有者，因此，产生了对隐私的担忧。

面编码背景技术

Netpage 表面编码由密集的平面铺盖的标签组成。每个标签都编码其自身在该平面中的位置。每个标签还与相邻的标签结合起来对包含其的区域的标识符进行编码。该区域 ID 在所有区域中是唯一的。在 Netpage 系统中该区域通常对应于被标记表面的整个范围，如一页纸的一面。

设计表面编码是为了使大到足以保证能获取整个标签的获取视场大到能足以保证获取包含该标签的区域的 ID。获取该标签本身保证了获取该标签在该区域内的二维位置，以及其它该标签特有的数据。因此表面编码允许传感设备在仅仅与编码表面的局部交互作用的过程中(例如在用笔“点击”或敲打编码表面的过程中)获取区域 ID 和标签位置。

Netpage 表面编码的使用在下面的共同未决专利申请中有更为详细的描述，即 2004 年 4 月 2 日提交的 USSN 10/815, 647 (案卷号 HYG001US)，

名称为“Obtaining Product Assistance”; 2004年4月2日提交的 USSN 10/815609 (案卷号 HYT001US), 名称为“Laser Scanner Device for Printed Product Identification Code”。

加密技术的背景技术

加密技术用于在存储和发送中保护敏感信息并验证交易各方。现有两类加密技术正广泛使用：秘密密钥加密和公用密钥加密。

秘密密钥加密也称为对称加密，其采用相同的密钥来对消息加密和解密。希望交换消息的双方首先必须协商安全地交换密钥。

公用密钥加密也称为非对称加密，其使用两个加密密钥。这两个密钥在数学上以使用一个密钥加密的任何消息都只能用另一个密钥解密的方式相关。然后将一个密钥公布，而另一个密钥保持秘密。它们分别被称为公用密钥和专用密钥。公用密钥用于对任何要发送给专用密钥持有者的消息进行加密。一旦使用公用密钥加密，则只能用专用密钥对消息解密。因此双方可以安全地交换消息而不必首先交换秘密密钥。为了保证专用密钥是可靠的，通常专用密钥的持有者要产生公用-专用密钥对。

公用密钥加密可用于创建数字签名。如果专用密钥的持有者创建了已知的消息的散列，然后使用专用密钥对该散列加密，则任何人只需通过使用公用密钥对已加密的散列解密并针对该消息验证该散列，就可以验证加密的散列是否构成专用密钥持有者对于该特定消息的“签名”。如果该消息添加了该签名，则该消息的接收者可以验证消息是否真实和是否在发送过程中被更改过。

秘密密钥也可以用于创建数字签名，但存在签名验证也可以由与该密钥有利害关系的一方执行的缺陷。

为了使公用密钥加密工作，必须存在防止假冒的分发公用密钥的途径。这在正常情况下使用证书和认证机构来实现。认证机构是受信的第三方，其验证公用密钥与个人或其它实体的身份之间的联系。认证机构通过检查身份

文件等等来验证身份，然后创建并签署包含该身份细节和公用密钥的数字证书。任何受信该认证机构的人都可以在高度确认其真实性的情况下使用该证书中的公用密钥。他们只需要验证该证书是否确实由该认证机构签名，该认证机构的公用密钥是公知的。

为了达到与秘密密钥加密相类似的安全性，公用密钥加密利用长度量级更大的密钥，即密钥为几百位，而公用密钥为几千位。

Schneier B. (Applied Cryptography, Second Edition, John Wiley & Sons 1996) 对密码技术进行了详细的讨论。

发明内容

根据第一基本形式，本发明提供了一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少一部分身份；至少一部分签名；以及该编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

该签名优选是至少部分身份和至少部分预定填充位的数字签名。

该填充位优选与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：预定数；以及随机数。

每个数据部分优选编码签名单段。

优选在多个数据部分内编码整个签名。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名的第二符号的位置。

该编码数据优选对于目视基本上不可见。

优选至少利用如下之一，在该表面上印刷该编码数据：不可见油墨；以及红外吸收油墨。

优选基本上与可见的人可读信息重合设置该编码数据。

至少一些编码数据部分优选编码至少表示如下之一的数据：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名片段的身份；以及被指示区位的诸单元。

该编码数据优选包括至少如下之一：冗余数据；允许纠错的数据；RS（Reed-Solomon）数据；以及循环冗余校验（CRC）数据。

数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；以及利用专用密钥产生的，而利用相应公用密钥可核实的密码文本。

该身份优选包括至少如下之一的身份：用于限定该表面的对象；该表面；该表面上的区域；以及与该表面相关的对象。

至少一个编码数据部分优选至少进一步对数据对象片段进行编码。

数据对象优选包括至少如下之一：数字签名；多用途因特网邮件扩展（MIME）数据；文本数据；图像数据；声频数据；视频数据；应用数据；联系数据；业务名片数据；以及目录数据。

该表面优选与对象相关，该对象包括至少如下之一：制造项目；药品项目；钞票；支票；信用卡或者借记卡；可赎回票、凭单或者息票；彩票或者即刻兑奖票；以及身份证件或者诸如驾驶证或者护照的身份证件。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该编码数据优选适合被感测装置感测，以确定身份以及至少一部分签名。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

该表面优选具有布置在其内或者其上、根据权利要求 1 的编码数据，该编码数据编码该对象的身份。

该编码数据优选包括多个编码数据部分，每个编码数据部分至少编码数据对象片段，以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

优选将该编码数据布置在对象表面之内或者之上。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数

据设置在与该对象相关的表面之上或者之内，每个编码数据部分对下述进行编码：该对象的身份；以及签名片段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段；利用该指示数据，确定收到的身份和多个收到的签名片段；利用该多个签名片段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

用于验证对象的装置优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：传感器，用于感测编码数据，该编码数据编码：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第二基本形式，本发明提供了一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少一部分身份；至少一部分签名；以及该编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

其中该填充位优选与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：预定数；以及随机数。

每个数据部分优选编码签名片段。

优选在多个数据部分内编码整个签名。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

该编码数据优选对于目视基本上不可见。

优选至少利用如下之一，在表面上印刷该编码数据：不可见油墨；以及红外吸收油墨。

优选基本上与可见的人可读信息重合设置该编码数据。

至少一些编码数据部分优选编码至少表示如下之一的数据：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名片段的身份；以及被指示区位的诸单元。

该编码数据优选包括至少如下之一：冗余数据；允许纠错的数据；里德-索罗门（Reed-Solomon）数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；以及利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一的身份：用于限定该表面的对象；该表面；该表面上的区域；以及与该表面相关的对象。

至少一个编码数据部分优选至少进一步对数据对象片段进行编码。

数据对象优选包括至少如下之一：数字签名；多用途因特网邮件扩展（MIME）数据；文本数据；图像数据；声频数据；视频数据；应用数据；联系数据；业务名片数据；以及目录数据。

该表面优选与对象相关，该对象包括至少如下之一：制造项目；药品项目；钞票；支票；信用卡或者借记卡；可赎回票、凭单或者息票；彩票或者即刻兑奖票；以及身份证件或者诸如驾驶执照或者护照的身份证件。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该编码数据优选适合被感测装置感测，以确定身份以及至少一部分签名。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

一种优选与表面相关的对象，该表面具有布置在其内或者其上的编码数据，其中该编码数据编码该对象的身份。

该编码数据优选布置在表面之上或者之内，该编码数据包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

优选将该编码数据布置在对象表面之上或者之内。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该

指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利

用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

用于验证对象的装置优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：传感器，用于感测编码数据，该编码数据编码：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第三基本形式，本发明提供了一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及该编码数据部分在该表面上的位置。

每个数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该数据对象优选包括至少部分签名，该签名是至少部分身份的数字签名。

该签名优选是至少部分身份和至少部分预定填充位的数字签名。

该填充位优选与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：预定数；以及随机数。

每个数据部分优选编码签名单段。

优选在多个数据部分内编码该数据对象。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分数据对象的第二符号的位置。

该编码数据优选对于目视基本上不可见。

优选至少利用如下之一，在表面上印刷该编码数据：不可见油墨；以及红外吸收油墨。

优选基本上与可见的人可读信息重合设置该编码数据。

至少一些编码数据部分优选编码至少表示如下之一的数据：各数据部分的区位；各数据部分在该表面上的位置；数据部分的大小；数据对象的大小；数据对象片段的身份；以及被指示区位的诸单元。

该编码数据优选包括至少如下之一：冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该签名包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一的身份：用于限定该表面的对象；该表面；该表面上的区域；以及与该表面相关的对象。

该数据对象优选包括至少如下之一：多用途因特网邮件扩展(MIME)数据；文本数据；图像数据；声频数据；视频数据；应用数据；联系数据；业

务名片数据；以及目录数据。

该表面优选与对象相关，该对象包括至少如下之一：制造项目；药品项目；钞票；支票；信用卡或者借记卡；可赎回票、凭单或者息票；彩票或者即刻兑奖票；以及身份证件或者诸如驾驶证或者护照的身份证件。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该编码数据优选适合被感测装置感测，以至少确定身份以及数据对象。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

一种优选与表面相关的对象，该表面具有布置在其内或者其上、根据权利要求 1 的编码数据，该编码数据编码该对象的身份和与该对象相关的数据对象。

每个编码数据部分优选进一步编码至少部分签名，该签名是至少部分身份的数字签名。

每个编码数据部分优选进一步编码至少部分签名，该签名是至少如下之一的数字签名：部分身份；以及部分预定填充位。

编码数据优选布置在对象表面之内或者之上，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在计算机系统中：从感测装置接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名片段；利用该多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括：感测该编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名片段，该签名是至少部分

身份的数字签名；利用该多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该方法包括，在处理器内：接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证对象的方法中优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，每个编码数据部分进一步编码签名片段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段；利用该指示数据，确定收到的身份和多个收到的签名片段；利用该多个签名片段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

用于验证对象的装置优选使用该编码数据，而且将该编码数据设置在与该对象相关的表面之上或者之内，该装置包括：传感器，用于感测编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第四基本形式，本发明提供了一种具有表面的对象，该表面具有布置在其上或者其内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分

身份的数字签名。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

其中该签名优选是至少部分身份和至少部分预定填充位的数字签名。

该填充位优选与该身份相关，而且对于该身份是唯一的，该填充位是至少如下之一：预定数；以及随机数。

每个数据部分优选编码签名单段。

优选在多个数据部分内编码整个签名。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名的第二符号的位置。

该编码数据优选对于目视基本上不可见。

优选至少利用如下之一，在该表面上印刷该编码数据：不可见油墨；以及红外吸收油墨。

优选基本上与可见的人可读信息重合设置该编码数据。

至少一些编码数据部分优选编码至少表示如下之一的数据：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名片段的身份；以及被指示区位的诸单元。

该编码数据优选包括至少如下之一：冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；以及利用专用密钥产生的，而利用

相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

至少一个编码数据部分优选至少进一步对数据对象片段进行编码。

该数据对象优选包括至少如下之一：数字签名；多用途因特网邮件扩展(MIME)数据；文本数据；图像数据；声频数据；视频数据；应用数据；联系数据；业务名片数据；以及目录数据。

该对象优选包括至少如下之一：制造项目；药品项目；钞票；支票；信用卡或者借记卡；可赎回票、凭单或者息票；彩票或者即刻兑奖票；以及身份证件或者诸如驾驶证或者护照的身份证件。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该编码数据优选适合被感测装置感测，以确定该身份以及至少一部分签名。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

其中该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

在验证该对象的方法中优选使用该对象，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证该对象的方法中优选使用该对象，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

在验证对象的方法中优选使用该对象，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在验证该对象的方法中优选使用该对象，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用

该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证该对象的方法中优选使用该对象，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

在使用处理器验证该对象的方法中优选使用该对象，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

用于验证该对象的装置优选使用该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第五基本形式，本发明提供了一种用于验证对象的方法，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及利用该指示数据，确定收到的身份和收到的签名部

分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，在计算机系统中：产生表示该验证是成功还是失败的验证数据；以及将该验证数据传送到用户。

该方法优选包括，在计算机系统中，将该验证数据传送到感测装置。

该指示数据优选进一步表示签名部分的身份，而且其中该方法包括，在计算机系统中：利用该指示数据，确定收到的签名部分身份；利用收到的身份，确定一被确定的签名；以及利用确定的签名和收到的签名部分身份，确定一被确定的签名部分。

该方法优选包括，在计算机系统中，利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

该方法优选包括，在计算机系统中，利用该存储数据和收到的身份，产生确定的签名部分。

该方法优选包括，在计算机系统中：利用该存储数据和收到的身份，产生确定的签名；选择确定的签名的一部分；以及将选择的签名部分与收到的签名部分进行比较。

该方法优选包括，在计算机系统中：利用指示数据确定收到的签名部分身份；利用收到的签名部分身份，选择部分确定签名。

该方法优选包括，在计算机系统中，从远程数据库中检索存储数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在计算机系统中：利用收到的身份，确定预定填充位；以及利用该预定填充位和收到的身份，确定一被确定的签名部分。

计算机系统优选构成该感测装置的部分。

该方法优选包括，在该计算机系统中，通过至少如下之一，与该感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名部分的大小；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

布置在与该对象相关的表面之上或者之内的编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

布置在与该对象相关的表面之上或者之内的编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下之一的数字签名：部分身份；以及部分预定填充位。

布置在该对象表面之上或者之内的编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较

结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

根据第六基本形式，本发明提供了一种用于验证对象的方法，该方法包括，在感测装置：感测设置在与该对象相关的表面之上或者之内的编码数据；利用感测的编码数据，确定指示数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及将该指示数据传送到计算机系统，该计算机系统响应该指示数据，以：利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较

结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少一部分身份；至少一部分签名；以及该编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份和至少部分签名，该方法包括感测至少一个数据部分。

该方法优选包括，在感测装置内：接收表示该验证是成功还是失败的验证数据；以及将该验证是成功还是失败的指示提供给用户。

优选在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：感测许多编码部分；以及产生指示整个签名的指示数据。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，在该表面上印刷该编码数据，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

计算机系统优选构成该感测装置的部分。

该方法优选包括，在该感测装置内，通过至少如下之一，与该计算机系统通信：通信网；因特网；移动电话网；以及无线连接。

该方法优选包括，在该感测装置内，产生至少指示如下之一的指示：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第七基本形式，本发明提供了一种验证对象的方法，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据；该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部

分进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及该编码数据部分在该表面上的位置。

每个编码数据部分优选编码该整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，产生表示该验证是成功还是失败的表示。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少签名单段；其中该方法包括，至少感测一个编码数据部分。

该编码数据优选进一步表示签名部分的身份，而且其中该方法包括：确定感测的签名部分的签名部分身份；利用感测的身份，确定一被确定的签名；以及利用感测的签名部分的签名部分身份且根据确定的签名来选择确定的签名部分。

该方法优选包括利用感测的身份从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

该方法优选包括，利用该存储数据和感测的身份，确定一被确定的签名部分。

该方法优选包括从远程数据库检索存储数据。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名部分的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该

表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括：利用身份，确定预定填充位；以及利用该预定填充位和确定的签名，产生一被产生的身份。

优选在感测装置内执行该方法，该感测装置具有：图像传感器，用于感测编码数据；以及处理器，用于验证该对象。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名部分的大小；签名部分的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选根据至少一个具有 n 重旋转对称的布局，排列该编码数据，其中 n

至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，

产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

处理器优先用于验证该对象的方法中，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

优先利用处理器验证该对象，该对象与在其上或者其内布置了该编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

装置优先利用该方法验证该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第八基本形式，本发明提供了一种用于验证对象的方法，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名片段；利用多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，在计算机系统中：产生表示该验证是成功还是失败的验证数据；以及将该验证数据传送到用户。

该方法优选包括，在计算机系统中，将该验证数据传送到感测装置。

该指示数据优选进一步表示多个签名片段中每个签名片段的身份，而且其中该方法包括，在计算机系统中：利用该指示数据，确定多个签名片段中每个签名片段的身份；以及利用确定的签名片段身份，确定一被确定的签名。

该方法优选包括，在计算机系统中：利用收到的身份，从数据存储装置中检索存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；以及公用密钥；以及利用该存储数据和确定的签名，产生一被产生的身份。

优选利用至少如下之一索引该存储数据：该身份；以及一范围的身份。

该方法优选包括，在计算机系统中，从远程数据库中检索该存储数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其

中该方法包括，在计算机系统中：利用收到的身份，确定预定填充位；以及利用该预定填充位和确定的签名，产生一被产生的身份。

多个签名字段优选指示整个签名。

该计算机系统构成该感测装置的部分。

该方法优选包括，在计算机系统中，通过至少如下之一，与该感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名片段的大小；签名片段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n

至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

装置优选利用该方法验证该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第九基本形式，本发明提供了一种用于验证对象的方法，该方法包括，在感测装置内：感测设置在与该对象相关的表面上的编码数据；根据感测的编码数据，确定指示如下所述的指示数据：该对象的身份；以及多个签

名片段，该签名是至少部分身份的数字签名；将该指示数据传送到计算机系统，该计算机系统响应该指示数据，以：利用该指示数据，确定该身份和多个签名单段；利用多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，在感测装置内：接收表示该验证是成功还是失败的验证数据；以及将该验证是成功还是失败的指示提供给用户。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少签名单段；其中该方法包括，在该感测装置内，感测多个编码数据部分，从而确定指示数据。

每个编码数据部分优选分别编码签名单段身份，而且其中该方法包括，在该感测装置内：确定每个确定的签名单段的签名单段身份；以及利用确定的签名单段身份、确定的签名，产生该指示数据。

多个签名单段优选指示整个签名。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名单段的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在该感测装置内，利用红外检测器感测该编码数据。

该计算机系统优选构成该感测装置的部分。

该方法优选包括，在该感测装置内，通过至少如下之一，与该计算机系统通信：通信网；因特网；移动电话网；以及无线连接。

该方法优选包括，在该感测装置内，产生至少指示如下之一的指示：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSM 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据

的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第十基本形式，本发明提供了一种用于验证对象的方法，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据；利用感测的编码数据确定：该对象的身份；多个签名片段，该签名是至少部分身份的数字签名；利用多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，产生表示该验证是成功还是失败的表示。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少签名片段；其中该方法包括感测多个编码数据部分，从而确定多个签名片段。

每个编码数据部分优选分别编码签名片段身份，而且其中该方法包括：确定每个确定的签名片段的签名片段身份；以及利用确定的签名片段身份，确定一被确定的签名。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名片段的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括利用红外检测器感测该编码数据。

多个签名单段优选指示整个签名。

该方法优选包括：利用该身份，从数据存储装置中检索存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；以及公用密钥；以及利用该存储数据和确定的签名，产生一被产生的身份。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

该方法优选包括，从远程数据库中检索该存储数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括：利用该身份确定预定填充位；以及利用该预定填充位和确定的签名，产生一被产生的身份。

该方法优选包括，在感测装置中：利用传感器感测该编码数据；利用处理器：根据感测的编码数据，确定：该对象的身份；多个签名单段，该签名是至少部分身份的数字签名；利用多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行

国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身

份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用该多个签名单段，确定一被确定的签名部分；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单片

段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

装置优选利用该方法验证该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第十一基本形式，本发明提供了一种利用处理器验证对象的方法，该方法包括，在处理器中：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，在处理器中：产生表示该验证是成功还是失败的验证数据；以及将该验证数据传送到用户。

该方法优选包括，在处理器中，将该验证数据传送到感测装置。

该指示数据优选进一步表示签名部分的身份，而且其中该方法包括，在处理器中：利用该指示数据，确定收到的的签名部分身份；利用收到的身份，选择确定的签名的部分；以及通过将被确定的签名部分与至少一个收到的签名部分进行比较，验证该对象。

该方法优选包括，在处理器中，利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

该方法优选包括，在处理器中，利用该存储数据和收到的身份，产生确定的签名部分。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在处理器中：利用收到的身份，确定预定填充位；以及利用该预定填充位和收到的身份，确定一被确定的签名部分。

该处理器优选构成感测装置的一部分，而且其中该方法包括从该感测装置内的传感器接收该指示数据。

该处理器优选与产生该指示数据的感测装置通信，而且其中该方法包括，从该感测装置接收该指示数据。

该方法优选包括，在处理器中，通过至少如下之一，与该感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名部分的大小；签名部分的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上

的区域。

该身份优选包括至少如下之一：电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名部分的第二符号的位置。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

该方法优选包括，在处理器中，从远程数据库中检索该存储数据。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：该身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名单段；利用多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名单段，该签名是至少部分身份的数字签名；利用该多个签名单段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

装置优选利用该方法验证该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名单段；利用感测的身份和至少一个感测的签名单段，验证该对象。

根据第十二基本形式，本发明提供了一种利用处理器验证对象的方法，该方法包括，在感测装置内：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定指示如下所述的指示数据：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；将该指示数据送到处理器，该处理器响应该指示数据，以：利用该身份和保密密钥，产生签名；将确定的签名与该至少部分签名进行比较；以及利用该比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

根据第十三基本形式，本发明提供了一种用于验证对象的处理器，该对象与其上或者其内设置了编码数据的表面相关，该编码数据指示：该对象的

身份；以及至少部分签名，该签名是至少部分身份的数字签名，其中该处理器：接收指示数据，响应感测到该编码数据，产生该指示数据，该指示数据指示该身份和至少部分签名；利用该指示数据，确定该身份和至少部分签名；利用确定的身份和保密密钥，产生确定的签名；将确定的签名与该至少部分签名进行比较；利用该比较结果，验证对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

该编码数据优选包括许多编码数据部分，每个编码数据部分编码该身份以及至少部分签名，该方法包括至少感测一个数据部分。

该方法优选包括，在感测装置内：接收表示该验证是成功还是失败的验证数据；以及将该验证是成功还是失败的指示提供给用户。

优选在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：感测许多编码部分；以及产生指示整个签名的指示数据。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少部分签名的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

该处理器优选构成该感测装置的部分。

该方法优选包括，在该感测装置内，通过至少如下之一，与该处理器通信：通信网；因特网；移动电话网；以及无线连接。

该方法优选包括，在该感测装置内，产生至少指示如下之一的指示：各数

据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；
签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德
-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的
键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份
的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身
份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公
用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的
区域。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)
号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面
额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；
发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少
如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理
器利用收到的身份和保密密钥产生确定的签名。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至
少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一
个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数
据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至
少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中
 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个
区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的
 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的
旋转程度。

该处理器优选：产生表示该验证是成功还是失败的验证数据；以及将该验

证数据传送到用户。

该处理器优选将该验证数据传送到感测装置。

该指示数据优选进一步表示签名部分的身份，而且其中该处理器：利用该指示数据，确定收到的签名部分身份；利用收到的身份，选择确定的签名的部分；以及通过将被确定的签名部分与该至少一个收到的签名部分进行比较，验证该对象。

优选利用收到的身份，该处理器从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

利用该存储数据和收到的身份，该处理器产生确定的签名部分。

该处理器优选从远程数据库中检索该存储数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该处理器：利用收到的身份，确定预定填充位；以及利用该预定填充位和收到的身份，确定一被确定的签名部分。

该处理器优选构成该感测装置的部分。

该处理器优选与产生指示数据的感测装置通信，而且其中该处理器从该感测装置接收该指示数据。

优选通过至少如下之一，该处理器与该感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名部分的大小；签名部分的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公

用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的身份和保密密钥产生确定的签名。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第十四基本形式，本发明提供了一种利用处理器验证对象的方法，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名单段，该签名是至少部分身份的数字签名，该方法包括，在该处理器内：从感测装置接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的签名部分；将被确定的身份与收到的身份进行比较；以及利用该

比较结果，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该方法优选包括，在处理器中：产生表示该验证是成功还是失败的验证数据；以及将该验证数据传送到用户。

该方法优选包括，在处理器中，将该验证数据传送到感测装置。

该指示数据优选进一步表示每个签名单段的身份，而且其中该方法包括，在处理器中：利用该指示数据，对每个收到的签名单段确定收到的签名单段身份；利用每个收到的签名单段的收到的签名单段身份，确定一被确定的签名；以及利用确定的签名和保密密钥，确定一被确定的身份。

该方法优选包括，在处理器中，利用收到的身份，从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

该方法优选包括，在处理器中，利用该存储数据和收到的签名单段，确定一被确定的身份。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，利用红外检测器感测该编码数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该方法包括，在处理器中：利用收到的身份，确定预定填充位；以及利用该预定填充位和收到的签名单段，确定一被确定的身份。

该处理器优选构成感测装置的一部分，而且其中该方法包括从该感测装置内的传感器接收该指示数据。

该处理器优选与产生该指示数据的感测装置通信，而且其中该方法包括，

从该感测装置接收该指示数据。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该指示数据优选指示整个签名。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的签名单段和保密密钥产生确定的身份。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的

n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一个签名单段的第二符号的位置。

该方法优选包括在该处理器中从远程数据库中检索该存储数据。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

该方法优选包括，在该处理器内，通过至少如下之一，与感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示；该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签

名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名片段；利用多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该方法优选进一步包括：感测设置在与该对象相关的表面之上或者之内的编码数据；根据感测的编码数据，确定：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

优选利用处理器验证该对象，该方法包括，在处理器内：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用该收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

装置优选利用该方法验证该对象，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用感测的身份和至少一个感测的签名部分，验证该对象。

根据第十五基本形式，本发明提供了一种用于验证对象的处理器，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名片段，

该签名表示至少部分身份的数字签名，其中该处理器：从感测装置接收指示数据，响应于感测多个编码数据部分，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及多个签名单段；利用该指示数据，确定收到的身份和多个收到的签名单段；利用该多个签名单段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；利用该比较结果，验证对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及该编码数据部分在该表面上的位置。

每个编码数据部分优选编码该整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该处理器优选将该验证数据传送到感测装置。

该指示数据优选进一步表示每个签名单段的身份，而且其中该处理器：利用该指示数据，确定每个收到的签名单段的收到签名部分身份；利用每个收到的签名单段的收到签名部分身份，确定一被确定的签名；以及利用确定的签名和保密密钥，确定一被确定的身份。

优选利用收到的身份，该处理器从数据存储装置中检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名。

优选至少利用如下之一索引该存储数据：该身份；以及一范围的身份。

优选利用该存储数据和收到的签名单段，该处理器确定一被确定的身份。

该处理器优选从远程数据库中检索该存储数据。

该签名优选是至少部分身份和至少部分预定填充位的数字签名，而且其中该处理器：利用收到的身份，确定预定填充位；以及利用该预定填充位和收到的签名单段，确定一被确定的身份。

该处理器优选构成该感测装置的部分。

该处理器优选与产生指示数据的感测装置通信，而且其中该处理器从该感测装置接收该指示数据。

优选通过至少如下之一，该处理器与该感测装置通信：通信网；因特网；移动电话网；以及无线连接。

该指示数据优选进一步指示至少如下之一：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与该身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的签名单段和保密密钥产生确定的身份。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第十五基本形式，本发明提供了一种利用处理器验证对象的方法，该对象与其上或者其内设置了编码数据的表面相关，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名片段，该签名是至少部分身份的数字签名，该方法包括，在感测装置中：感测多个编码数据部分；利用感测的编码数据部分，确定指示数据，该指示数据指示：该对象的身份；以及多个签名片段；将该指示数据送到该处理器，响应该指示数据，该处理器：利用该指示数据，确定收到的身份和多个收到的签名片段；利用该多个签名片段和保密密钥，确定一被确定的身份；将被确定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

该方法优选包括，在感测装置内：接收表示该验证是成功还是失败的验证数据；以及将该验证是成功还是失败的指示提供给用户。

优选在多个数据部分内编码整个签名，而且其中该方法包括，在感测装置内：感测许多编码部分；以及产生指示整个签名的指示数据。

该编码数据优选包括多个布局，每个布局用于限定多个用于编码该身份的第一符号和多个用于限定至少一部分签名的第二符号的位置。

该编码数据优选包括多个标签，每个编码数据部分至少由一个标签构成。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该方法包括，在感测装置内，利用红外检测器感测该编码数据。

该处理器优选构成该感测装置的部分。

该方法优选包括，在该感测装置内，通过至少如下之一，与该计算机系统通信：通信网；因特网；移动电话网；以及无线连接。

该方法优选包括，在该感测装置内，产生至少指示如下之一的指示：各数据部分的区位；各数据部分在表面上的位置；数据部分的大小；签名的大小；签名单段的身份；被指示区位的诸单元；冗余数据；允许纠错的数据；里德-索罗门数据；以及循环冗余校验（CRC）数据。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密，产生的密码文本。

该身份优选包括至少如下之一的身份：该对象；该表面；以及该表面上的区域。

该身份优选包括至少如下之一：电子产品代码(EPC)；国家药品代码(NDC)号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选通过与第二处理器通信，该处理器确定一被确定的签名，该第二处理器利用收到的签名单段和保密密钥产生确定的身份。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n

个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第十七基本形式，本发明提供了一种用于验证对象的装置，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少一部分签名，该签名是至少部分身份的数字签名；以及处理器，用于：利用感测的编码数据，确定感测的身份和至少一个感测的签名部分；利用确定的身份和至少一个感测的签名部分，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

优选由多个签名部分构成该整个签名，而且其中每个编码数据部分编码各自的签名部分。

该装置优选包括指示器，用于指示该验证是成功还是失败。

该处理器优先用于：利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该处理器优先用于：利用感测的身份和密钥，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比较结果，验证该对象。

该处理器优先用于：利用感测的编码数据，确定多个感测的签名部分；利用感测的签名部分，确定一被确定的签名；利用确定的签名部分和密钥，确定一被确定的身份；将感测的身份与确定的身份进行比较；以及利用该比较结果，验证该对象。

该装置优选包括数据存储装置，而且其中该处理器：利用感测的身份，

检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名；利用该存储数据，验证该对象。

该数据存储装置优选是远程数据库。

该处理器优选利用感测的编码数据确定多个用于指示整个签名的签名部分。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该传感器是至少如下之一：红外检测器；以及激光扫描仪。

该装置优选是至少如下之一：文件扫描仪；现金出纳机；Netpage 笔；钞票扫描仪；手持扫描仪；具有内置扫描仪的移动电话；自动柜员机；以及自动售货机。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一：至少如下之一的身份：该对象；该表面；以及该表面上的区域；以及电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n

至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该装置优选包括指示器，用于指示该验证是成功还是失败。

优选利用不可见油墨和红外吸收油墨至少之一，将该编码数据印刷在该表面上，而且其中该传感器是至少如下之一：红外检测器；以及激光扫描仪。

该装置优选是至少如下之一：文件扫描仪；现金出纳机；Netpage 笔；钞票扫描仪；手持扫描仪；具有内置扫描仪的移动电话；自动柜员机；以及自动售货机。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一：至少如下之一的身份：该对象；该表面；以及该表面上的区域；以及电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

该处理器优选根据感测的编码数据确定指示数据，该指示数据指示多个代表整个签名的签名部分。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示

数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名。

该编码数据优选包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少部分签名，该签名是至少如下的数字签名：部分身份；以及部分预定填充位。

该编码数据优选包括多个编码数据部分，每个编码数据部分对下述进行编码：身份；以及至少数据对象片段；以利用多个编码数据部分对整个数据对象编码至少一次的方式，排列该数据部分。

该装置优选用于验证对象的方法，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，该感测装置产生该指示数据，该指示数据指示：该对象的身份；以及至少部分片段，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和收到的签名部分；利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该装置优选用于验证对象的方法，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用感测的编码数据，确定感测的身份和感测的签名部分；利用感测的身份，确定至少一被确定的签名部分；将被确定的签名部分与感测的签名部分进行比较；以及利用该比

较结果，验证该对象。

该装置优先用于验证对象的方法，该方法包括，在计算机系统中：从感测装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该指示数据，确定该身份和多个签名片段；利用多个签名片段，确定一被确定的签名；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该装置优先用于验证对象的方法，该方法包括：感测设置在与该对象相关的表面之上或者之内的编码数据；利用感测的编码数据，确定：该对象的身份；以及多个签名片段，该签名是至少部分身份的数字签名；利用该多个签名片段，确定一被确定的身份；利用被确定的签名和密钥，产生一被产生的身份；将该身份与被产生的身份进行比较；以及利用该比较结果，验证该对象。

该装置优先用于验证对象的方法，该方法包括，在处理器中：接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和保密密钥，确定一被确定的签名；将确定的签名与该至少一个收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该装置优先用于验证对象的方法，该编码数据具有许多编码数据部分，每个编码数据部分对下述进行编码：该对象的身份；以及签名片段，该签名是至少部分身份的数字签名；该方法包括，在处理器内：接收指示数据，响应于感测多个编码数据部分，产生该指示数据，该指示数据指示：该对象的身份；以及多个签名片段；利用该指示数据，确定收到的身份和多个收到的签名片段；利用该多个签名片段和保密密钥，确定一被确定的身份；将被确

定的身份与收到的身份进行比较；以及利用该比较结果，验证该对象。

根据第十八基本形式，本发明提供了一种用于验证对象的装置，该装置包括：传感器，用于感测设置在与该对象相关的表面之上或者之内的编码数据，该编码数据编码：身份；以及至少部分签名，该签名是至少部分身份的数字签名；以及处理器，用于利用感测的编码数据，确定指示数据，该指示数据指示：该身份；至少一个签名部分；通信系统，用于将该指示数据传递到计算机系统，该计算机系统响应该指示数据验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该装置优选通过至少如下之一与该计算机系统通信：通信网；因特网；移动电话网；以及无线连接。

该计算机系统优选用于：利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

根据第十九基本形式，本发明提供了一种用于验证对象的计算机系统，该计算机系统用于：从装置接收指示数据，响应于对设置在与该对象相关的表面之上或者之内的编码数据进行感测，产生该指示数据，该指示数据指示：该对象的身份；以及至少部分签名，该签名是至少部分身份的数字签名；利用该指示数据，确定收到的身份和至少一个收到的签名部分；利用收到的身份和至少一个收到的签名部分，验证该对象。

该编码数据优选包括许多编码数据部分，而且其中每个编码数据部分至少部分地指示至少如下之一：至少部分身份；至少部分签名；以及编码数据部分在该表面上的位置。

每个编码数据部分优选编码整个签名。

该整个签名优选由多个签名部分构成，而且其中每个编码数据部分编码各自的签名部分。

该计算机系统优选用于：利用收到的身份，确定至少一被确定的签名部分；将被确定的签名部分与收到的签名部分进行比较；以及利用该比较结果，验证该对象。

该计算机系统优选用于：利用该指示数据，确定多个收到的签名部分；利用收到的签名部分，确定一被确定的签名；利用被确定的签名和密钥，确定一被确定的身份；将收到的身份与确定的身份进行比较；以及利用该比较结果，验证该对象。

该计算机系统优选：产生表示该验证是成功还是失败的验证数据；以及将该验证数据传送到用户。

该计算机系统优选包括数据存储装置，而且其中该计算机系统：利用感测的身份，检索指示该数字签名的存储数据，该存储数据包括至少如下之一：与该签名相关的填充位；专用密钥；公用密钥；一个或者多个数字签名部分；以及数字签名；利用该存储数据，验证该对象。

该数据存储装置优选是远程数据库。

该计算机系统优选利用感测的编码数据确定多个用于指示整个签名的签名部分。

该计算机系统优选将验证数据传送到该装置。

该计算机系统优选通过至少如下之一与该装置通信：通信网；因特网；移动电话网；以及无线连接。

该数字签名优选包括至少如下之一：与身份有关的随机数；至少该身份的键控散列；利用专用密钥产生的，而利用相应公用密钥可核实的至少该身份的键控散列；通过对至少该身份进行加密产生的密码文本；通过对至少该身份和随机数进行加密产生的密码文本；利用专用密钥产生的，而利用相应公用密钥可核实的密码文本；以及利用 RSA 加密产生的密码文本。

该身份优选包括至少如下之一：至少如下之一的身份：该对象；该表面；

以及该表面上的区域；以及电子产品代码（EPC）；国家药品代码（NDC）号；药品项目序列号；钞票属性，包括至少如下之一：货币；发行国家；面额；券面；印刷工厂；以及序列号；支票属性，包括至少如下之一：货币；发行机构；账号；序列号；到期日；支票值；以及限额；卡属性，包括至少如下之一：卡类型；发行机构；账号；发行日期；到期日；以及限额。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局包括 n 个围绕旋转中心绕 $1/n$ 圈间隔的相同子布局，至少一个子布局包括用于将该子布局与每个其他子布局互相区别开的旋转指示数据。

优选至少根据一个具有 n 重旋转对称的布局，排列该编码数据，其中 n 至少是 2，该布局编码包括 n 个符号的 m 整数倍的序列的取向指示数据，其中 m 是 1 或者大于 1，每个编码符号分布在围绕该布局的旋转对称中心的 n 个区位，以致在该布局的 n 个取向的每个上来解码各符号产生取向指示数据的 n 个表示，每个表示包括取向指示数据的不同循环移位，而且指示该布局的旋转程度。

根据第十二基本形式，本发明提供了一种用于核实对象的方法，其中该方法包括，在计算机系统中：接收核实请求，至少该请求的一部分表示：该对象的身份；至少一个签名单段，该签名是至少部分身份的数字签名；利用该核实请求，确定一被确定的身份；利用确定的身份，从数据库中，至少确定一个与该核实有关的判据；将收到的核实请求与该至少一个判据进行比较；以及如果满足该至少一个判据，则确认该对象。

该至少一个判据优选至少与如下之一的限制有关：大量收到的核实请求；收到核实请求的速率；以及收到核实请求的时间。

优选根据至少如下之一确定该限制：该对象的身份；该签名；该签名单段；核实请求信源；以及该对象。

该限制优选与签名单段的大小成比例。

该方法优选包括，在计算机系统中：利用该核实请求，确定：请求历史，表示先前收到的核实请求的数目；以及相应限制；利用该核实请求和该请求

历史，确定请求数量；以及如果该请求数量不超过相应限制，则确认该对象。

该方法优选包括，在计算机系统中，响应核实请求，更新该请求历史。

该请求历史优选表示收到核实请求的时间。

请求历史优选与如下相关：该对象的身份；该签名；该签名单段；核实请求信源；以及该对象。

该方法优选包括，在计算机系统中，通过利用该对象的身份和至少一个签名单段验证该对象，确认该对象。

至少该核实请求的一部分优选表示该签名单段的身份。

该对象优选与其上或者其内设置了编码数据的表面相关，该编码数据包括许多编码数据部分，每个编码数据部分至少表示该身份和签名单段，而且其中响应感测到至少一个编码数据部分，感测装置产生核实请求。

优选至少该核实请求的一部分表示签名单段的身份，该片段身份至少基于如下之一：在至少一个感测的编码数据部分内编码的数；以及该至少一个感测的编码数据部分在该表面上的位置。

该方法优选包括，在计算机系统中，仅在核实失败后，将收到的核实请求与该至少一个判据进行比较。

该方法优选包括，在计算机系统中：接收核实请求，至少该请求的一部分表示：该对象的身份；并置的：签名单段，该签名单段是至少部分身份的数字签名；和随机签名；利用该核实请求，确定一被确定的身份；利用该并置，确定该签名单段；以及利用确定的身份和签名单段，核实该对象。

该方法优选包括，在计算机系统中：利用确定的身份，确定密钥；利用确定的身份和密钥，产生产生的签名；将产生的签名与该并置进行比较，从而识别和验证该签名单段。

根据另一个基本形式，本发明提供了一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，每个编码数据部分对下述进行编码：身份；签名单段，该签名是至少部分身份的数字签名；以及随机数；

根据另一个基本形式，本发明提供了一种布置在表面之上或者之内的编码数据，该编码数据包括许多编码数据部分，至少每个编码数据部分的一部分

表示：身份；至少部分签名，该签名是至少部分身份的数字签名；以及该编码数据在该表面上的位置。

至少每个编码数据部分的一部分优选指示数据部分身份，对于每个编码数据部分，该数据部分身份是唯一的，该数据部分身份表示该位置。

优选利用某种布局将该编码数据布置在该表面之上或者之内，对于每个数据部分身份，该布局表示相应编码数据部分的位置。

优选利用 RSA 加密，产生该签名。

附图说明

现在，将参考附图说明本发明的示例，附图中：

图 1 是包括超标记（Hyperlabel）编码的文档示例；

图 2 是用于与图 1 的超标记文档交互的系统示例；

图 3 是用于与图 1 的超标记文档交互的系统的又一个示例；

图 4 是标签结构的第一示例；

图 5 是图 4 的标签结构的符号单位单元的示例；

图 6 是图 5 的符号单位单元阵列的示例；

图 7 是图 5 的单位单元内排序的符号位的示例；

图 8 是每位均被设置的图 4 的标签结构的示例；

图 9 是图 4 的标签结构的标签组内的标签类型的示例；

图 10 是图 9 的标签组的连续铺盖的示例；

图 11 是图 4 的标签结构的交错码字示例；

图 12 是图 4 的标签结构的码字示例；

图 13 是分别利用其在活动区映射中的相应位索引标识的标签及其 8 个紧邻的示例；

图 14 是图 4 的标签结构的标签组内的标签类型的可选示例；

图 15 是图 14 的标签组的连续铺盖示例；

图 16 是图 14 的标签组的取向指示循环定位码字 R 的示例；

- 图 17 是图 14 的标签组的本机码字 A 的示例；
图 18 是图 14 的标签组的分布式码字 B、C、D 和 E 的示例；
图 19 是完整标签组的布局示例；
图 20 是图 14 的标签组的码字示例；
图 21 是标签结构的第二示例；
图 22 是图 21 的标签结构的符号单位单元的示例；
图 23 是图 22 的符号单位单元阵列的示例；
图 24 是图 22 的单位单元内排序的符号位的示例；
图 25 是每位被设置的图 21 的标签结构的示例；
图 26 是图 21 的标签结构的标签组内的标签类型的示例；
图 27 是图 26 的标签组的连续铺盖的示例；
图 28 是图 21 的标签结构的取向指示循环定位码字的示例；
图 29 是图 21 的标签结构的码字示例；
图 30 是图 21 的标签结构的分布式码字片段的示例；
图 31 是图 21 的标签组的连续铺盖的示例；
图 32 是图 21 的标签组的标签分段示例；
图 33 是图 21 的标签组的分段间间隔示例；
图 34 是图 21 的标签组的分段间间隔对目标位置的影响的示例；
图 35 是图 21 的标签组的码字示例；
图 36 是图 21 的标签组的标签坐标示例；
图 37 是分别利用其在活动区映射中的相应位索引标识的标签及其 6 个紧邻标签的示例；
图 38 是构成数据块的邻接组标签的示例；
图 39 是扩展标签结构的示例；
图 40 是图 39 的标签结构的码字示例；
图 41 是图 39 的标签结构的分布式码字片段示例；
图 42 是图 39 的标签结构的分布式码字片段的第二示例；

- 图 43 是项目签名对象模型的示例；
- 图 44 是零售机交互时的扫描示例；
- 图 45 是在线扫描交互细节的示例；
- 图 46 是脱机扫描交互细节的示例；
- 图 47 是 Netpage 笔扫描交互示例；
- 图 48 是 Netpage 笔扫描交互细节的示例；
- 图 49 是超标记标签分级图的示例；
- 图 50 是项目 ID 分级图的示例；
- 图 51 是注释 ID 分级图的示例；
- 图 52 是药品 ID 分级图的示例；
- 图 53 是对象描述、所有权和群集分级图的示例；
- 图 54 是对象扫描历史分级图的示例；
- 图 55 是扫描仪分级图的示例；
- 图 56 是对象 ID 热列表的示例；
- 图 57 是有效 ID 范围分级图的示例；
- 图 58 是公用密钥列表分级图的示例；
- 图 59 是可信验证符分级图的示例；
- 图 60 是标签和跟踪对象管理的示例。

具体实施方式

Netpage 面编码包括致密平面铺盖的标签。每个标签编码其自己在平面上的区位。每个标签还结合邻近标签编码含有该标签的区域的标识符。在 Netpage 系统中，区域通常对应于标签面的整个范围，例如，一张纸的一侧。

超标记是 Netpage 标签用于各种应用的唯一项目识别中的改进，它包括保密文档保护、对象跟踪、药品安全、超市自动化、交互式产品标签、从印刷面进行 web 浏览、基于纸的电子邮件等等。

采用 MemjetTM 数字印刷技术（它是包括 USSN 10/407,212 的许多美国

未决专利申请的主题), 利用红外 (IR) 油墨, 基本上在诸如保密文档、钞票或者药品包装的整个表面上印刷超标记标签。因此, 通过利用红外吸收油墨在红外反射近红外波的任意基片上印刷标签, 该标签对肉眼是不可见的, 但是利用具有适当滤色片的固态图像传感器可以轻而易举地感测到它。这使得机器可读信息可以在票据或者另一个表面的大部分上编码, 而不会对其上的原始票据文本或者图形产生可视影响。扫描激光器或者图像传感器可以读取该表面任意部分上的标签, 以执行相关动作, 例如, 验证每个单独票据或者项目。

图 1 示出这种超标记编码文档的示例。在该例中, 超标记文档包括: 利用可见油墨印刷的图形数据 2; 以及由超标记标签 4 构成的编码数据 3。该文档包括对应于相应图形 8 的空间范围的分区 7 确定的交互式单元 6。在使用中, 标签编码包括 ID 的标签数据。通过感测至少一个标签, 然后, 利用适当系统确定并解释编码的 ID, 这样可以执行相关动作。

在一个示例中, 根据在标签数据内编码的 ID, 利用标签映射确定超标记文档上的标签布局。该 ID 还可以用于查询文档描述, 该文档描述用于描述超标记文档的各单元, 而且尤其用于描述诸如按钮或者文本区的交互式单元的类型和空间范围(区)。因此, 在该例中, 单元 6 具有对应于相应图形 8 的空间范围的分区 7。这样可以使计算机系统解释与超标记文档的交互。

在位置指示技术中, 在每个标签的标签数据内编码的 ID 使得可以根据标签映射确定标签在超标记文档上的准确位置。然后, 根据文档描述, 可以利用该位置确定感测的标签是否位于交互式单元分区内。

在对象指示技术中, 在标签数据内编码的 ID 使得根据标签映射确定在该文档区域内存在标签(还可以指示标签在该区域内的相对位置)。在这种情况下, 可以利用文档描述确定该区域是否对应于交互式单元分区。

现在, 将参考图 2 和 3 说明该处理过程的示例, 图 2 和 3 示出 Netpage 或者 Netpage 笔 101 形式的感测装置如何与诸如保密文档、标签、产品包装等的印刷超标记文档 1 上的编码数据进行交互。

Netpage 笔 101 利用面图像传感器感测标签并检测标签数据。Netpage 笔 101 利用感测的数据标签产生交互数据，通过短距离无线电链路 9 将该交互数据发送到中继器 44，中继器 44 可以构成计算机 75 或者印刷机 601 的一部分。通过网络 19，该中继器将交互数据发送到文档服务器 10，该文档服务器 10 利用该 ID 访问文档描述并解释该交互。在适当环境下，文档服务器将相应消息发送到应用服务器 13，然后，该应用服务器 13 可以执行相应动作。

在可替换实施例中，PC、web 终端、Netpage 印刷机或者中继装置可以直接与包括本地或远程 Web 服务器的本地或者远程应用软件通信。相关地，并不局限于利用 Netpage 印刷机印刷输出。它还可以显示在 PC 或者 web 终端上，而且进一步交互可以是基于屏幕的，而非基于纸张的，或者可以是它们二者的混合。

通常 Netpage 笔用户登记到登记服务器 11，该登记服务器将该用户与存储在相应的 Netpage 笔中的标识符相关联。通过提供感测装置标识符作为交互数据的一部分，可以识别用户，从而允许执行交易等。

通过使 ID 服务器产生被传送到文档服务器 10 的 ID 来产生超标记文档。文档服务器 10 确定文档描述，然后，记录文档描述与 ID 之间的关联，以便之后利用该 ID 检索该文档描述。

然后在通过超标记印刷机 601 印刷该文档之前，该 ID 用于利用页面描述和标签映射来产生下面将详细描述的标签数据。

每个标签都由包含两种元素的图案来代表。第一类元素是目标。目标使得标签可以位于编码表面的图像中，还可以推断出该标签的透视失真。第二类元素是宏点（macrodot）。每个宏点都通过其是否存在编码位值。

图案以允许光学成像系统、特别是在近红外具有窄带响应的光学系统可以获取其的方式被表示在编码面上。通常使用窄带近红外油墨将该图案印刷在表面上。

在该超标记系统中，区域通常对应于整个产品项目的表面，或者对应于

保密文档，而区域 ID 对应于唯一项目 ID。为了清楚起见，在下面的说明中，我们称之为项目和项目 ID（或者简称 ID），要理解项目 ID 对应于区域 ID。

设计表面编码以使得大到足以保证能获取整个标签的获取视场大到能足以保证获取包含该标签的区域的 ID。获取该标签本身保证了获取该标签在该区域内的二维位置，以及其它该标签特有的数据。因此表面编码允许传感设备在仅仅与编码表面的局部交互作用的过程中(例如在用笔“点击”或敲打编码表面的过程中)获取区域 ID 和标签位置。

可以利用大量不同标签结构，现在，将说明一些示例。

标签结构的第一示例

图 4 示出完整标签的结构。四个黑色圆分别是目标。在物理层次，该标签和整个图案为四重旋转对称。

每个方形区域代表符号，每个符号代表 4 位信息。

图 5 示出符号的结构。其包含 4 个宏点，每个宏点通过其存在 (1) 还是不存在 (0) 表示 1 位的值。

贯穿本文档，宏点间隔由参数 s 规定。基于每英寸 1600 个点的间距印刷的 9 个点，该参数的额定值是 $143\mu\text{m}$ 。但是根据用于产生图案的设备的能力，允许有 $\pm 10\%$ 的变化。

图 6 示出 9 个相邻符号的阵列。在符号内和符号之间，宏点间隔均是均匀的。

图 7 示出符号内各位的顺序。位 0 是符号内的最低有效位；位 3 是最高有效位。要注意该顺序是相对于该符号的取向。特定符号在标签内的取向通过该符号的标记在标签图中的取向来指示。通常在标签的特定分段内的所有符号的取向都具有相同的取向，与最接近该标签中心的符号的底部一致。

只有宏点是该图案中的符号表示的一部分。符号的方形轮廓在本说明书中用于更为清楚地说明标签的结构。图 8 以图解的方式示出标签的实际图案，其中每个位都被设置。要注意在实际中可以始终不置位标签的各位。

宏点名义上是圆形的，具有 $(5/9)s$ 的额定直径。但是根据用于产生图案的设备的能力，允许其大小有 $\pm 10\%$ 的变化。

目标名义上是圆形的，具有 $(17/9)s$ 的额定直径。但是根据用于产生图案的设备的能力，允许其大小有 $\pm 10\%$ 的变化。

根据用于产生图案的设备的能力，允许标签图案的尺度变化 $\pm 10\%$ 。与额定尺度之间的任何不同都记录在标签数据中以允许准确产生位置采样。

图 4 的标签结构中示出的每个符号都具有唯一的标记。每个标记都由字母前缀和数字后缀组成。

标签组

将标签排列为标签组。每个标签组包括以方形排列的四个标签。因此，根据其在方形标签组内的区位，每个标签具有四种可能的标签类型之一。标签类型被标记为 00、10、01 和 11，如图 9 所示。

图 10 示出标签组是如何以标签连续铺盖的方式重复的。铺盖确保任意一组四个相邻标签包括每种类型的一个标签。

码字

标签含有四个完整码字。每个码字分别是穿孔的 2^4 -ary(8,5)里德-索罗门码。

两个码字对于该标签是唯一的。将它们称为局部码字并且标记为 A 和 B。因此，该标签至多编码 40 位对该标签唯一的信息。

剩余的两个码字是对标签类型唯一的，但是对于邻接铺盖标签内的所有相同类型的标签是共同的。这两个码字被称为全局码字并且被标记为 C 和 D，利用标签类型标示它们。因此，标签组编码至多 160 位对紧接铺盖标签内的所有标签组共同的信息。

图 11 示出四个码字的布局。

里德-索罗门码

利用穿孔的 2^4 -ary(8,5)里德-索罗门码编码各码字。

2^4 -ary(8,5)里德-索罗门码编码每个码字中的 20 个数据位（即，5 个四位符号）和 12 个冗余位（即，3 个四位符号）。其检错容量是 3 个符号。其纠错容量是一个符号。

如图 12 所示，以系数顺序索引码字坐标，而且数据位顺序遵循码字位顺序。

穿孔的 2^4 -ary(8,5)里德-索罗门码是去除了 7 个冗余坐标的 2^4 -ary(15,5)里德-索罗门码。去除的坐标是最高有效冗余坐标。

该代码具有下面的原始多项式：

$$P(x)=x^4+x+1$$

该代码具有下面的生成多项式：

$$g(x)=(x+\alpha)(x+\alpha^2)\dots(x+\alpha^{10})$$

关于里德-索罗门码的详细说明，请参考 Wicker, S.B. 和 V.K. Bhargava, eds., Reed-Solomon Codes and Their Applications, IEEE Press, 1994。

标签坐标空间

标签坐标空间具有两个分别被标记为 x 和 y 的正交轴。如果正 x 轴指向右时，则正 y 轴指向下。

表面编码不规定在特定标签表面上的标签坐标空间原点的区位，也不规定该标签坐标空间相对于该表面的取向。该信息是特定于应用的。例如，如果加标签的表面是一张纸，则将标签印刷在该纸上的应用可以记录实际的偏移和取向，这些可用于对随后结合该表面获取的任何数字油墨进行标准化。

被编码在标签内的位置以标签为单位来定义。通常该位置是最靠近原点的目标中心的位置。

标签信息内容

表 1 定义了嵌入表面编码的信息字段。表 2 定义了这些字段如何映射到码字。

表 1. 字段定义

字段	宽度	描述
每个码字		
码字类型	2	码字类型即 A(b'00')、B(b'01')、C(b'10')和 D(b'11')之一。
每个标签		
标签类型	2	标签类型，即 00(b'00')、01(b'01')、10(b'10')和 11(b'11')之一，对应于标签的 x 坐标和 y 坐标的后 2 位。
X 坐标	13	标签的不带符号 x 坐标允许具有约 14 m 的最大坐标值。
y 坐标	13	标签 ^b 的不带符号坐标
有效区标志	1	表示该标签是否是有效区的成员的标志。b'1'表示成员资格。
有效区映射标志	1	表示是否存在有效区映射的标志。b'1'表示存在映射（参考下一个字段）。如果不存在映射，则根据有效区标志，求得每个映射项的值（参考前面的字段）。
有效区映射	8	该标签的 8 个紧邻标签是有效区的成员的映射 ¹ 。b'1'表示成员资格（图 13 示出该映射的位顺序。）
数据片段	8	嵌入数据流内的片段。仅在不存在

		有效区映射时存在。
每个标签组		
编码格式	8	编码格式。 0: 当前编码 其它值是 TBA。
区域标志	8	用于对解释和路由选择区域相关信息进行控制的标志。 0: 区域 ID 是 EPD 1: 区域被链接 2: 区域是交互式的 3: 区域是带符号的 4: 区域包括数据 5: 区域涉及移动应用 其它位被保留, 而且必须是 0。
标签大小调整	16	在 10nm 单元内, 以带符号大小 (sign-magnitude) 格式, 实际标签大小与正常标签大小之间的差 (1.7145 mm (基于 1600 dpi, 每个宏点 9 点, 而每个标签 12 的宏点))。
区域 ID	96	含有该标签的区域的 ID
CRC	16	标签组数据的 CRC (CCITT CRC-16 (ITU, 数据终端装置 (DTE) 与用于以分组方式工作且通过专用电路 ITU-TX.25(10/96) 连接到公众数据网的的终端的数据电路终止装置 (DCE) 之间的接

		口))
合计	320	

有效区映射表示相应标签是否是有效区的成员。有效区是在其内立即将捕获的任意输入转发到相应超标记服务器以进行解释的区域。还允许超标记感测装置将该输入具有直接作用通知该用户。

表 2. 字段到码字的映射

码字	码字位	字段	宽度	字段位
A	1:0	码字类型 (b'00')	2	全部
	10:2	x 坐标	9	12:4
	19:11	y 坐标	9	12:4
B	1:0	码字类型 (b'01')	2	全部
	2	标签类型	1	0
	5:2	x 坐标	4	3:0
	6	标签类型	1	1
	9:6	y 坐标	4	3:0
	10	有效区标志	1	全部
	11	有效区映射标志	1	全部
C ₀₀	19:12	有效区映射	8	全部
	19:12	数据片段	8	全部
	1:0	码字类型 (b'10')	2	全部
	9:2	编码格式	8	全部
C ₀₁	17:10	区域标志	8	全部
	19:18	标签大小调整	2	1:0
	1:0	码字类型 (b'10')	2	全部

	15:2	标签大小调整	14	15:2
	19:16	区域 ID	4	3:0
C ₁₀	1:0	码字类型 (b'10')	2	全部
	19:2	区域 ID	18	21:4
C ₁₁	1:0	码字类型 (b'10')	2	全部
	19:2	区域 ID	18	39:22
D ₀₀	1:0	码字类型 (b'11')	2	全部
	19:2	区域 ID	18	57:40
D ₀₁	1:0	码字类型 (b'11')	2	全部
	19:2	区域 ID	18	75:58
D ₁₀	1:0	码字类型 (b'11')	2	全部
	19:2	区域 ID	18	93:76
D ₁₁	1:0	码字类型 (b'11')	2	全部
	3:2	区域 ID	2	95:94
	19:4	CRC	16	全部

请注意，可以将标签类型移入全局码字，以最大化局部码字的利用。这样又可以允许更大的坐标和/或 16 位数据片段（通常可以结合坐标精度潜在地配置）。然而，这样降低了解码位置与解码的区域 ID 的无关性，因此不包括在这次的技术规范中。

嵌入数据

如果设置了区域标志中的“区域包括数据”标志则表面编码包含嵌入数据。该数据编码为多个相邻的标签的数据片段，并在表面编码中复制尽可能多的其达到适合的次数。

该嵌入数据以随机和部分扫描包含该嵌入数据的表面编码就足以检索出整个数据的方式编码。扫描系统将来自检索出的片段的数据重新整合，并在没

有错误地检索出足够多片段之后向用户报告。

如表 3 所示, 200 位数据块编码 160 位数据。该块数据编码在排列为 5×5 正方形的 25 个相邻标签的一个组的数据片段中。每个标签属于其整数坐标等于该标签坐标除以 5 的块。在每个块内数据都排列为 x 坐标随着 y 坐标增长而增长的标签。

在存在有效区映射的块中可能缺少数据片段。但是所缺少的数据片段有可能从该块的其它副本中恢复。

将任意大小的数据编码为由排列为矩形的相邻块的集合组成的超级块。将该超级块的大小编码在每个块中。每个块属于整数坐标等于该块的坐标除以超级块大小的超级块。数据在每个超级块内排列为 x 坐标随着 y 坐标的增长而增长的块。

以表面编码将超级块重复尽可能多的其达到适合的次数，包括沿着该表面编码的边缘进行部分重复。

在超级块内编码的数据可以包括更精确的类型信息，更精确的大小信息以及更大的检错数据和/或者纠错数据。

表 3: 嵌入数据块

字段	宽度	描述
数据类型	8	超级块内的数据类型。 值包括： 0: 区域标志控制类型 1: MIME 其它值是 TBA
超级块宽度	8	以块为单位的超级块的宽度
超级块高度	8	以块为单位的超级块的高度
数据	160	块数据
CRC	16	块数据的 CRC

合计	200
----	-----

标签结构的第一变换示例

标签组

标签被布置为标签组。每个标签组包含布置为方形的 4 个标签。因此每个标签根据其在该标签方形组中的位置而具有 4 个可能的标签类型之一。标签类型被标记为 00、10、01 和 11，如图 14 所示。

标签组中的每个标签如图所示旋转，即标签类型 00 旋转 0 度，标签类型 10 旋转 90 度，标签类型 11 旋转 180 度，而标签类型 01 旋转 270 度。

图 15 示出标签组以邻接的标签铺盖而重复。该铺盖保证任何一组 4 个相邻标签都包含每个类型的一个标签。

取向指示循环位置代码

标签包含 2^4 -ary (4, 1) 循环位置码字，其可以在该标签的 4 个可能取向的任何一个取向上被解码，以确定该标签的实际取向。作为该循环位置码字的一部分的符号具有前缀“R”并且以重要性逐渐增加的顺序被编号为 0 到 3。

该循环位置码字是 (0, 7, 9, E₁₆)。要注意只使用了 4 个不同的符号值，尽管 4 位符号具有 16 个可能值。在解码期间，如果检测到任何未用到的符号值的话，都应当当作擦除。为了将由低权重位错误图案导致擦除而不是符号错误的概率最大化，将符号值选择为尽量在超立方体上平均间隔开。

循环位置码的最小距离是 4，因此其纠错能力在多至一个擦除的情况下是一个符号，在存在两个或更多个擦除的情况下是 0 个符号。

图 16 示出取向指示循环位置码字的布局。

局部码字

标签在局部包含一个完整的码字，该码字用于编码该标签独有的信息。

该码字是穿孔的 2^4 -ary (13, 7) 里德-索罗门码。因此该标签编码了该标签独有的至多 28 位信息。

图 17 示出局部码字的布局。

分布式码字

标签还包含 4 个码字的片段，它们分布在标签组中的 4 个相邻标签上，并用于编码一组相邻标签所共用的信息。每个码字是 2^4 -ary (15,11) 里德-索罗门码。因此任何 4 个相邻标签一起编码一组相邻标签所共用的至多 176 位信息。

图 18 示出分布在标签组中 4 个相邻标签上的 4 个完整的码字的布局。

图 18 中该标签组中的 4 个标签的顺序就是图 14 的 4 个标签的顺序。

图 19 示出完整标签组的布局。

里德-索罗门编码—局部码字

局部码字是利用穿孔的 2^4 -ary (13,7) 里德-索罗门码编码而成的。该码在每个码字中编码 28 个数据位(即 7 个符号)和 24 个冗余位(即 6 个符号)。其检错能力是 6 个符号。其纠错能力是 3 个符号。

如图 20 所示，按照系数顺序给码字坐标编出索引，并且数据位顺序遵循码字位顺序。

该代码是去掉了两个冗余坐标的 2^4 -ary (15,7) 里德-索罗门码。所去掉的坐标是最高有效冗余坐标。

该代码具有下面的本原多项式：

$$P(x)=x^4+x+1 \quad (\text{EQ1})$$

该代码具有下面的生成多项式：

$$g(x)=(x+\alpha)(x+\alpha^2)\dots(x+\alpha^8) \quad (\text{EQ2})$$

里德-索罗门编码—分布式码字

分布式码字是利用 2^4 -ary (15,11) 里德-索罗门码编码而成的。该代码在每个码字中编码 44 个数据位（即 11 个符号）和 16 个冗余位（即 4 个符号）。其检错能力是 4 个符号。其纠错能力是 2 个符号。

按照系数顺序给码字坐标编出索引，并且数据位顺序遵循码字位顺序。

该代码具有与局部码字代码相同的本原多项式：

该代码具有下面的生成多项式：

$$g(x)=(x+\alpha)(x+\alpha^2)\dots(x+\alpha^4) \quad (\text{EQ3})$$

标签坐标空间

该标签坐标空间具有两个分别被标记为 x 和 y 的正交轴。如果正 x 轴指向右，则正 y 轴指向下。

表面编码不规定在特定标签表面上的标签坐标空间原点的区位，也不规定该标签坐标空间相对于表面的取向。该信息是特定于应用的。例如，如果加标签的表面是一张纸，则将标签印刷在该纸上的应用可以记录实际的偏移和取向，这些可用于对随后结合该表面获取的任何数字油墨进行标准化。

被编码在标签内的位置以标签为单位来定义。通常该位置是最靠近原点的目标中心的位置。

标签信息内容

字段定义

表 4 定义了嵌入表面编码中的信息字段。表 5 定义了这些字段如何映射到码字。

表 4. 字段定义

字段	宽度 (位)	描述
----	--------	----

每个标签		
x 坐标	9 或者 13	标签的不带符号 x 坐标允许分别具有约 0.9 m 和 14 m 的最大坐标值。
y 坐标	9 或者 13	标签的不带符号 y 坐标允许分别具有约 0.9 m 和 14 m 的最大坐标值。
有效区标志	1	表示紧紧包围该标签的区域(以标签为中心的区域直径正常是该标签的对角线大小的 5 倍)是否与有效区交叉的标志。 b'1' 表示交叉。
数据片段标志	1	表示是否存在数据片段的标志(请参考下面的字段)。 b'1' 表示存在数据片段。 如果存在数据片段, 则 x 和 y 坐标字段的宽度是 9。如果不存在, 则该宽度是 13。
数据片段	0 或者 8	嵌入数据流的片段。
每个标签组 (即, 每个区域)		
编码格式	8	编码格式。 0: 当前编码 保留其它值。
区域标志	8	控制区域数据的解释的标志。 0: 区域 ID 是 EPC 1: 区域具有签名

		2: 区域具有嵌入数据 3: 嵌入数据是签名 其它位被保留，而且必须是 0。
标签大小 ID	8	标签大小的 ID 0: 基于 1600dpi, 每个宏点 9 个点， 每个标签 12 个宏点，当前标签大 小，额定标签大小是 1.7145mm， 保留其它值
区域 ID	96	含有标签的区域的 ID
签名	36	区域的签名
高序坐标宽度 (w)	4	标签的 x 和 y 坐标的高序部分的宽 度
高序 x 坐标	0 至 15	标签的 x 坐标的高序部分使最大 坐标值分别扩展到约 2.4 km 和 38 km。
高序 y 坐标	0 至 15	该标签的 y 坐标的高序部分使最 大坐标值分别扩展到约 2.4 km 和 38 km。
CRC	16	标签组数据的 CRC

有效区是在其内立即将捕获的任意输入转发到相应超标记服务器以进
行解释的区域。这还允许超标记服务器将该输入具有直接作用通知该用户。
由于该服务器可以访问精确的区域定义，因此表面编码内的任何有效区指示
只要是有界限的就可能是不准确的。

高序坐标字段的宽度如果是非零则将签名字段的宽度减小相应的位数。
完整的坐标是通过将每个高序坐标字段添加到其对应的坐标字段之前来计
算。

表 5.字段到码字的映射

码字	码字位	字段	宽度	字段位
A	12:0	x 坐标	13	全部
	12:9	数据片段	4	3:0
	25:13	y 坐标	13	全部
	25:22	数据片段	4	7:4
	26	有效区标志	1	全部
	27	数据片段标志	1	全部
B	7:0	编码格式	8	全部
	15:8	区域标志	8	全部
	23:16	标签大小 ID	8	全部
	39:24	CRC	16	全部
	43:40	高序坐标宽度 (w)	4	3:0
C	35:0	签名	36	全部
	(35-w):(36-2w)	高序 x 坐标	w	全部
	35:(36-w)	高序 y 坐标	w	全部
	43:36	区域 ID	8	7:0
D	43:0	区域 ID	44	51:8
E	43:0	区域 ID	44	95:52

嵌入数据

如果设置了区域标志中的“区域具有嵌入数据”标志，则表面编码包含嵌入数据。该数据编码为多个相邻的标签的数据片段，并在表面编码中复制尽可能多的其达到适合的次数。

该嵌入数据以随机和部分扫描包含该嵌入数据的表面编码就足以检索出整个数据的方式编码。扫描系统将来自检索出的片段的数据重新整合，并

在没有错误地检索出足够多片段之后向用户报告。

如表 6 所示, 200 位数据块编码 160 位数据。该块数据编码在排列为 5×5 正方形的 25 个相邻标签的一个组的数据片段中。各个标签属于整数坐标等于该标签坐标除以 5 的块。在每个块内数据都排列为 x 坐标随着 y 坐标增长而增长的标签。

在存在有效区映射的块中可能缺少数据片段。但是所缺少的数据片段有可能从该块的其它副本中恢复。

将任意大小的数据编码为由排列为矩形的相邻块的集合组成的超级块。将该超级块的大小编码在每个块中。每个块属于其整数坐标等于该块的坐标除以超级块大小的超级块。数据在每个超级块内排列为 x 坐标随着 y 坐标的增长而增长的块。

以表面编码将超级块重复尽可能多的其达到适合的次数，包括沿着该表面编码的边缘进行部分重复。

编码在超级块中的数据可能包括更为精确的类型信息、更为精确的大小信息和更大量的检错和/或纠错数据。

表 6: 嵌入数据块

字段	宽度	描述
数据类型	8	超级块内的数据类型。 值包括： 0: 区域标志控制的类型 1: MIME 其它值是 TBA
超级块宽度	8	以块为单位的超级块的宽度
超级块高度	8	以块为单位的超级块的高度
数据	160	块数据
CRC	16	块数据的 CRC

合计	200
----	-----

应当理解，可以采用任意形式的嵌入数据，例如，包括：诸如产品信息、应用数据、联系数据、业务名片数据以及目录数据的文本、图像。声频、视频数据。

区域签名

如果设置了区域标志中的“区域具有签名”标志，则该签名字段包含最大宽度为 36 位的签名。该签名通常是与安全数据库中的区域 ID 相关联的随机数。理想情况下利用真实的随机过程如量子过程来产生该签名，或通过从随机事件中提取随机性来产生。

在在线环境下可以结合区域 ID 通过查询可访问安全数据库的服务器来验证签名。

如果设置了区域标志中的“区域具有嵌入数据”标志和“嵌入数据是签名”标志，则表面编码包含区域 ID 的 160 位密码签名。该签名编码在一个块的超级块中。

在在线环境下可以结合区域 ID 并且可选择地结合随机签名，用任意数量的签名字段通过查询知道全部签名或对应的专用密钥的服务器来验证该签名。

在脱机（或在线）环境下，可以通过读取多个标签恢复整个签名，然后可以利用对应的公用签名密钥来验证该签名。

下面详细说明签名核实过程。

标签结构的第二示例

图 21 示出完整标签的结构。6 个黑色圆分别是目标。在物理层次，标签和整个图案为六重旋转对称。

每个菱形区分别表示符号，而每个符号分别表示四位信息。

图 22 示出符号的结构。它含有四个宏点，每个宏点分别利用其存在 (1) 或者不存在 (0) 表示 1 位的值。

贯穿本文档，宏点间隔由参数 s 指定。基于每英寸 1600 个点的间距印刷的 9 个点，该参数的额定值是 $143\mu\text{m}$ 。但是根据用于产生图案的设备的能力，允许有 $\pm 10\%$ 的变化。

图 23 示出 5 个相邻符号的阵列。在符号内和符号之间，宏点间隔均是均匀的。

图 24 示出符号内各位的顺序。位 0 是符号内的最低有效位；位 3 是最高有效位。请注意，该顺序是相对于符号的取向的。标签图中符号标记的取向表示标签内特定符号的取向。通常，该标签的特定分段内的所有符号的取向具有与最靠近该标签中心的符号底部一致的相同取向。

只有宏点是该图案中的符号表示的一部分。符号的菱形轮廓在本说明书中用于更为清楚地说明标签的结构。图 25 以图解的方式示出标签的实际图案，其中每个位都被设置。要注意在实际中可以始终不置位标签的各位。

宏点名义上是圆形的，具有 $(5/9)s$ 的额定直径。但是根据用于产生图案的设备的能力，允许其大小有 $\pm 10\%$ 的变化。

目标名义上是圆形的，具有 $(17/9)s$ 的额定直径。但是根据用于产生图案的设备的能力，允许其大小有 $\pm 10\%$ 的变化。

根据用于产生图案的设备的能力，允许标签图案的尺度变化 $\pm 10\%$ 。与额定尺度之间的任何不同都记录在标签数据中以允许准确产生位置采样。

图 21 的标签结构中示出的每个符号都具有唯一的标记。每个标记都由字母前缀和数字后缀组成。

标签组

将标签排列为标签组。每个标签组分别包括以直线排列的三个标签。因此，根据其在标签组内的区位，每个标签具有三种可能的标签类型之一。标

签类型被标记为 P、Q、和 R，如图 26 所示。

图 27 示出标签组是如何以标签连续铺盖的方式重复的。铺盖确保任意一组三个相邻标签包括每种类型的一个标签。

取向指示循环位置代码

标签含有 2^4 -ary(6,1)循环位置码字（当前，该工作是标题分别为“Cyclic position codes” 和 “Orientation indicating cyclic position codes”、申请号为 10/120,441 和 10/409,864 的两个美国未决专利申请的主题），可以在标签的 6 个可能取向之任一解码该 2^4 -ary(6,1)循环位置码字，以确定标签的实际取向。作为循环位置码字的一部分的符号具有前缀“R”，而且以有效位增大的顺序，将它们编号为 0 至 5。

取向指示循环位置码字的布局示于图 28 中。

循环位置码字是 $(0,5,6,9,A_{16},F_{16})$ 。请注意，它仅使用 6 个相异符号值，即使四位符号具有 16 个可能值。在解码期间，如果检测到任何未使用的符号值，则应当将其处理为擦除。为了将由低权重位错误图案导致擦除而不是符号错误的概率最大化，将符号值选择为尽量在超立方体上平均间隔开。

循环位置代码的最小距离是 6，因此其纠错能力在多至一个擦除的情况下是二个符号，在存在两个或三多个擦除的情况下是一个符号，在存在四个或更多个擦除的情况下是 0 个符号。

局部码字

该标签在局部含有一个完整码字，标记为 A，该完整码字用于编码对该标签唯一的信息。码字是穿孔 2^4 -ary(12,7)里德-索罗门码。因此，该标签编码对该标签唯一的至多 28 位信息。

图 29 示出局部码字的布局。

分布式码字

标签还含有分别被标记为 B 至 G 的 6 个码字的片段，它们分布在 3 个相邻标签上，并且被用于编码一组连续标签共用的信息。每个码字是穿孔 2^4 -ary(12,7) 里德-索罗门码。因此，任意 3 个相邻标签一起编码一组邻接标签共用的至多 168 位信息。

图 30 示出标签类型 P 中的 6 个码字 B 至 G 的头 4 个片段的布局。其它标签类型中的布局遵循标签类型 P 中的布局，其中标签类型 Q 中具有符号 4 至 7，标签类型 R 中具有片段 8 至 11。

图 31 示出分布在 3 种标签类型 P、Q 和 R 上的 6 个完整码字 B 至 G 的布局。

如图 27 所示，铺盖确保任意一组三个相邻标签包括每种类型的一个标签，并因此含有完整一组分布式码字。根据在每个标签的局部码字内编码的 x-y 坐标，可以推断用于确定对特定一组相邻标签记录分布式码字的标签类型。

标签分段几何形状

图 32 示出标签分段的几何形状。

图 33 示出为了在宏点之间保持一致间隔要求的标签分段之间的间隔 d，其中下式给出 d：

$$d = (1 - \sqrt{3}/2)s$$

图 34 示出目标位置上的分段间间隔 d 的效果。与其和密堆分段(closely-packed segment)相关的正常位置(即，d=0)相比，必须使对角目标移位如下：

$$(\Delta_x, \Delta_y) = (\pm 1/\sqrt{3}, \pm 1)d$$

而必须使水平目标移位如下：

$$(\Delta_x, \Delta_y) = (\pm 2/\sqrt{3}, 0)d$$

里德-索罗门编码

利用穿孔 2^4 -ary(12,7)里德-索罗门码编码码字。

2^4 -ary(12,7) 里德-索罗门码编码每个码字内的 28 个数据位（即，7 个四位符号）和 20 个冗余位（即，5 个四位符号）。其检错容量是 5 个符号。其纠错容量是 2 个符号。

如图 35 所示，按照系数顺序给码字坐标编出索引，并且数据位顺序遵循码字位顺序。

穿孔 2^4 -ary(12,7)里德-索罗门码是去除了 3 个冗余坐标的 2^4 -ary(15,7) 里德-索罗门码。去除的坐标是最高有效冗余坐标。

代码具有下面的本原多项式：

$$P(x)=x^4+x+1$$

代码具有下面的生成多项式：

$$g(x)=(x+\alpha)(x+\alpha^2)\dots(x+\alpha^8)$$

关于里德-索罗门码的详细说明，请参考 Wicker, S.B. 和 V.K. Bhargava, eds., Reed-Solomon Codes and Their Applications, IEEE Press, 1994。

标签坐标空间

标签坐标空间具有两个分别被标记为 x 和 y 的正交轴。如果正 x 轴指向右，则正 y 轴指向下。

表面编码不规定在特定标签表面上的标签坐标空间原点的区位，也不规

定该标签坐标空间相对于表面的取向。该信息是特定于应用的。例如，如果加标签的表面是一张纸，则将标签印刷在该纸上的应用可以记录实际的偏移和取向，这些可用于对随后结合该表面获取的任何数字油墨进行标准化。

以标签为单位来定义在标签内编码的位置。如图 36 所示来排列各标签坐标，其中坐标为 (0, 0) 的标签是 P 型标签。按照惯例，定义具有偶数坐标的标签位置是该标签的中心位置。因此，定义具有奇数坐标的标签位置是该标签的中心与其左侧相邻标签的中心之间的中点的位置。

根据中心到中心标签的标签间隔，如下给出水平标签单元和垂直标签单元：

$$u_x = 4(2\sqrt{3}s) + 2d \approx 14.1s$$

$$u_y = 6(2s) + 2\left(d\frac{\sqrt{3}}{2}\right) \approx 12.2s$$

其中 d 是如下给出的分段间间隔

$$d = (1 - \sqrt{3}/2)s$$

如果 3 种标签类型 P、Q 和 R 被分别指定值 0、1 和 2，则根据其 (x,y) 坐标，如下推算标签类型 t。如果 y 是偶数，则：

$$t=x \bmod 3$$

如果 y 是奇数，则

$$t=(x-1) \bmod 3$$

标签信息内容

表 7 定义了嵌入表面编码的信息字段。表 8 定义了这些字段如何映射到码字。

表 7. 字段定义

字段	宽度(位)	描述
每个标签		
x 坐标	10	标签的不带符号 x 坐标允许约 2.1 m (根据 EQ4) 的最大 x 坐标值。
Y 坐标	10	标签的不带符号 y 坐标允许约 1.8 m (根据 EQ5) 的最大 y 坐标值。
有效区标志	1	表示该标签是否是有效区的成员的标志。b'1' 表示成员资格。
有效区映射标志	1	表示是否存在有效区映射的标志。b'1' 表示存在映射 (参考下一个字段)。如果不存在映射，则根据该有效区标志 (参考前面的字段)，求得每个映射项目的值。
有效区映射	6	该标签的 6 个紧邻标签是有效区的成员的映射。b'1' 表示成员资格 — 图 37 示出映射的位顺序。
数据片段	6	嵌入数据流内的片段。仅在不存在有效区映射时，存在。
每个标签组		
编码格式	12	编码格式。 0：当前编码 其它值是 TBA。

宏点间隔调整	16	在带符号大小格式中,以 nm 为单位的、实际宏点间隔与正常宏点间隔之间的差, 正常宏点间隔是 142875 nm (根据 1600 dpi 和每个宏点 9 个点)
区域标志	12	用于对解释和路由选择区域相关信息进行控制的标志。 0: 区域 ID 是 EPC 1: 区域被链接 2: 区域是交互式的 3: 区域是带符号的 4: 区域包括数据 5: 区域涉及移动应用 其它位被保留, 而且必须是 0。
区域 ID	112	含有该标签的区域的 ID
CRC	16	标签组数据的 CRC (CCITT CRC-16)

有效区映射表示相应标签是否是有效区的成员。有效区是在其内立即将捕获的任意输入转发到相应超标记服务器以进行解释的区域。这还允许超标记感测设备将该输入具有直接作用通知该用户。

表 8. 字段到码字的映射

码字	码字位	字段宽度	字段位	字段
A	9:0	10	全部	x 坐标
	19:10	10	全部	y 坐标
	20	1	全部	有效区标志

	21	1	全部	有效区映射标志
	27:22	6	全部	有效区映射
	27:22	6	全部	数据片段
B	11:0	12	全部	编码格式
	27:12	16	全部	宏点间隔调整
C	11:0	12	全部	区域标志
	27:12	16	27:12	区域 ID
D	27:0	28	55:28	
E	27:0	28	83:56	
F	27:0	28	111:84	
G	11:0	12	11:0	
	27:12	16	全部	CRC

嵌入数据

如果设置了区域标志中的“区域包括数据”标志，则表面编码包含嵌入数据。该数据编码为多个相邻的标签的数据片段，并在表面编码中复制尽可能多的其达到适合的次数。

该嵌入数据以随机和部分扫描包含该嵌入数据的表面编码就足以检索出整个数据的方式编码。扫描系统将来自检索出的片段的数据重新整合，并在没有错误地检索出足够多片段之后向用户报告。

如表 9 所示，216 位数据块编码 160 位的数据。

表 9: 嵌入数据块

字段	宽度	描述
数据类型	16	超级块内的数据类型。值包括： 0: 区域标志控制的类型 1: MIME

		其它值是 TBA
超级块宽度	12	以块为单位的超级块的宽度
超级块高度	12	以块为单位的超级块的高度
数据	160	块数据
CRC	16	块数据的 CRC
合计	216	

如图 38 所示, 该块数据编码在排列为 6×6 方形的 36 个相邻标签的一个组的数据片段中。各个标签属于整数 x 和 y 坐标等于该标签的 x 和 y 坐标除以 6 的块。在每个块内数据都排列为 x 坐标随着 y 坐标增长而增长的标签。

在存在有效区映射的块中可能缺少数据片段。但是所缺少的数据片段有可能从该块的其它副本中恢复。

将任意大小的数据编码为由排列为矩形的相邻块的集合组成的超级块。将该超级块的大小编码在每个块中。每个块属于其整数坐标等于该块的坐标除以超级块大小的超级块。数据 R 在每个超级块内排列为 x 坐标随着 y 坐标的增长而增长的块。

以表面编码将超级块重复尽可能多的其达到适合的次数, 包括沿着该表面编码的边缘进行部分重复。

编码在超级块中的数据可能包括更为精确的类型信息、更为精确的大小信息和更大量的检错和/或纠错数据。

一般需要考虑的事项

区域 ID 的密码签名

如果置位区域标志内的“区域带符号”标志, 则该表面编码含有该区域 ID 的 160 位密码签名。在一块超级块内编码该签名。

在线环境下, 可以结合区域 ID 使用任意签名片段来验证该签名。在脱机环境下, 通过读取多个标签来恢复整个签名, 然后利用相应公用签名密

钥对其进行验证。

MIME 数据

如果嵌入数据类型是“MIME”则超级块包含按照 RFC 2045 (Freed, N., 和 N.Borenstein, “Multipurpose Internet Mail Extensions(MIME)-Part One: Format of Internet Message Bodies”, RFC 2045, 1996 年 11 月), RFC 2046 (Freed , N. , 和 N.Borenstein , “ Multipurpose Internet Mail Extensions(MIME)-Part Two: Media Types”, RFC 2046, 1996 年 11 月) 和有关 RFC 的多目的互联网邮件扩展 (MIME) 数据。MIME 数据由头部和后面的正文组成。头部被编码为可变长度的文本字符串, 前面加上 8 位的字符串。正文被编码为可变长度的特定于类型的八位位组流, 前面加上大端 (big-endian) 格式的 16 位大小。

RFC 2046 中描述的基本高级媒体类型包括文本、图像、声音、视频和应用程序。

RFC 2425 (Howes, T., M.Smith 和 F.Dawson, “A MIME Content-Type for Directory Information”, RFC 2045, 1998 年 9 月) 和 RFC 2426 (Dawson, F., 和 T.Howes, “vCard MIME Directory Profile”, RFC 2046, 1998 年 9 月) 描述了一种用于通讯录信息的文本子类型, 其适用于例如对可能出现在名片上的联系信息进行编码。

编码和印刷需要考虑的事项

印刷引擎控制器 (PEC) (这是包括 09/575108; 10/727162; 09/575110; 09/607985; 6,398,332; 6,394,573; 6,622,923 在内的多个未决美国专利申请的主题) 支持用 (每页) 两个固定的 2^4 元 (15,7) 里德-索罗门码字和 (每标签) 4 个可变的 2^4 -ary (15,7) 里德-索罗门码字编码, 尽管对于不同的方案可以采用其它数量的码字。

此外，PEC 支持通过矩形单位单元（unit cell）来对标签润色，所述单位单元（每页）布局恒定但不同单位单元之间的变化码字数据可以不同。PEC 不允许单位单元在页面移动的方向重叠。

与 PEC 兼容的单位单元包含由 4 个标签组成的一个标签组。该标签组包含该标签组独有的但在该标签组内重复了 4 次的一个 A 码字和 4 个唯一的 B 码字。可以用 PEC 的 6 个被支持可变码字中的 5 个来对它们编码。该标签组还包含 8 个固定的 C、D 码字。其中一个可以用剩下的那一个 PEC 可变码字来编码，另外两个可以用 PEC 的两个固定码字编码，剩下的 5 个可以被编码并被预润色为提供给 PEC 的标签格式结构（TFS）。

PEC 施加了每个 TFS 行 32 个唯一地址的限制。单位单元的内容遵循这一限制。PEC 还施加了 TFS 的宽度为 384 的限制。单位单元的内容也遵循这一限制。

要注意对于合理的页面尺寸来说，A 码字中的可变坐标位的个数是适度的，使得通过查找表进行编码是易于操作的。还可能通过查找表对 B 码字进行编码。要注意由于里德-索罗门码字是系统性的，因此只有冗余数据才需要出现在查找表中。

成像和解码要考虑的事项

考虑到表面编码和视场之间的任意对准，保证获取整个标签所需要的最小成像视场具有 39.6s 的直径，即

$$(2 \times (12 + 2))\sqrt{2}s$$

假定宏点间隔为 $143\mu\text{m}$ ，该公式给出了所需要 5.7mm 的视场。

表 10 给出当前表面编码针对不同采样率可达到的间距范围，假定图像传感器的大小是 128 个像素。

表 10

当前表面编码针对不同采样率可达到的间距范围，采用优化超标记光学系统计算；点间距=1600dpi，宏点间距=9 个点，视距=30mm，尖头（nib）与视场间

隔=1mm, 图像传感器大小=128 个像素

采样率	间距范围
2	-40 到+49
2.5	-27 到+36
3	-10 到+18

对于第一示例的表面编码，对应的解码顺序如下：

- 定位完整标签的目标
- 根据目标，推断透视变换
- 采样并解码标签的 4 个码字之一
- 确定码字类型，并因此确定标签取向
- 采样并解码要求的局部（A 和 B）码字
- 码字冗余仅 12 位，因此，仅检测错误
- 在检错标志上具有不良位置采样
- 参照标签取向，确定标签的 x-y 地址
- 参照取向目标，推断 3D 标签变换
- 根据标签的 x-y 区位和 3D 变换，确定尖端 x-y 区位
- 参照有效区映射，确定尖端区位的有效区状态
- 根据尖端有效区状态，产生局部反馈
- 根据 A 码字，确定标签类型
- 采样并解码所需的全局（C 和 D）码字（参照标签类型，采用模窗对准（modulo window alignment））
 - 尽管码字冗余仅 12 位，但是纠错；后续 CRC 校验也检测错误纠错
 - 核实标签组数据 CRC
 - 根据检测错误标志不良区域 ID，采样
 - 确定编码方式，而且拒绝未知编码
 - 确定区域标志

- 确定区域 ID
- 以数字油墨编码区域 ID、尖端 x-y 区位、尖端有效区状态
- 根据区域标志，路由选择数字油墨

注意不需要以与位置解码相同的速率进行区域 ID 解码。

注意如果发现码字与已知的好码字相同，则可以避免对该码字的解码。

对于第一个示例的变换例的表面编码，下面是相应解码顺序：

- 定位完整标签的目标
- 根据目标，推断透视变换
- 采样循环位置代码
- 解码循环位置代码
- 根据循环位置代码，确定取向
- 采样并解码局部里德-索罗门码字
- 确定标签 x-y 地址
- 根据取向目标，推断 3D 标签变换
- 根据标签的 x-y 区位和 3D 变换，确定尖端 x-y 区位
- 参照有效区映射，确定尖端区位的有效区状态
- 根据尖端有效区状态，产生局部反馈
- 确定标签类型
- 采样分布式里德-索罗门码字(根据标签类型，采用模窗对准(modulo window alignment))
 - 解码分布式里德-索罗门码字
 - 核实标签组数据 CRC
 - 根据检测错误标志不良区域 ID，采样
 - 确定编码方式，而且拒绝未知编码
 - 确定区域标志
 - 确定区域 ID

- 以数字油墨编码区域 ID、尖端 x-y 区位、尖端有效区状态
- 根据区域标志，路由选择数字油墨

不需要以与位置解码相同的速率进行区域 ID 解码并且如果发现码字与已知的好码字相同，则可以避免对该码字的解码。

如果高序坐标宽度不是 0，则必须特别关注低序 x 或者 y 坐标重叠的各标签之间的边界，否则就可能产生码字错误。如果在低序 x 或者 y 坐标检测到重叠（即，它含有全部 0 位或者全部 1 位），则可以在解码码字之前，调整相应高序坐标。如果在高序坐标上不存在真符号错误，则这样可以防止偶然引入码字错误。

扩展标签

通过附加关于其周边的附加符号带，可以扩展该标签以提高其数据容量。该附录描述了具有一个附加符号带的扩展标签。尽管在该说明书的主要部分描述的标签具有 36 个符号的原始容量，但是扩展标签具有 60 个符号的原始容量。

扩展标签的容量的确足以允许在每个标签组内包括整个 160 位数字签名。这样利用表面编码，通过“单击”交互，可以执行完整数字签名核实。

标签结构

图 39 示出完整 (P 型) 扩展标签的结构。除了附加符号带和目标位置的相关变化，它与上面描述的标签具有相同物理结构。

在扩展标签中，根据以每英寸 1600 点的间距印刷的 7 个点，宏点间隔 s 的正常值为 $111 \mu\text{m}$ 。

宏点通常是额定直径为 $(3/7)s$ 的圆。

目标通常是额定直径为 $(10/7)s$ 的圆。

扩展标签与上面描述的标签相同，也加入标签组，而且每个扩展标签具

有 3 种可能的标签类型 P、Q 和 R 之一。

扩展标签与上面描述的标签相同，也含有取向指示循环位置代码。

局部码字

该扩展标签在局部含有一个完整码字，该完整码字用于编码对该标签唯一的信息。该码字是穿孔 2^4 -ary(12,7)里德-索罗门码。因此，该标签至多编码对该标签唯一的 28 位信息。

图 40 示出局部码字的布局。

分布式码字

该扩展标签含有被标记为 B 至 M 的 12 个码字的片段，它们分布在 3 个相邻标签上，而且它们用于编码对一组相邻标签共用的信息。每个码字是穿孔 2^4 -ary(12,7)里德-索罗门码。因此，任意 3 个相邻标签一起编码对一组相邻标签共用的至多 336 位信息。

图 41 示出标签类型 P 中的 6 个码字 B 至 G 的头 4 个片段的布局。其它标签类型的布局遵循标签类型 P 的布局，其中标签类型 Q 中具有符号 4 至 7，而且标签类型 Q 中具有片段 8 至 11。

图 42 示出标签类型 P 中的 6 个码字 H 至 M 的头 4 个片段的布局。其它标签类型的布局遵循标签类型 P 的布局，其中标签类型 Q 中具有符号 4 至 7，而且标签类型 Q 中具有片段 8 至 11。

如图 37 所示，铺盖确保任意一组三个相邻标签包括每种类型的一个标签，并因此含有完整的一组分布式码字。根据在每个标签的局部码字内编码的 x-y 坐标，可以推断用于确定对特定一组相邻标签注册分布式码字的标签类型。

标签坐标空间

除了标签单位不同之外（因为标签结构和宏点间隔都发生变化），在扩

展标签内编码的标签坐标空间与在上面描述的标签内编码的标签坐标空间相同。

根据中心到中心标签的标签间隔，如下给出水平标签单元和垂直标签单元：

$$u_x = 5(2\sqrt{3}s) + 2d \cong 17.6s$$

$$u_y = 7.5(2s) + 2\left(d\frac{\sqrt{3}}{2}\right) \cong 15.2s$$

其中 d 是如下给出的分段间间隔

$$d = (1 - \sqrt{3}/2)s$$

标签信息内容

表 11 定义了嵌入扩展标签表面编码的信息字段。表 12 定义了这些字段如何映射到码字。

表 11. 字段定义

字段	宽度	描述
每个标签		
x 坐标	10	该标签的不带符号 x 坐标允许约 2.0 m (根据 EQ8) 的最大 x 坐标值。
y 坐标	10	标签的不带符号 y 坐标允许约 1.7 m (根据 EQ9) 的最大 y 坐标值。

有效区标志	1	表示该标签是否是有效区的成员的标志。b'1'表示成员资格。
有效区映射标志	1	表示是否存在有效区映射的标志。b'1'表示存在映射（参考下一个字段）。如果不存在映射，则根据该有效区标志（参考前面的字段），求得每个映射项目的值。
有效区映射	6	该标签的 6 个紧邻标签是有效区的成员的映射。b'1'表示成员资格—图 37 示出映射的位顺序。
数据片段	6	嵌入数据流内的片段。仅在不存在有效区映射时存在。
每个标签组		
编码格式	12	编码格式。 关于各值，请参考表 5。
宏点间隔调整	16	在带符号大小格式中，以 nm 为单位的实际宏点间隔与正常宏点间隔之间的差，正常宏点间隔是 111125 nm（根据 1600 dpi 和每个宏点 7 个点）
区域标志	12	用于对解释和路由选择区域相关信息进行控制的标志。 关于各值，请参考表 5。
区域 ID	112	含有该标签的区域的 ID
签名	160	该区域 ID 的数字签名
CRC	16	标签组数据的 CRC (CCITT CRC-16)

表 12. 字段到码字的映射

码字	码字位	字段宽度	字段位	字段
A	9:0	10	全部	x 坐标
	19:10	10	全部	y 坐标
	20	1	全部	有效区标志
	21	1	全部	有效区映射标志
	27:22	6	全部	有效区映射
	27:22	6	全部	数据片段
B	11:0	12	全部	编码格式
	27:12	16	全部	宏点间隔调整
C	11:0	12	全部	区域标志
	27:12	16	27:12	区域 ID
D	27:0	28	55:28	
E	27:0	28	83:56	
F	27:0	28	111:84	
G	11:0	12	11:0	CRC
	27:12	16	全部	
H	27:0	28	27:0	签名
I	27:0	28	55:28	
J	27:0	28	83:56	
K	27:0	28	111:84	
L	27:0	28	139:112	
M	19:0	20	159:140	
	27:20	8	全部	未使用

编码与印刷原理

如果宏点间隔从 9 点减小到 7 点，则该扩展标签的标签组单位单元仅遵守 PEC 的 TFS 宽度限制，正如 $111 \mu\text{m}$ 的宏点间隔 s 所反映的。

成像与解码原理

确保获取整个扩展标签所需的最小成像视场的直径为 $44 s$ ，即，

$$2(1 + 8 + 2)2s$$

表面编码与视场之间可以任意对准。如果宏点间隔是 $111 \mu\text{m}$ ，则这样得出约 4.0 mm 的要求视场。

表面编码安全性

安全性要求

定义项目安全性有两个相关目的：

- 允许验证项目
- 防止伪造项目

伪造的难度越大，验证的可信度越高。在编码项目时，超标记表面编码的安全性有两个相应目的：

- 允许验证编码项目
- 利用新项目 ID 防止伪造编码项目

如果用户可以确定项目表面编码的真实性，则该用户可以对项目的可能真实性进行有根据的判定。

如果非常难以伪造新 ID 的表面编码，则利用真实表面编码伪造项目的唯一便利方式是复制现有项目的表面编码（并因此复制其 ID）。如果用户可以利用其它方式确定项目的 ID 可能是唯一的，则该用户可以认为该项目是

真实的。

由于超标记表面编码允许在纯粹本地交互期间，在感测装置与编码表面之间进行有意义的交互，所以在类似的本地交互期间，希望该表面编码支持验证，即不需要增大感测装置视场的尺寸。

由于在真实编码项目的创建者与可能希望验证该项目的用户之间不存在先验关系 (priori relationship)，所以不希望要求创建者与用户之间的信任关系。例如，不希望要求各创建者与用户共享秘密签名密钥。

许多用户依赖在线访问创建者受信的用于验证各项目的验证器是合理的。相反，还希望允许在不进行在线访问的情况下进行验证。

保密性描述

如上所述，验证取决于核实数据与该数据的签名之间的对应关系。伪造签名的难度越大，则基于签名验证的可信度越高。

项目 ID 是唯一的，并且因此提供了用于签名的基础。如果假定在线验证访问，则该签名可以简单地是受信在线验证器可以访问的验证数据库内与项目 ID 有关的随机数。可以利用任意适当方法，例如，利用确定性（伪随机）算法或者利用随机物理方法产生该随机数。可以优选利用键控散列或者加密散列作为随机数，因为不需要增加验证数据库的空间。然而，与键控签名具有同样长度的随机签名比键控签名更安全，因为不容易受到密钥攻击 (key attack)。同理，较短的随机签名与较长键控签名具有同样的安全性。

在极限情况下，实际上不需要签名，因为数据库内仅存在的项目 ID 表示真实性。然而，签名的使用将伪造者限制在伪造它实际看到的项目。

为了防止伪造未看到的 ID 的签名，签名必须足够大，以致难以通过重复访问在线验证器进行穷尽搜索。如果不是随机地而是利用密钥产生签名，则其长度还必须大到足以防止伪造者根据已知的 ID 签名对推算出该密钥。几百位的签名被认为是安全的，而无论是利用专用密钥还是利用秘密密钥产生的。

尽管在标签（或者本机标签组）内包括合理保密随机数是实际的，特别是如果为了对签名提供更大的空间而缩短 ID 的长度，但是在标签内包括保密 ID 导出签名是不可行的。为了支持保密 ID 导出签名，我们可以代之以将该签名的片段分布到多个标签上。如果可以与 ID 分离分别核实每个片段，则可以实现在不增加感测装置视场的情况下，支持验证。不利用片段的长度而利用该签名的全长可以实现签名的安全性，因为伪造者不能预测用户将随机选择哪个片段进行核实。受信验证器可以始终进行片段核实，因为它们可以利用该密钥和/或者存储的整个签名，因此，在可以在线访问受信验证器时，始终可以进行片段核实。

片段核实要求我们防止强力攻击各片段，否则，通过轮番攻击每个片段，伪造者就可以确定整个签名。通过根据每个 ID 调整验证器，可以防止强力攻击。然而，如果各片段短，则需要非常多的调整。作为调整验证器的一种选择，验证器可以代之以根据给定的片段数量强制限制它愿意响应的核实请求的数量。即使该限制相当少，正常用户也不可能将它全部用于给定的片段，因为有许多片段可用并且用户选择的实际片段可以变化。通常，该限制应该与片段的大小成比例，即，片段越小，限制也越少。因此，用户的经可能稍许改变片段的大小。调整和强制片段核实限制意味着串行化送到验证器的请求。一旦核实失败，只需要执行片段核实限制，即，在第一次失败之前，可以出现不受限制的成功核实的次数。强制片段核实限制还要求验证器保持满足核实请求的每个片段计数。

通过将片段与在标签内编码的随机签名并置，也可以防止强力攻击。尽管可以认为随机签名可以保护片段，但是也可以认为该片段仅增加了随机签名的长度，因此，提高了其保密性。如果为了防止进一步核实该项目 ID，攻击者蓄意利用无效核实请求超过该限制，则片段核实限制可以拒绝服务攻击。这可以通过在伴生随机签名正确时仅对片段强制进行片段核实来防止。

通过要求同时核实最少量的片段，可以使片段核实更安全。

片段核实需要片段识别。可以对各片段进行明确编号，也可以利用其标

签的二维坐标、取模（modulo）连续铺盖标签上的签名的重复更经济地识别各片段。

有限长度的 ID 本身使得更加易受攻击。理想情况是，应该至少有几百位。在 Netpage 表面编码中，它是 96 位或者少于 96 位。为了解决该问题，可以填充该 ID。为了使其产生预期效果，该填充位必须是可变的，即各 ID 的填充位必须互不相同。理想情况是，该填充位仅是随机数，然后，必须将它们存储在利用 ID 索引的验证数据库内。如果根据 ID 确定地产生了填充位，则其毫无价值。

脱机验证秘密密钥签名要求使用受信脱机验证装置。QA 芯片（它是包括第 09/112,763、09/112,762、09/112,737、09/112,761、09/113,223 号的几个美国未决专利申请的主题）提供了这种装置的基础，但是限制了容量。可以对 QA 芯片进行编程，以利用安全保存在其内部存储器上的秘密密钥，核实签名。然而，在这种情况下，支持对每个 ID 填充不可行，甚至支持非常多的保密密钥也不可行。此外，以这种方式编程的 QA 芯片易受选择消息的攻击。这些制约限制了将基于 QA 芯片的受信脱机验证装置应用于适当场所的应用。

通常，不管任意特定受信脱机验证装置所要求的安全性，保密项目的创建者很可能不愿意将其秘密签名密钥交付给该装置，而且这还可能限制这种装置应用于适当场所的应用。

相反，脱机验证公用密钥签名（即，利用相应专用密钥产生）非常可行。利用公用密钥的脱机验证装置可以轻而易举地保存任意数量的公用密钥，而且在该脱机验证装置遇到它知道没有相应公开签名密钥的 ID 时，利用瞬间在线连接，该脱机验证装置可以根据需要检索附加公用密钥。未受信脱机验证对保密项目的大多数创建者有吸引力，因为他们可以继续完全控制他们的专用签名密钥。

脱机验证公用密钥签名的缺陷是，必须从编码获取整个签名，这违背了我们利用最小视场支持验证的要求。脱机验证公用密钥签名的相应优点是不

再要求利用 ID 填充, 因为利用公开签名密钥解密该签名产生 ID 及其填充位, 然后可以忽略该填充位。伪造者不能利用脱机验证期间忽略填充位的情况, 因为在线验证期间没有忽略填充位。

获取整个分布式签名并不特别费力。在编码表面上任意随机或者直线挥动手持感测装置使其可以迅速获取该签名的所有片段。可以容易地对该感测装置进行编程, 以在它获得一组全部片段并完成验证时, 对用户发送信号。扫描激光器也可以轻而易举地获取该签名的所有片段。可以对两种装置进行编程, 以在该标签指示存在签名时仅进行验证。

请注意, 以与任意签名相同的方式, 利用其任意片段可以在线验证公用密钥签名, 而无论是否随机产生或者使用秘密密钥。受信在线验证器根据需要利用专用密钥和 ID 填充位产生签名, 也可以明确地将该签名存储在验证数据库内。后一种方法不需要存储 ID 填充位。

还请注意, 即使可以在在线访问受信验证器时, 也可以利用基于签名的验证代替基于片段的验证。

表 13 根据上面的讨论概括列出哪些方案可行。

表 13 可行签名方案概括

在标签上编码	根据标签获取	签名产生	在线验证	脱机验证
本机	全部	随机	好	对于存储每个 ID 信息不可行
		秘密密钥	签名太短不安全	不希望存储保密密钥
		专用密钥	签名太短不安全	
分布式	片段	随机	好	不可行 ^b

		秘密密钥	好	不可行 ^c
		专用密钥	好	不可行 ^b
全部		随机	好	不可行 ^b
		秘密密钥	好	不可行 ^c
		专用密钥	好	好

安全性说明

图 43 示出示例性项目签名对象模型。

项目具有 ID (X) 和其它详细内容 (未示出)。它可选地具有秘密签名 (Z)。它还可以可选地具有公用密钥签名。公用密钥签名明确记录了签名 (S)，而且/或者记录与 ID 结合产生签名的填充位 (P)。公用密钥签名具有相关公开一专用密钥对 (K, L)。该密钥对与一系列或者多系列项目 ID 相关。

通常，保密文档的发行人和药物的供应商利用一系列 ID 识别一系列文档等。此后，发行人使用这些详情对每个项目或者要标记的文档产生相应 ID。

然后，通过感测在该标签内编码的标签数据可以在线或者脱机验证该产品，并且根据情况利用几种不同机制进行验证。

现在将分别对公用密钥加密和专用密钥加密描述相关处理的示例。

基于公用密钥签名的验证

每一 ID 系列的设置：

- 产生共用-专用签名密钥对 (K, L)
- 存储利用 ID 系列索引的密钥对 (K,L)

每个 ID 的设置：

- 产生 ID 填充位 (P)

- 利用 ID (X) 检索专用签名密钥 (L)
- 通过利用专用密钥 (L) 加密 ID (X) 和填充位 (P) 产生签名 (S):

$$S \leftarrow E_L(X, P)$$
- 将签名 (S) 存储在利用 ID(X)索引的数据库内 (和/或者存储填充位 (P))
- 编码所有标签组内的 ID (X)
- 以重复方式编码位于多个标签上的签名 (S)

基于片段的在线验证 (用户):

- 从标签获取 ID (X)
- 从标签获取位置(x,y)_i 和签名单段(T_i)
- 根据位置(x,y)_i 产生片段号 (i):

$$i \leftarrow F[(x,y)_i]$$
- 利用 ID(X)检查受信验证器
- 将 ID(X)、片段 (S_i) 以及片段号 (i) 发送到受信验证器

基于片段的在线验证 (受信验证器)

- 从用户接收 ID(X)、片段 (S_i) 和片段号 (i)
- 利用 ID(X)从数据库检索签名 (S) (或者再生签名)
- 将收到的片段 (T_i) 与签名 (S_i) 的相应片段进行比较
- 向用户报告验证结果

基于签名的脱机验证 (用户):

- 从标签 (X) 获取 ID
- 从标签获取位置(x,y)_i 和签名单段(T_i)
- 根据位置(x,y)_i 产生片段号 (i):

$i \leftarrow F[(x,y)_i]$

$S \leftarrow S_0 | S_1 | \dots | S_{n-1}$

- 从 (n) 个片段产生签名 (S)
- 利用 ID(X) 检索公用签名密钥 (K)
- 利用公用密钥 (K) 解码签名 (S)，以获取 ID(X') 和填充位 (P')：
 $X' | P' \leftarrow D_K(S)$
- 将获取的 ID(X) 与解码的 ID(X') 进行比较
- 向用户报告验证结果

基于秘密密钥签名的验证

每个 ID 的设置：

- 产生秘密 (Z)
- 将秘密 (Z) 存储在利用 ID(X) 索引的数据库内
- 在所有标签组内编码 ID(X) 和秘密 (Z)

基于秘密的在线验证（用户）：

- 从标签获取 ID (X)
- 从标签获取 (Z')
- 利用 ID(X) 检查受信验证器
- 将 ID(X) 和秘密 (Z') 发送到受信验证器

基于私密的在线验证（受信验证器）

- 从用户接收 ID(X) 和秘密 (Z')
- 利用 ID(X) 从数据库检索秘密 (Z)
- 将收到的秘密 (Z') 与秘密 (Z) 进行比较
- 向用户报告验证结果

如上所述，可以结合基于片段的验证使用基于秘密的验证。

密码算法

在脱机验证公用密钥签名时，用户的认证装置通常不能访问在原始产生签名时使用的填充位。因此签名核实步骤必须对该签名解密以允许认证装置将签名中的 ID 与从标签中获取的 ID 相比较。这通过解密签名排除了使用不执行签名验证步骤的算法，如 U.S, Department of Commerce/National Institute of Standards and Technology, Digital Signature Standard(DSS) FIPS 186-2, 27 January 2000 中的数字签名算法标准。

RSA 加密在下面进行了描述

- Rivest, R.L., A. Shamir, and L.Adleman, “A Method for Obtaining Digital Signature and Public-Key Cryptosystems” Communications of the ACM, Vol.21, No. 2, February 1978, pp.120-126
- Rivest, R.L., A.Shamir, and L.M.Adleman, “ Cryptographic communications system and method”, 1983 年 9 月 20 日授予的第 4,405,829 号美国专利
- RSA Laboratories, PKCS #1 v2.0: RSA Encryption Standard, October 1,1998

RSA 提供了一种对签名进行解密的合适的公用密钥数字签名算法。RSA 为以下标准提供了基础：美国国家标准局的 ANSI X9.31 数字签名标准, ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry(rDSA), 1998 年 9 月 8 日。如果不使用填充，则可以使用任何公用密钥签名算法。

在超标记表面编码方案中，ID 是 96 位长或者比 96 位短。在被签名前，将它填充到 160 位。

理想情况下，使用真正的随机过程如量子过程[14, 15]或者通过从随机事件中提取随机性（Schneier, B., Applied Cryptography, Second Edition, John Wiley & Sons 1996）来产生填充。

在超标记表面编码方案中，随机签名或者秘密是 36 位长或者比 36 位短。此外，理想情况是，利用真正随机过程产生它。如果要求更长的随机签名，则可以缩短表面编码中的项目 ID 的长度，以对该签名提供附加空间。

设置安全标签和跟踪

可以对货币、支票和其他金融票据加标签，以检测伪造的货币，从而反对洗钱活动。可以通过金融系统确认、跟踪设置了超标记标签的货币。可以对诸如药品的设置了超标记标签的产品设置标签，以使得可以通过发送和零售系统验证和跟踪它们。

许多设置超标记安全标签和跟踪的概念特别是针对钞票和药品，但是超标记标签可以同等地用于可靠地标记和跟踪其它产品，如旅游支票、活期存折、护照、化学制品等。

用 Netpage 系统设置超标记标签提供了用于可靠确认和跟踪对象的机制。

对象表面上的超标记标签唯一识别该对象。每个超标记标签含有包括该对象的唯一 ID 的信息以及该标签在设置了超标记标签的表面上的地址。超标记标签还包括可以用于验证该对象的签名单段。扫描激光器或图像传感器可以读取该对象的任意部分上的标签，以识别该对象、确认该对象以及允许跟踪该对象。

货币加标签

为了检测伪造并允许跟踪货币运动，可以利用超标记为货币加标签。超标记标签可以印刷在整个钞票表面上或印刷在钞票的一个小区域内。除了诸如全息图、箔条、彩色偏移油墨等安全特征之外还可以使用超标记标签。扫

扫描激光器或图像传感器读取钞票任何一部分上的标签以确认每个钞票。

超标记货币标签识别钞票的货币性、发行国家和面额。该标签还识别钞票的序列号、钞票面（即正面或背面），标签还可以包含其它信息（如印刷钞票的准确印刷工厂）。每个实际银行票据有两个钞票 ID——每个票据面有一个。

每次扫描钞票时记录其位置。该位置信息可以收集在中央数据库中，使得可以分析和识别异常货币运动和检测伪钞。例如在超标记点图案被精确复制的复杂伪造的情况下，被准确伪造的钞票有许多副本（至少是原本和伪钞）。如果在不同地方同时出现许多同样的钞票，除一张之外其它都是伪钞。将所有钞票作为可疑钞票对待。

任意超标记扫描仪都可以读取超标记货币标签。可以将这些扫描仪并入各种装置中，以便进行验证和跟踪，例如，自动柜员机、点钞机（currency counter）以及自动售货机。还可以将扫描仪并入如下装置中：

- 点钞机
- 自动柜员机
- 现金出纳机
- 出售点（POS）付款台
- 具有内置扫描仪的移动电话
- Netpage 笔
- 自动售货机
- 超标记超级市场结账
- 具有内置扫描仪的移动电话
- 手持有效性（validity）扫描仪

这些扫描仪是多用途扫描仪，因为它们还可以用于扫描加超标记的消费类商品和印刷材料。小型手持扫描仪还可以用于扫描和确认货币。在扫描仪扫描钞票时，它将该钞票的详情、当前日期和时间以及扫描仪区位（如果知

道)通知货币服务器。可选地,如果知道,扫描仪还可以发送进行现金交易的人员的身份。在银行间交易、货币兑换以及大额现金交易中,可以利用该信息。

在未决专利申请号(我们将在此添加特定货币应用的案号)中,进一步详细说明了货币加标签过程。

药品加标签过程

可以在药品包装的整个表面上印刷超标记标签,也可以仅在该包装的小区域内印刷该超标记标签。超标记药品标签包括项目的产品 ID 和序列号,以唯一识别各项目。产品 ID 识别该项目的国家药品代码(NDC)号。FDA(美国食品及药物管理局)对药品和药品相关项目分配和管理 NDC 号,而且 NDC 号识别产品和制造商。作为一种选择,标签可以包括另一种产品 ID 代码,例如,欧洲国际商品编号(EAN)代码或者 EPC 等。

扫描仪可以读取药品 ID,而且利用该药品 ID 可以察看该项目批号的详情和到期日。作为一种选择,批号和到期日可以包括在药品标签内,以便利用任意扫描仪脱机检索该信息。药品 ID 还可以用于访问诸如剂量和施用信息、药物相互作用、预防措施、禁忌、产品警告、召回信息、产地等的详情。

在每次扫描药品项目时,记录其区位。可以在中心数据库采集该区位信息,以便分析和识别异常产品流动以及检测伪造药品。

适当扫描仪可以包括:

- 现金出纳机
- POS 付款台
- 具有内置扫描仪的移动电话
- Netpage 笔
- 自动售货机

在未决专利申请号（我们将在此添加特定货币应用的案号）中，进一步详细说明了药品加标签过程。

跟踪

为了进行跟踪和项目确认，该制造商，或者其他中心机构维护用于跟踪所有项目的区位和状态的数据库。

可以将超标记扫描仪内置在各种装置内。扫描仪可以是固定的，也可以是移动的。固定扫描仪具有已知永久区位。移动扫描仪没有固定区位。扫描仪可以在线，即，可以立即访问中心数据库，它也可以脱机。

扫描仪可以是诸如点钞机的特定产品应用专用的，也可以是通用超标记扫描仪。Hyperlabel 扫描仪可以嵌入其它多功能装置中，例如，可以嵌入移动电话或者 PDA 中。

中心数据库保存关于有效对象 ID 的最新信息、对象 ID 热列表（所有可疑对象 ID）以及对应于对象 ID 的公用密钥列表。为了跟踪对象流动，中心服务器还保存对象扫描历史。在每次扫描对象时，记录其加了时间戳的区位。如果知道，还可以记录对象所有者的详情。对于大额金融交易，例如，从银行提取大量现金，尤其要知道该信息。可以利用该对象扫描历史数据检测违法产品流动，例如药品的非法进口。还可以用于检测可能指示产品伪造的异常或可疑的产品流动。

如果已知对象已被盗窃，可以立即将该对象添加到中心服务器中的对象 ID 热表中。该热表被自动分发到所有在线扫描仪（或变得可被其访问），并在脱机扫描仪的下次更新时下载到所有脱机扫描仪上。以这种方式，被盗状态被自动并快速地分发到大量出口。同样，如果以任何其他方式怀疑一个对象，则可以将该对象添加到该热表中从而向扫描该对象的人员标志其状态。

在线扫描仪可以即时访问中心服务器以便可以在扫描时核实每个对象 ID。也可以在扫描该对象的同时更新中心服务器中的对象扫描历史。

脱机扫描仪内部存储对象状态数据以允许确认被扫描的对象。该对象状

态数据包括有效 ID 系列列表、对象 ID 热列表、公用密钥列表和对象扫描历史。每次扫描对象时都将详情记录在对象扫描历史中。每次连接扫描仪时从中心服务器中下载对象状态数据，并将对象扫描历史上传到中心服务器上。

可以通过扫描仪向应用提供移动扫描仪的区位，如果该扫描仪配备了 GPS 的话。可替换的，可以通过与该扫描仪通信的网络来提供该扫描仪的区位。

例如，如果手持扫描仪使用移动电话网络，可以通过移动电话网络供应商提供扫描仪的区位。有许多定位技术可供使用。一个是辅助全球定位系统（A-GPS）。其要求配备了 GPS 的手持设备，该设备从 GPS 卫星接收定位信号。电话网络从最近的小区站点了解手持设备（在这种情况下手持设备也是扫描仪）的大约区位。根据该位置，网络通知该手持设备使用哪个 GPS 卫星来计算位置。另一种不需要配备 GPS 的设备的技术是上行链路到达时间差（U-TDOA）。该技术利用三角测量的形式，通过比较无线手持设备的信号到达安装在网络小区站点上的若干区位测量单元（LMU）所花费的时间来确定无线手持设备的区位。然后基于 3 个（或更多个）信号到达时间的差来计算该手持设备的区位。

验证

每个对象 ID 具有签名。超标记标签结构内的有限空间使得无法在一个标签内包括全部密码签名，从而签名单段分布在多个标签上。标签内可以包括更小的随机签名或者秘密。

为了避免由于对象 ID 的有限长度而导致的弱点，理想情况下用随机数填充该对象 ID。填充位存储在根据对象 ID 索引的验证数据库中。该验证数据库可以由制造商管理，或者由第三方受信验证器管理。

每个超标记标签包含签名单段，可以针对对象 ID 单独核实每个片段（或片段的子集）。签名的安全性仍然来源于签名的全部长度而不是来自片段的长度，因为伪造者无法预测用户将随机选择哪个片段来核实。

片段核实需要片段识别。片段可以被明确地编号，或者通过标签的二维坐标对在连续标签铺盖上的签名的重复取模来识别。

要注意受信验证器总是可以执行片段核实，因此在可以在线访问受信验证器时总是可以进行片段核实。

建立验证数据库

在分配一系列新 ID 之前，需要一些设置任务来建立验证数据库。

对于每个系列 ID，产生公用专用签名密钥对，并将该密钥对存储在利用 ID 系列索引的验证数据库内。

对于该系列内的每个对象 ID，需要以下设置工作：

- 产生 ID 填充位，并将该填充位存储在利用对象 ID 索引的验证数据库内
- 利用对象 ID 检索专用签名密钥
- 通过利用专用密钥对对象 ID 和填充位进行加密产生签名
- 将签名存储在利用对象 ID 索引的验证数据库内，而且/或者存储该填充位，因为利用该 ID、填充位和专用密钥，可以再生该签名
- 以重复方式，编码多个标签上的签名

超标记标签需要该数据，因此必须在印刷超标记之前或同时建立验证数据库。

上面更详细描述了安全问题。

基于公用密钥的脱机验证

脱机验证装置利用公用密钥签名。该验证装置保存大量公用密钥。可选的，该装置在遇到它没有对应的公用密钥签名的对象 ID 时可以通过临时在

线连接按需要检索另外的公用密钥。

对脱机验证来说需要整个签名。验证装置在设置了超标记标签的表面上挥动，多个标签被读取。由此获取对象 ID 和多个签名单段及其区位。然后从这些签名单段中产生签名。使用对象 ID 从扫描装置查找公用密钥。然后利用该公用密钥解密该签名，给出对象 ID 和填充位。如果从该签名中获得的对象 ID 与超标记标签中的对象 ID 匹配，则认为该对象是真实的。

利用用作验证器的受信验证器，还可以在线使用该脱机验证方法。

基于公用密钥的在线验证

在线验证装置使用受信验证器来核实对象的真实性。对于在线验证来说，一个标签就可以是执行验证所需的全部。该验证装置扫描对象并获取一个或多个标签。由此获取对象 ID 以及至少一个签名单段及其位置。由该片段位置产生片段号。按照对象 ID 查找合适的受信验证器。向受信验证器发送对象 ID、签名单段和片段号。

受信验证器接收该数据并按照对象 ID 从验证数据库中检索该签名。将该签名与提供的片段比较，并向用户报告验证结果。

基于秘密的在线验证

可替换或附加的，如果在每个标签（或标签组）中包含了随机签名或秘密，则可以参照受信验证器可访问的秘密的复制品来验证。然后数据库设置包括为每个对象分配秘密，将该秘密存储在利用对象 ID 索引的验证数据库中。

验证装置扫描对象并获取一个或多个标签。由此获得对象 ID 以及秘密。利用该对象 ID 查找合适的受信验证器。向该受信验证器发送对象 ID 和秘密。

受信验证器接收数据并将利用对象 ID 从验证数据库检索秘密。将该秘密与所提供的秘密比较，并且将验证结果报告给用户。

基于秘密的验证可与上面详细讨论的基于片段的在线验证结合起来使

用。

产品扫描交互

图 44 示出零售商处的产品扫描。当仓库操作员扫描设置了超标记标签的产品时该标签数据被发送到服务终端 (A)。该服务终端向存储服务器发送交易数据 (B)。存储服务器向制造商服务器发送该数据以及零售商细节 (C)。超标记服务器从对象 ID 中了解要向哪一个制造商服务器发送该消息。在接收到该输入时，如果制造商是受信验证器，则制造商服务器验证该对象。可替换地，制造商服务器将该数据传递给验证服务器以核实对象 ID 和签名 (D)。验证服务器将验证结果返回给制造商服务器 (E)。制造商服务器检查对象 ID 的状态(对比其有效 ID 列表和热列表)，向存储服务器发送响应(F)，该存储服务器又将该结果返回给存储服务终端 (G)。存储服务器还可以直接与有关的验证服务器通信。

图 45 示出零售商处的在线产品扫描的交互细节。仓库操作员扫描设置了超标记标签的产品。扫描仪向服务终端发送扫描仪 ID 和标签数据。服务终端将该数据连同终端 ID 和扫描仪区位一起发送给存储服务器。然后存储服务器向制造商服务器发送请求，制造商服务器执行验证（自己进行或通过第三方验证服务器进行）并确定对象状态。然后将响应返回给存储服务器，并传递给操作员服务终端。

图 46 示出零售商处的脱机产品扫描的交互细节。仓库操作员扫描设置了超标记标签的产品。扫描仪向服务终端发送扫描仪 ID 和来自多个标签的标签数据。服务终端将该数据连同终端 ID 和扫描仪区位一起发送给存储服务器。然后存储服务器如 3.4.2 节描述的那样执行脱机验证，并通过其缓存的热列表、有效对象 ID 列表和公用密钥列表确定对象状态。存储服务器在其内部对象扫描历史中记录扫描细节。然后响应被返回给操作员服务终端。

脱机产品扫描仪的替换方案发生在扫描仪是手持的单机扫描仪时。在这种情况下缓存的验证数据存储在该扫描仪本身内部，并由扫描仪在内部执行

确认。对象扫描历史数据也缓存在该扫描仪内。扫描仪定期连接到中心数据库，上传其对象扫描历史，下载最新的公用密钥列表、对象 ID 热列表和有效 ID 系列列表。该连接可以是自动的（用户无法看见），或者可以由用户启动，例如当扫描仪放置在停泊站（docking station）/加载机（charger）中时。

图 47 示出用 Netpage 笔进行的产品扫描。当用户用 Netpage 笔扫描设置了超标记标签的产品时，该输入从用户的 Netpage 笔以通常的方式发送给 Netpage 系统（A）。为了扫描产品而不是与该产品交互，可以将该笔设置为特殊模式。这通常是单触发（one-shot）模式，可以通过敲击印刷在 Netpage 上的<扫描>按钮来启动。可替换的，该笔可具有用户可操作按钮，该按钮在敲击或者划过过程中按下时告诉笔将该交互作为产品扫描而不是正常交互来对待。标签数据从该笔发送给用户 Netpage 基站。Netpage 基站可以是用户的移动电话或 PDA，或者是其它 Netpage 装置如 PC。按照常见方式将该输入中继给超标记服务器（B）然后传递给制造商服务器（C）。在接收到该输入时，如果制造商是受信验证器则制造商服务器验证该对象。可替换的，制造商服务器将该数据传递给验证服务器以验证对象 ID 和签名（D）。验证服务器将验证结果返回给制造商服务器（E）。制造商服务器检查对象 ID 的状态（对比其有效 ID 列表和热列表），向超标记服务器发送响应（G）。作为 Netpage 系统的一部分，超标记服务器可以知道用户的身份和设备。超标记服务器将制造商服务器的响应中继给合适的用户电话（G）或 Web 浏览设备（H）。如果用户的 Netpage 笔具有 LED，则超标记服务器可以向用户笔发送命令以点亮合适的 LED（I, J）。

图 48 示出用 Netpage 笔扫描的交互细节。Netpage 笔点击设置了超标记标签的产品。Netpage 笔向超标记服务器发送笔的 ID、产品标记数据和笔的区位。如果笔的 ID 还没有与扫描仪关联，则超标记服务器可以为该笔创建新的扫描仪记录，或者将笔的 ID 用作扫描仪 ID。超标记服务器向制造商服务器发送扫描仪 ID、标签数据和扫描仪区位（如果已知），该制造商服务器执行验证（自己进行或通过第三方验证服务器进行）并确定对象状态。然后

将响应返回给超标记服务器，并传递给用户的默认 Web 浏览装置。

设置安全标签和跟踪对象模型

设置安全标签和跟踪对象模型围绕超标记标签、对象 ID 和签名。图 60 示出这些对象的管理和组织。

如图 49 所示，超标记标签包含标签类型、对象 ID、二维位置和签名单段。标签类型指示这是否是普通对象上的标签，或者该标签是否在诸如钞票或药品的特殊类型对象上。签名单段具有可选的片段号，其标识片段在整个签名中的位置。

如上所述，可以将产品的唯一项目 ID 看作特殊类型的唯一对象 ID。电子产品代码（EPC）是项目 ID 的一种原始标准。项目 ID 通常包括产品 ID 和序列号。产品 ID 识别产品类别，而序列号识别该类别中的特例，即，各产品项目。产品 ID 通常又包括制造商编号和产品分类号。最知名的产品 ID 是 EAN.UCC 通用产品代码（UFC）及其衍生代码。图 50 示出该项目 ID 分级图。

通过钞票 ID 识别钞票。钞票 ID 包括钞票数据和序列号。钞票数据确定钞票类型、发行国家、钞票面值、钞票面（正面或背面）和其它特定于钞票的信息。每张实际钞票存在两个钞票 ID——印刷钞票的每个面有一个。图 52 示出钞票 ID 分级图。

利用药品 ID 识别药品。通常，药品 ID 是 EPC。药品 ID 包括产品 ID 和序列号。产品 ID 通常又包括制造商编号和产品分类号。药物产品的最知名产品 ID 是美国食品与药物管理局分配和管理的国家药品代码（NDC）。图 52 示出药物 ID 分级图。

图 53 示出对象描述、所有权和群集分级图。上面对此做了详细说明。

图 54 示出对象扫描历史分级图。对象具有对象扫描历史，这是每次扫描仪扫描对象时记录的。每个对象扫描事件包括扫描仪 ID、扫描的日期和时间、扫描时的对象状态、扫描对象时扫描仪的区位。对象状态可以是有效、

被盗、伪造嫌疑等等。对象所有者细节如果已知也可以记录下来。

扫描仪具有唯一扫描仪 ID、网络地址、所有者信息和状态（例如在线、脱机）。扫描仪是区位可以改变的移动扫描仪，或者是区位已知且恒定的固定扫描仪。扫描仪具有当前区位，包括区位细节和时间戳。扫描仪可以是 Netpage 笔，在这种情况下该笔与 Netpage 笔记录相关联。如果扫描仪脱机，则其保持对象扫描历史，可选的还可以存储公用密钥列表、有效 ID 系列列表和对象 ID 热列表。扫描仪分级图在图 55 示出。

制造商或其它中心机构维护多个对象 ID 热列表，每一个热列表都具有一个唯一列表 ID 以及最近更新该列表的时间。每个热列表包含可疑对象 ID 列表，其包括对象 ID、日期、时间、状态（可疑的伪造、偷盗等）和其他信息。对象 ID 热表分类图在图 32 示出。

制造商或者其他中心机构保存有效 ID 系列列表。该列表中的每个有效 ID 系列表目分别包括开始对象 ID 和结束对象 ID（有效 ID 系列）以及该表目被更新的时间。图 57 示出有效 ID 系列列表分级图。制造商或其它中心机构维护有效 ID 系列列表。该列表中每个有效对象 ID 系列条目都包括起始对象 ID 和结束对象 ID（有效 ID 系列）以及更新该表目的时间。有效 ID 系列列表分级图在图 57 示出。

制造商或其它中心机构维护公用密钥列表。公用密钥列表由多项指示用于对象 ID 系列的公用密钥的表目组成。每个有效对象 ID 系列表目包括该表目的更新时间、该系列的起始对象 ID、该系列的结束对象 ID 和可用于给定系列中每个对象 ID 的公用密钥。公用密钥列表分级图在图 58 示出。

对象验证可以由制造商或第三方受信验证器来进行。受信验证器具有验证器 ID、名称和详情。受信验证器持有公用-专用密钥对列表，每一对都与一个或多个 ID 系列相关联。这是对象 ID 系列（通过起始和结束 ID 标识）和对应的公用/专用签名密钥对的列表。受信验证器还持有秘密签名列表和公用密钥签名列表。每个公用密钥签名标识实际的签名和/或用于产生该签名的填充位。每个秘密签名和公用密钥签名通过对象 ID 与唯一对象关联。受信

验证器分级图在图 59 示出。

应用

将会理解到，超标记标签可以与一系列对象一起使用，这一系列对象例如包括：制造项目、药物项目、钞票、支票、信用卡或者借记卡、可赎回票、凭单、息票、彩票、即刻兑奖票、或者身份证件或者诸如驾驶证或者护照的身份证件。

身份可以包括：电子产品代码（EPC）、国家药品代码（NDC）号、药品项目序列号、诸如币值等的钞票属性、支票属性，或者诸如卡类型、发行机构、账号、发行日期、到期日或者限额（limit）的卡属性

超标记的优点

与通常因为标签破损而难以读取而且扫描要求直接“瞄准线”的 2D 光学条形码不同，在整个产品标记或者大部分产品标记上印刷利用光学方法可读，但是不可见的红外超标记标签。超标记标签支持视线全向读取。实际上，超标记阅读器用于从至少两个大致垂直方向扫描扫描区。这样有助于该阅读器避免手握持项目时发生阻塞。为了提高可靠性，超标记标签还引入了里德-索罗门纠错方法。

超标记优于条形码的另一个优点是，不引起客户注意，因为它们没有使用可见标签空间，而且标签信息不只局限于标签的一部分。

因此，容易定位、读取而且可以准确自动扫描超标记标签。

超标记没有 RFID 标签那么杂乱，因为 RFID 标签要求视线读取。这意味着，客户难以扫描它们不知道信息的产品。超标记为客户提供了一种保护其隐私的方式。

超标记作为交互 web 页面

超标记技术的唯一有特色特征是，超标记提供了将包装标签作为交互

“web 页面”进行设计的机会，因此，制药业可以引入一系列全新产品链接的客户服务（product-linked customer services）。

在普遍使用数字笔时，可以对标记增加产品图形以指示交互区，而且提醒客户利用 Netpage 笔写入或者点击。数字 Netpage 笔可以识别标记上的 x-y 位置，而且可以在标记上的信息与服务器内的 web 页面之间建立链路。通过诸如移动电话或者计算机的辅助装置，Netpage 笔将客户连接到基于因特网的超标记服务器。

通过利用 Netpage 笔与标记交互，可以对客户提供关于药品使用、危险以及药物之间的可能相互作用忠告方面的附加信息。它还为客户提供了对参与新药品试验进行记录、进入促销、参与 web 聊天对话，或者接收“免费”试用的机会。可以根据客户概况、本地区卫生数据，或者利用诸如地理地点的一系列产品供应链数据，定制 Web 页面。

因此，超标记可以使制药业扩大使用产品标记和包装，以增大商标的长度，而且与客户建立更紧密联系。因此，利用超标记，可以使客户成为产品供应链的组成部分，而且可以将供应链数据与客户关系管理（CRM）或者保健数据库整合在一起，以提高总体效率和对客户提供的服务水平。

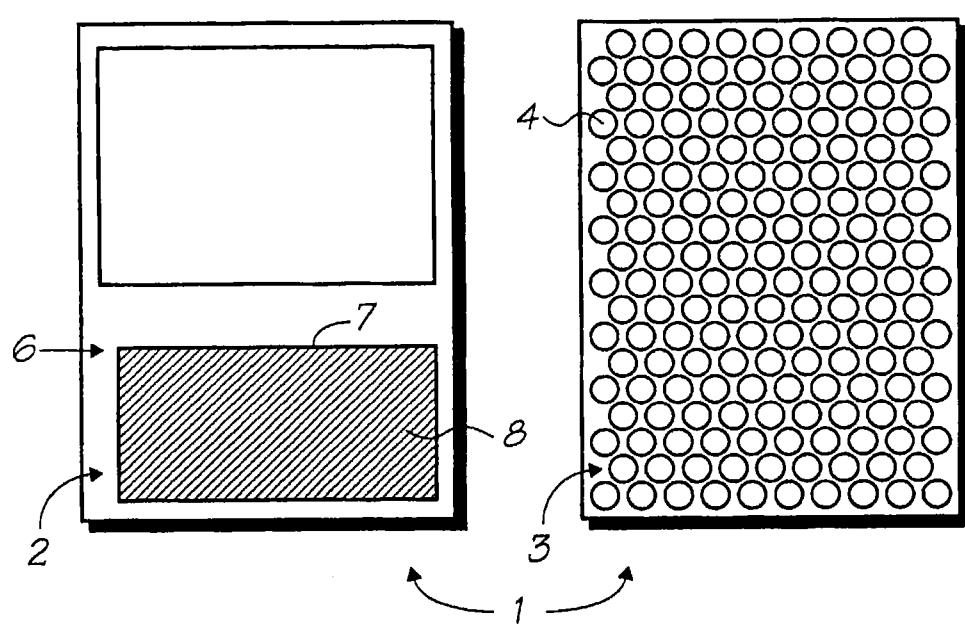


图 1

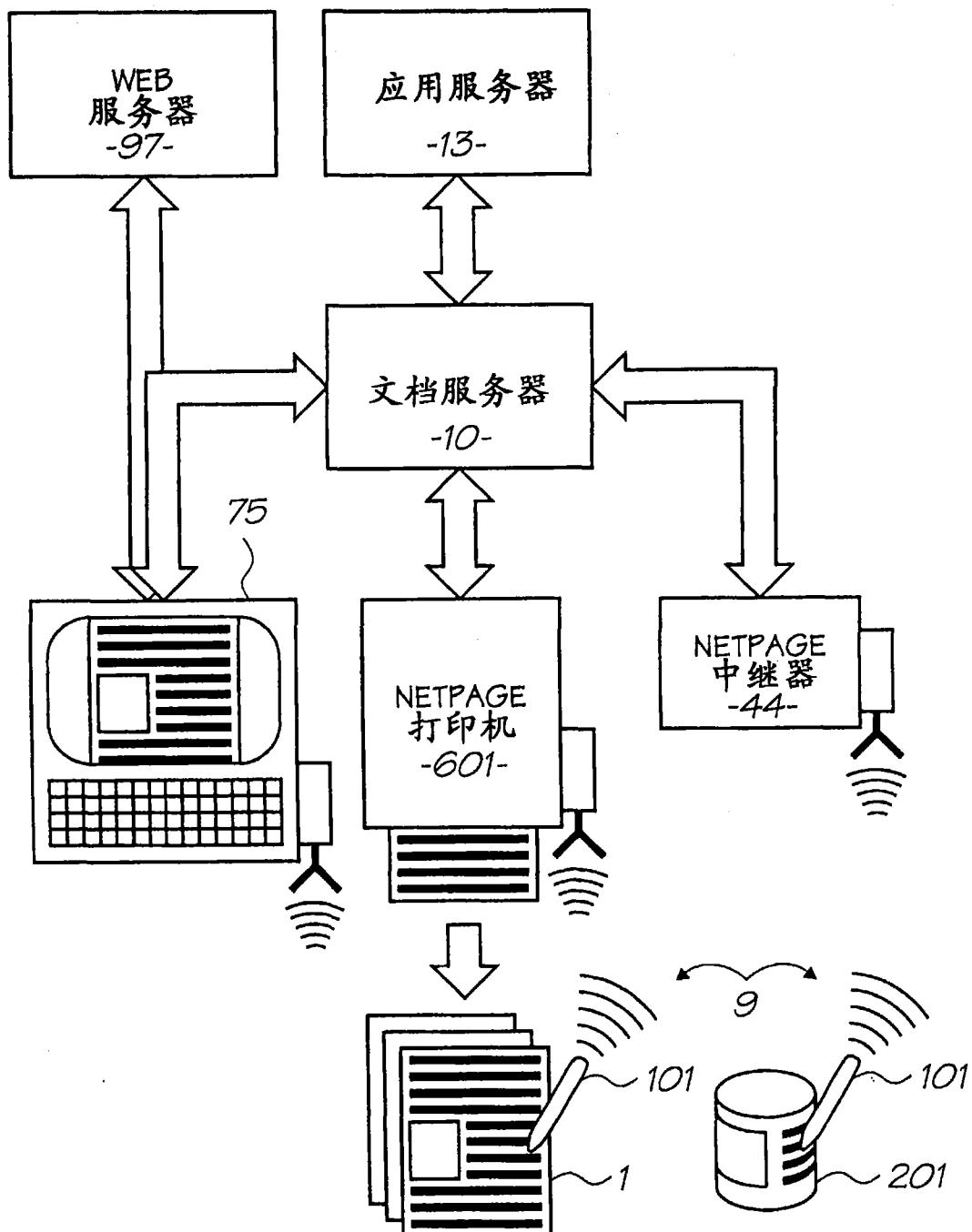


图 2

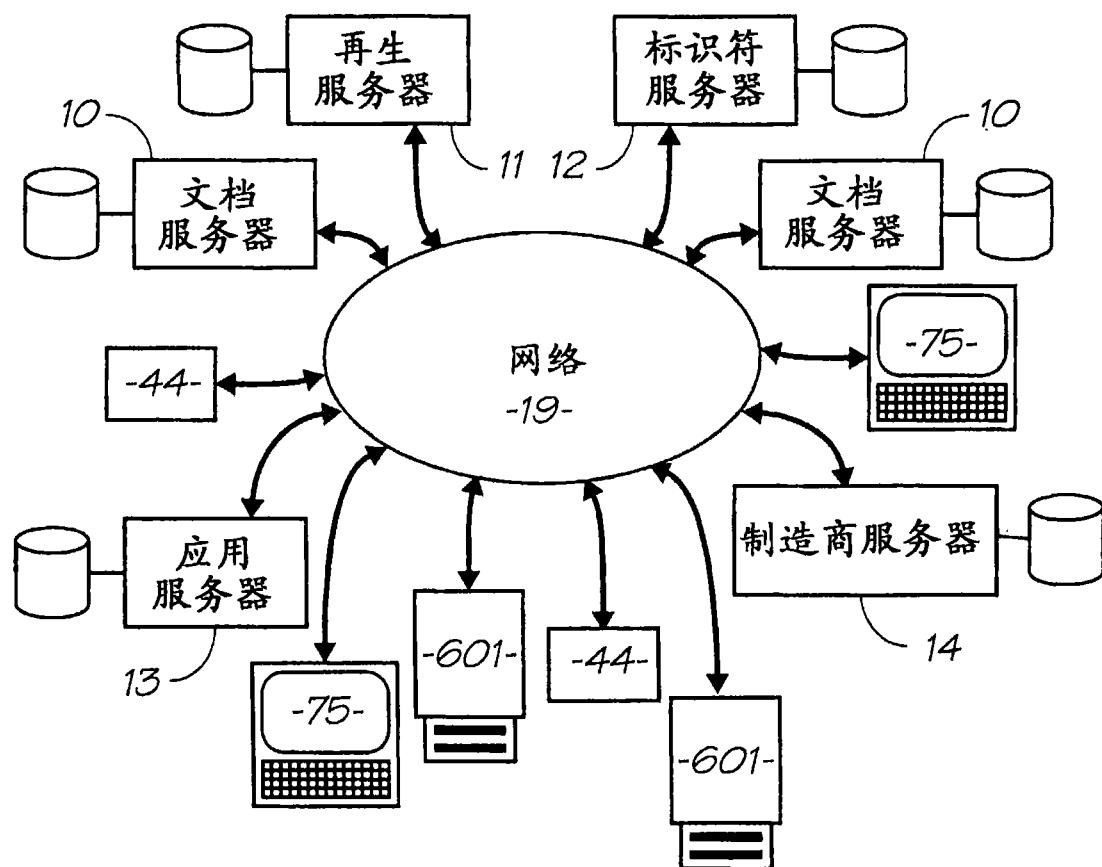


图 3

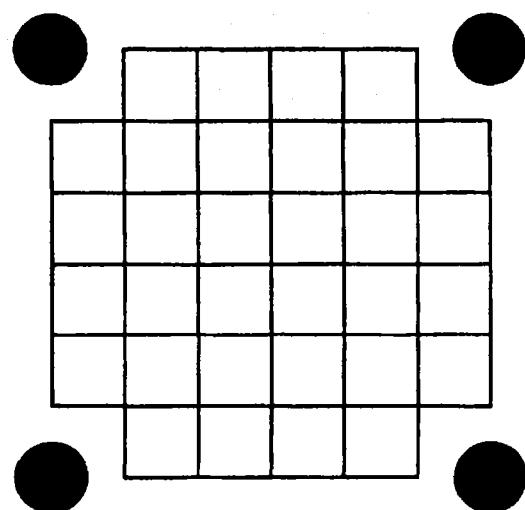


图 4

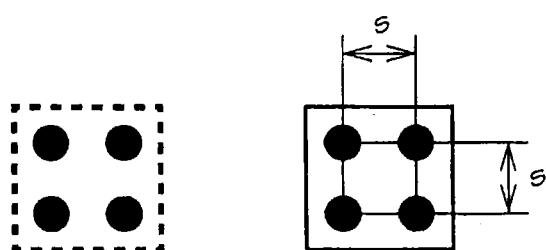


图 5

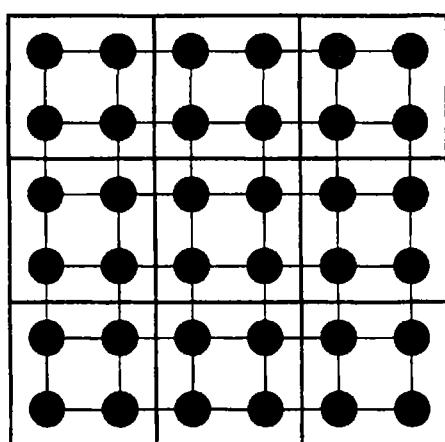


图 6



图 7

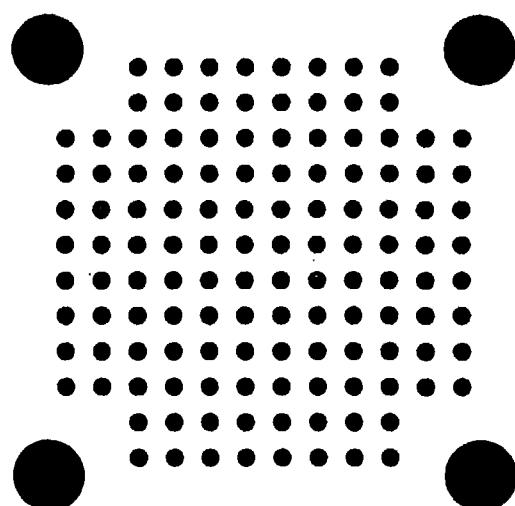


图 8

00	10
01	11

图 9

00	10	00	10	00	10
01	11	01	11	01	11
00	10	00	10	00	10
01	11	01	11	01	11

图 10

A0	D4	I4	D7				
B0	C5	B2	C6	B5	C7		
D1	A6	D5	A3	D5	A2	A4	
B1	C2	B3	C3	B6	C4		
D0	A5	D5	A6	D2	A7		
C0	B4	C1	B7				

图 11

7	6	5	4	3	2	1	0
冗余坐标				数据坐标			
19				数据位 0			

图 12

3	2	1
4	-	0
5	6	7

图 13

<u>oo</u>	π
π	π

图 14

<u>oo</u>	π	<u>oo</u>	π	<u>oo</u>	π
π	π	π	π	π	π
<u>oo</u>	π	<u>oo</u>	π	<u>oo</u>	π
π	π	π	π	π	π

图 15

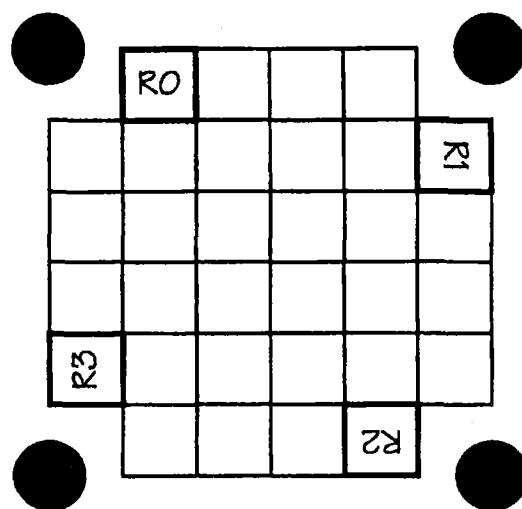


图 16

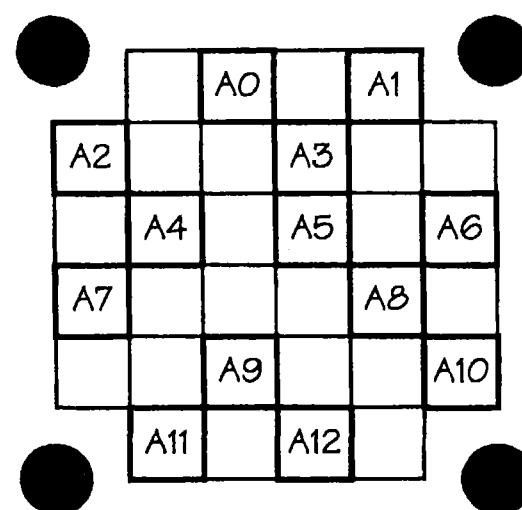


图 17

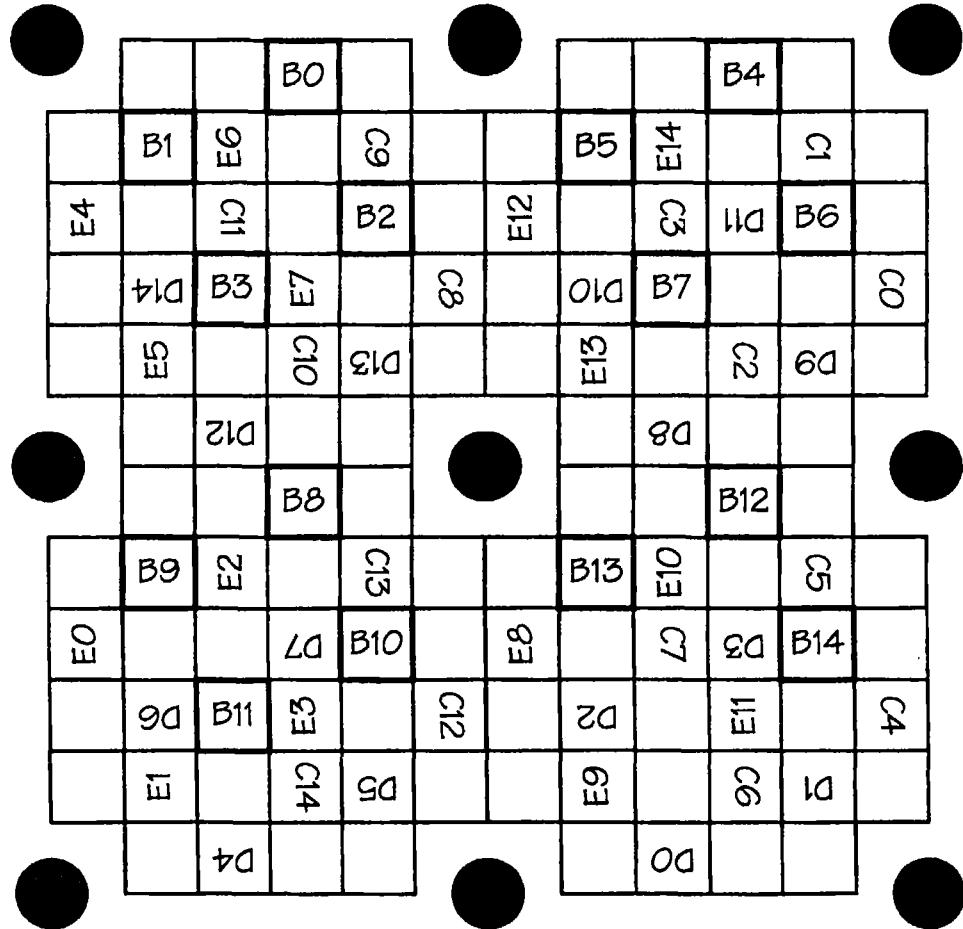


图 18

RO	AO	CO	A1	R3	R1	R2	R3	RO	AO	CO	A1
A2	B1	G	A3	G	E6	A9	B5	A2	C1	B6	A3
E4	A4	C1	A5	B2	A6	C8	A11	A4	D1	A5	B1
R3	E5	C10	D13	E7	B8	E8	R2	R3	R1	E14	E1
R1	A11	A12	E13	A10	R2	A12	R2	R1	D9	D10	R3
A11	B12	A6	R2	D8	A10	D12	A11	R1	A3	C2	E5
R3	C5	A9	E10	B13	A10	R2	R2	R1	D9	D10	R3
A7	B14	D3	C7	A8	E8	B10	D7	A12	B1	C1	E1
C4	A4	E11	A5	D2	A6	G	E9	A12	D1	A3	E0
RO	AO	EO	A1	R3	R1	A11	D5	R3	R1	E1	A2
A2	D1	C6	A3	E9	R1	A11	A11	R3	R1	E4	D4

图 19

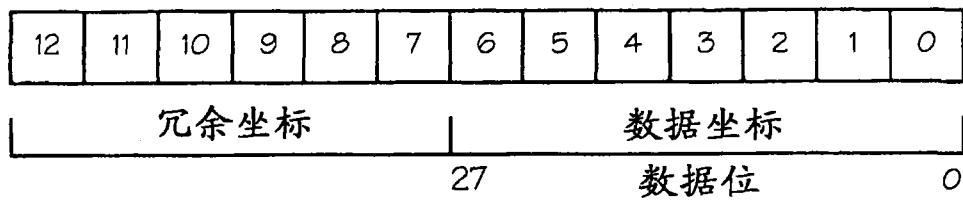


图 20

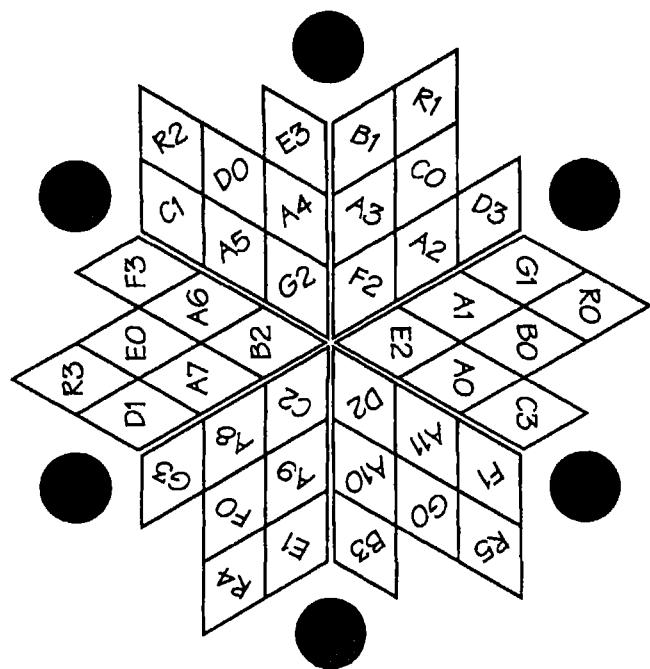


图 21

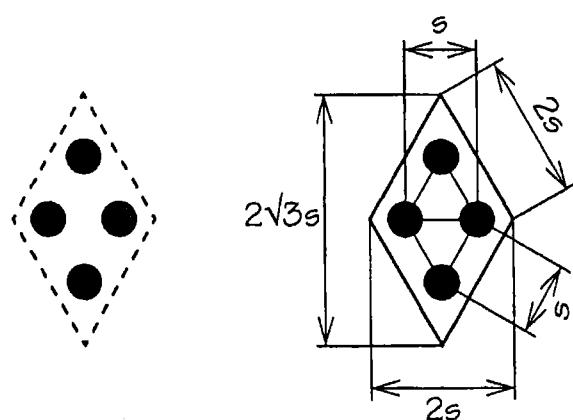


图 22

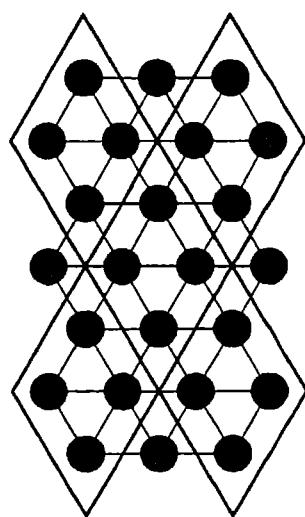


图 23

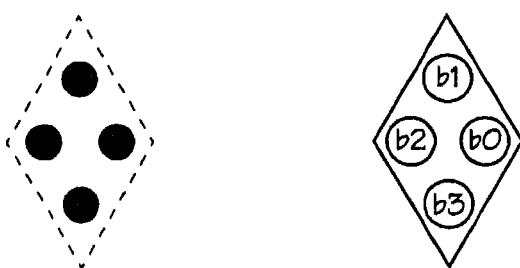


图 24

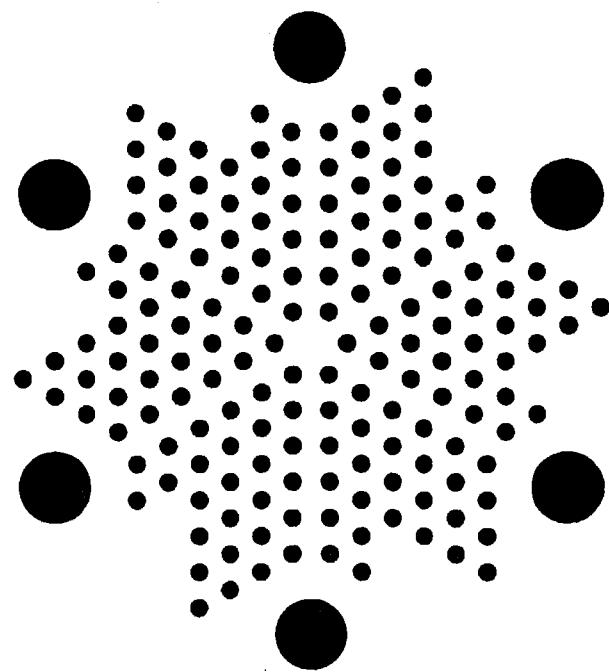


图 25

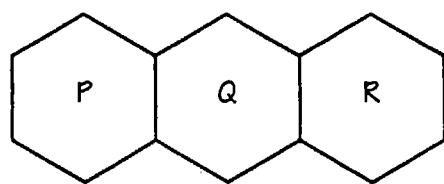


图 26

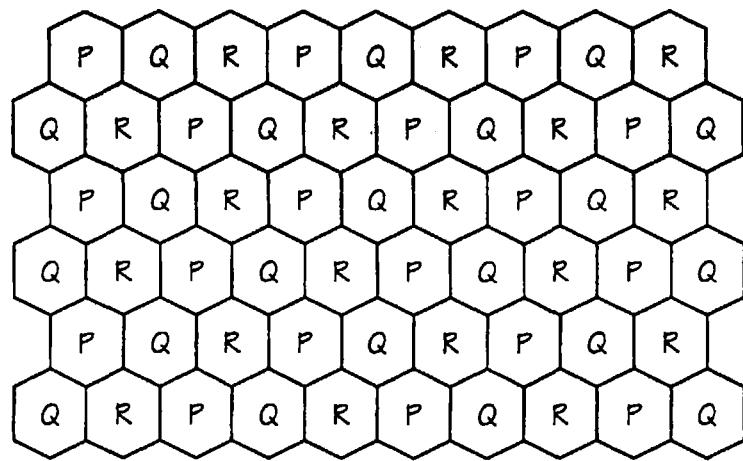


图 27

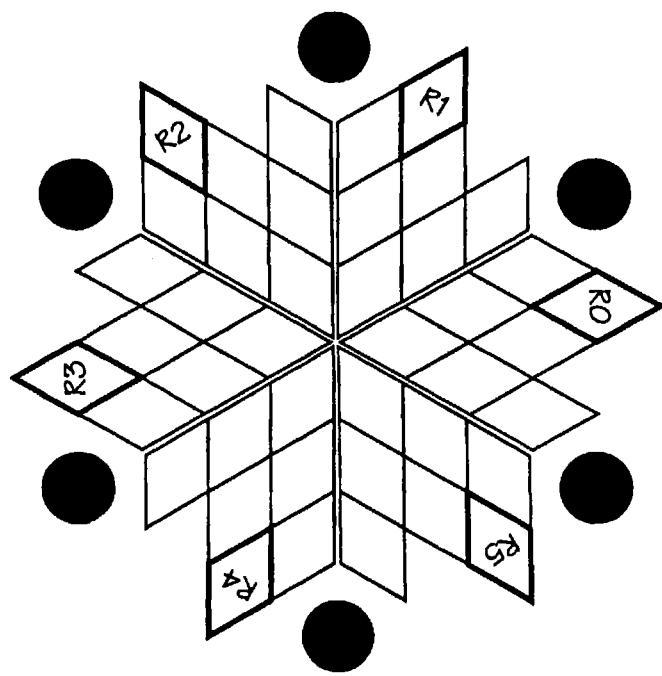


图 28

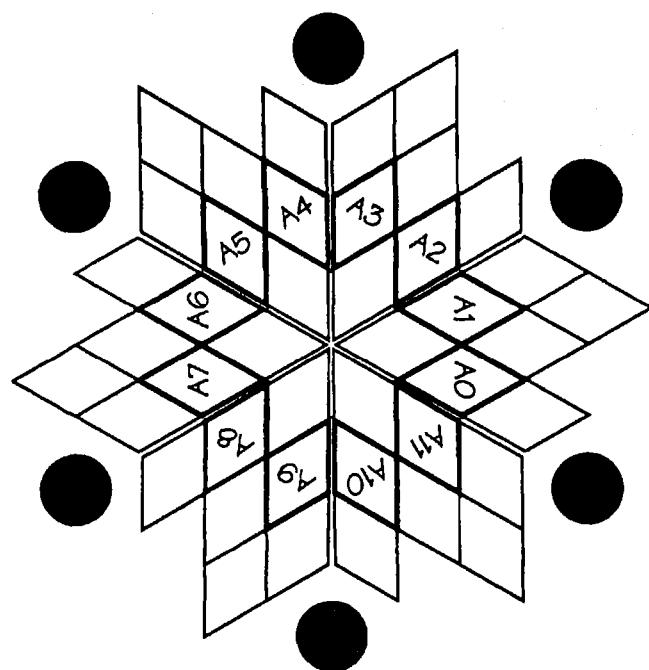


图 29

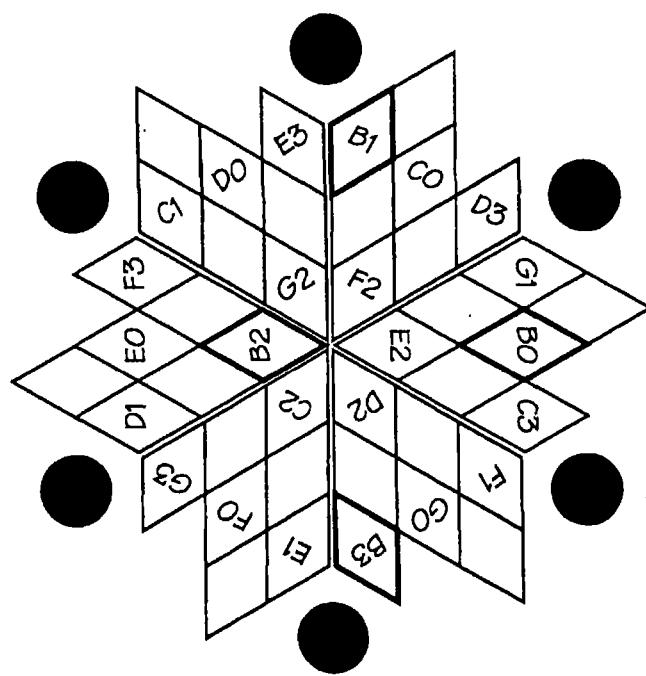


图 30

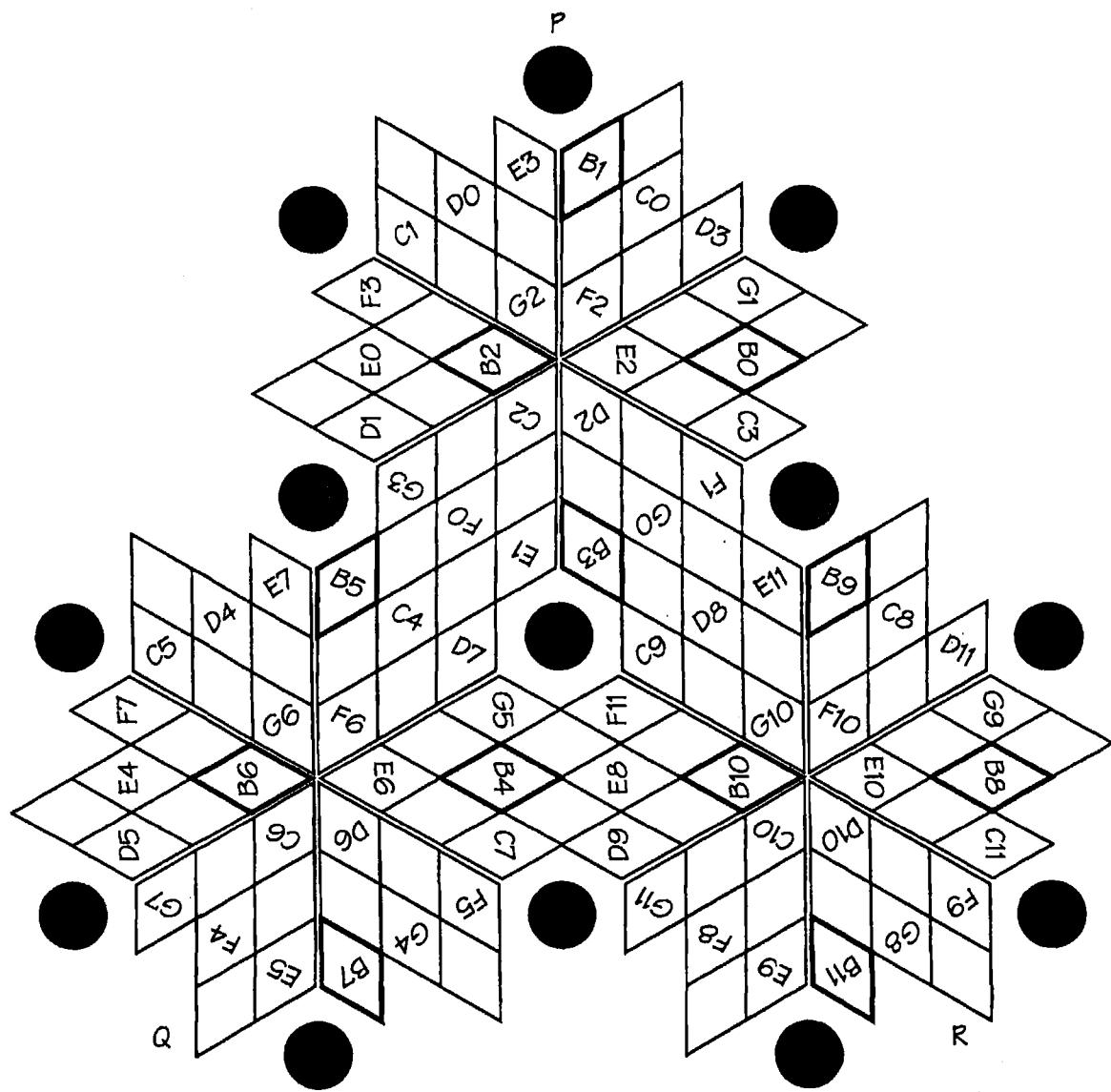


图 31

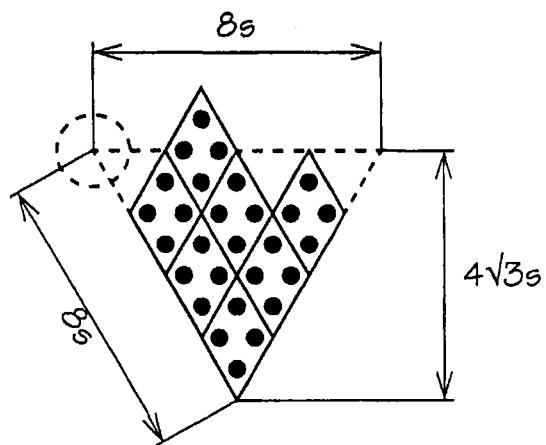


图 32

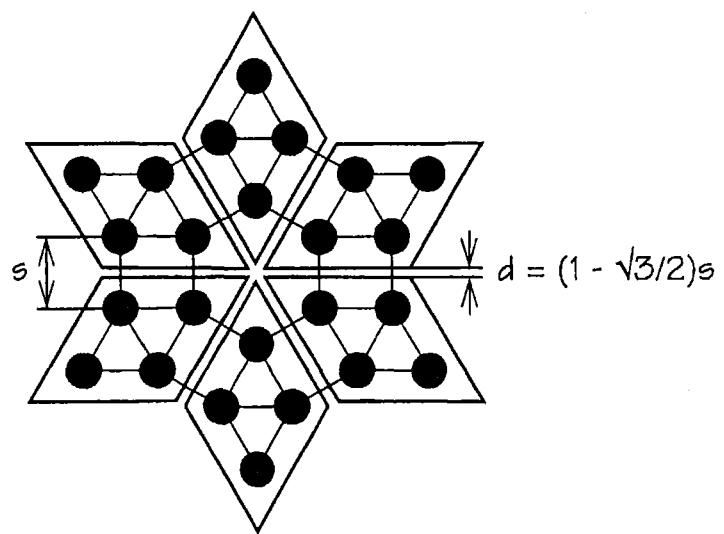


图 33

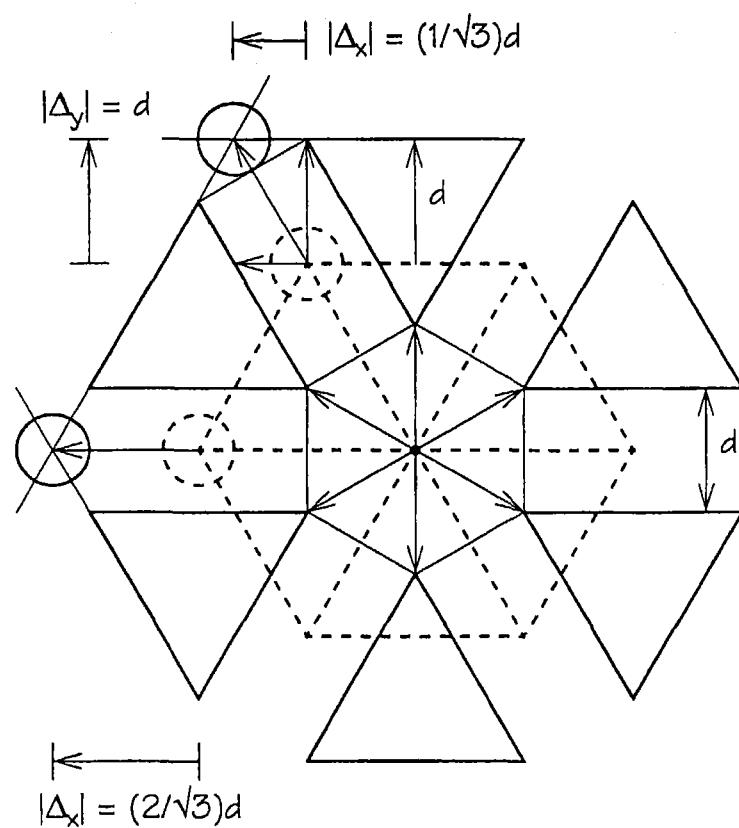


图 34

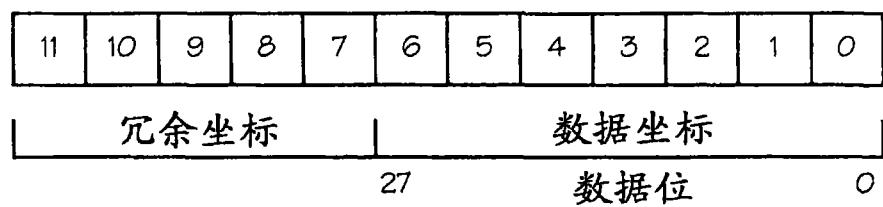


图 35

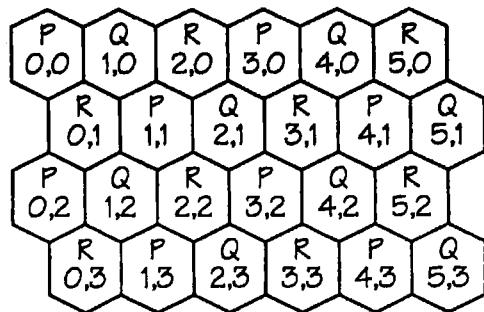


图 36

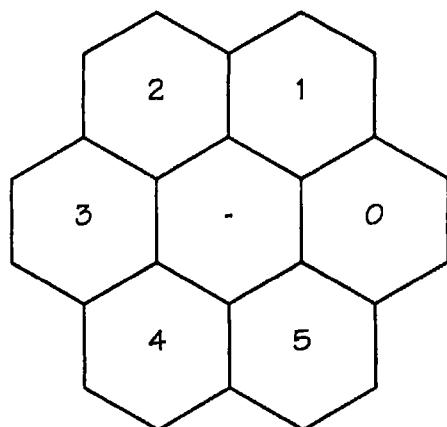


图 37

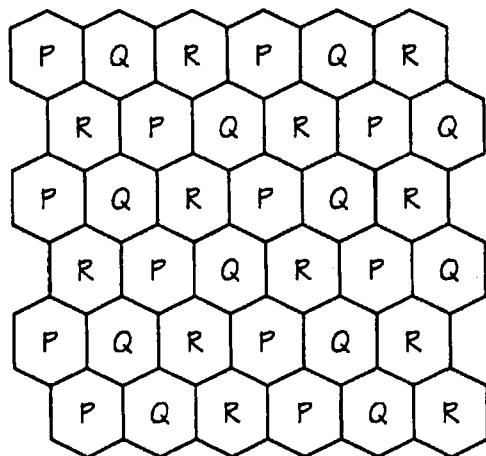


图 38

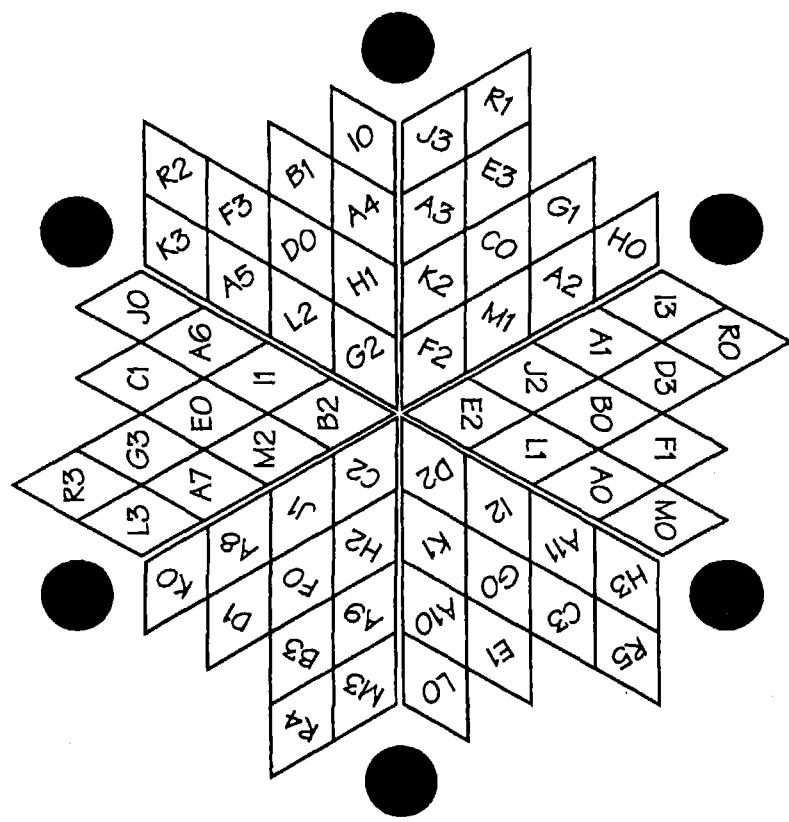


图39

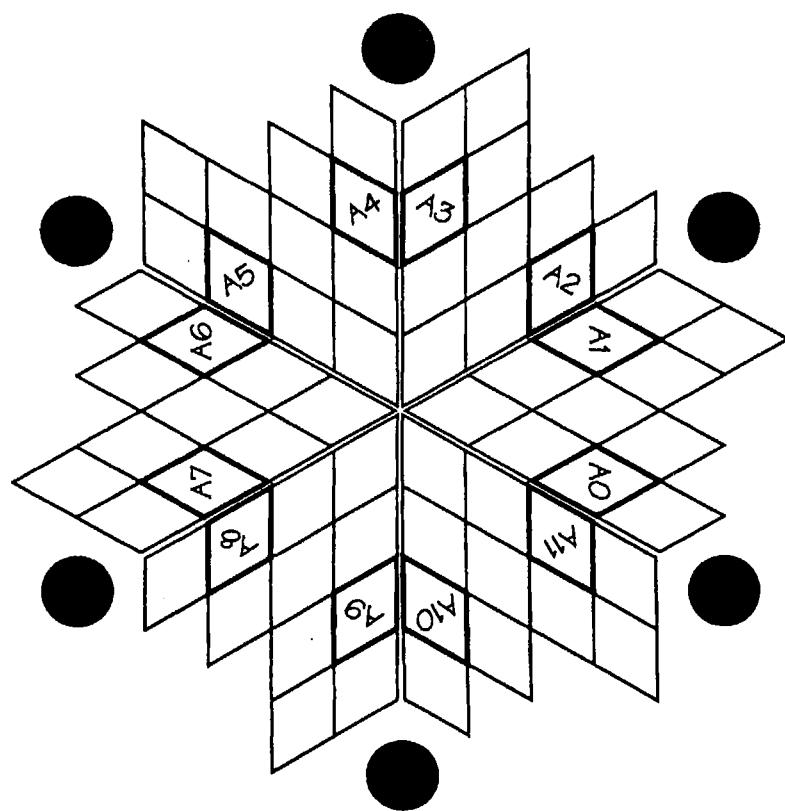


图 40

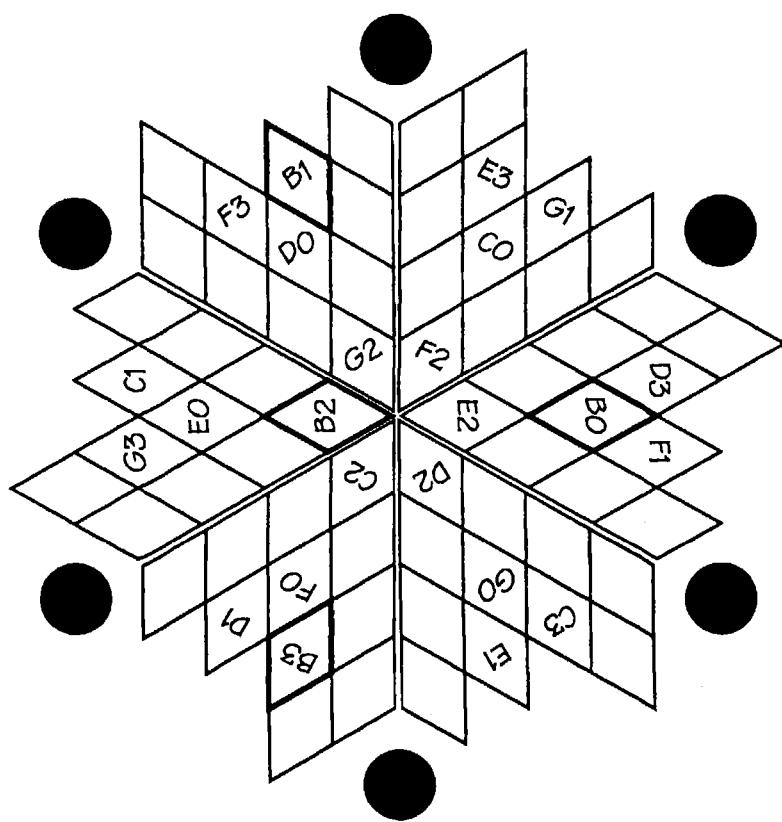


图 41

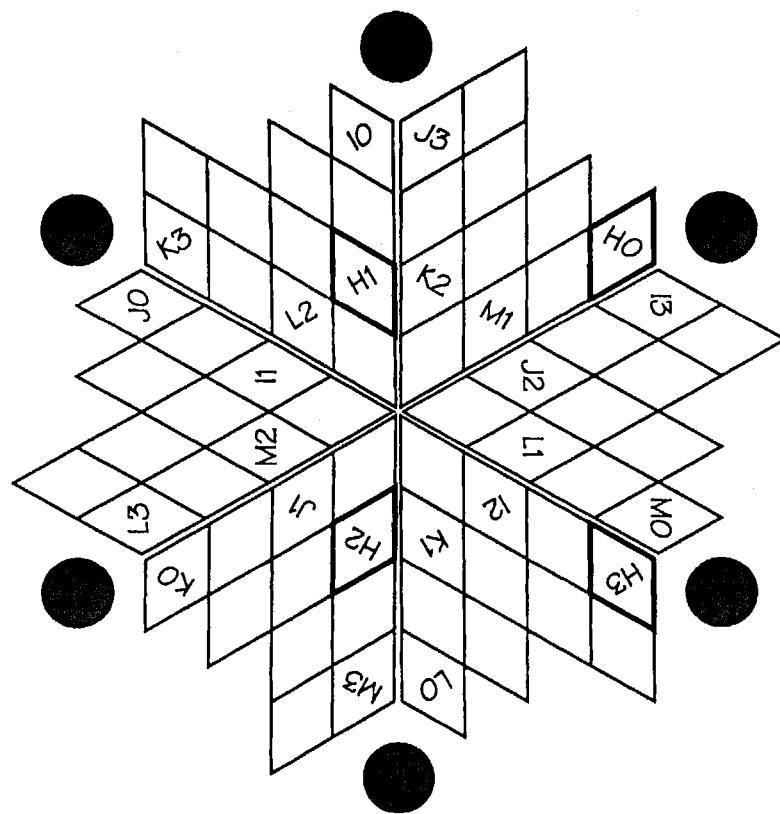


图 42

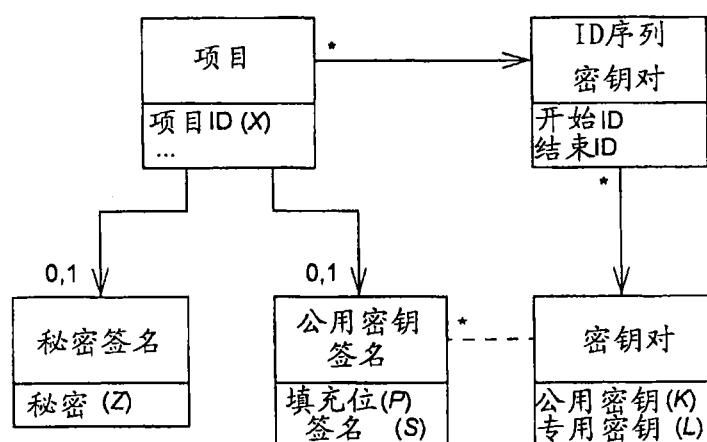


图 43

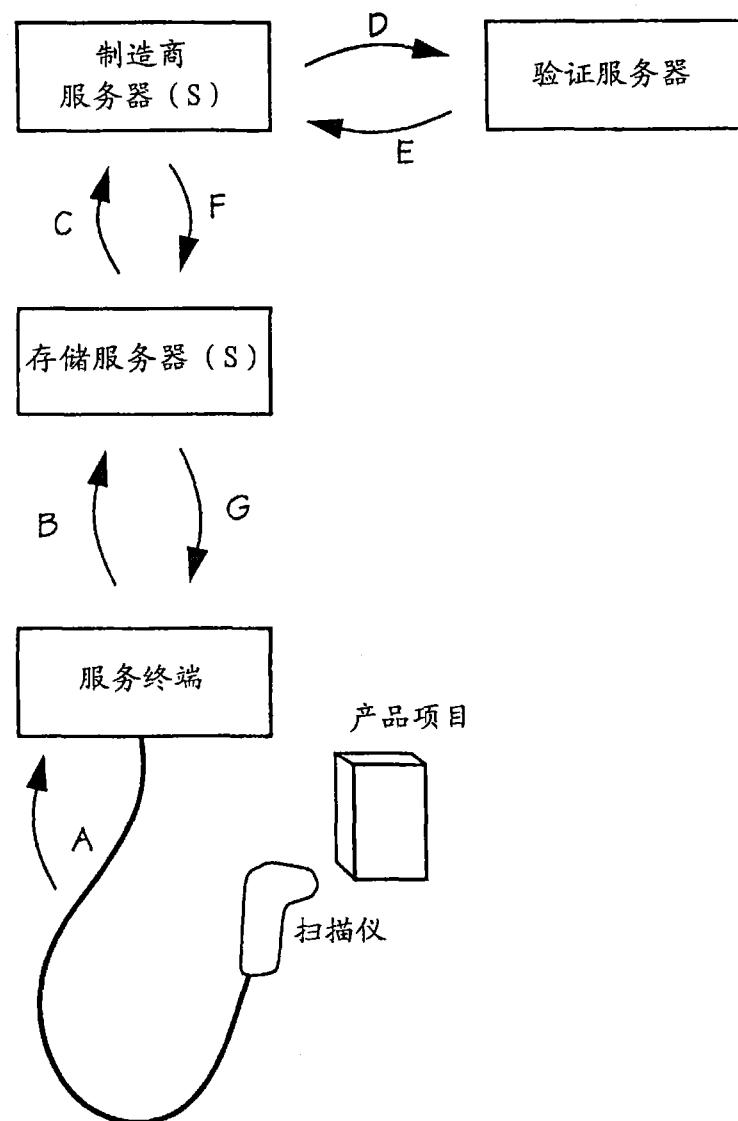


图 44

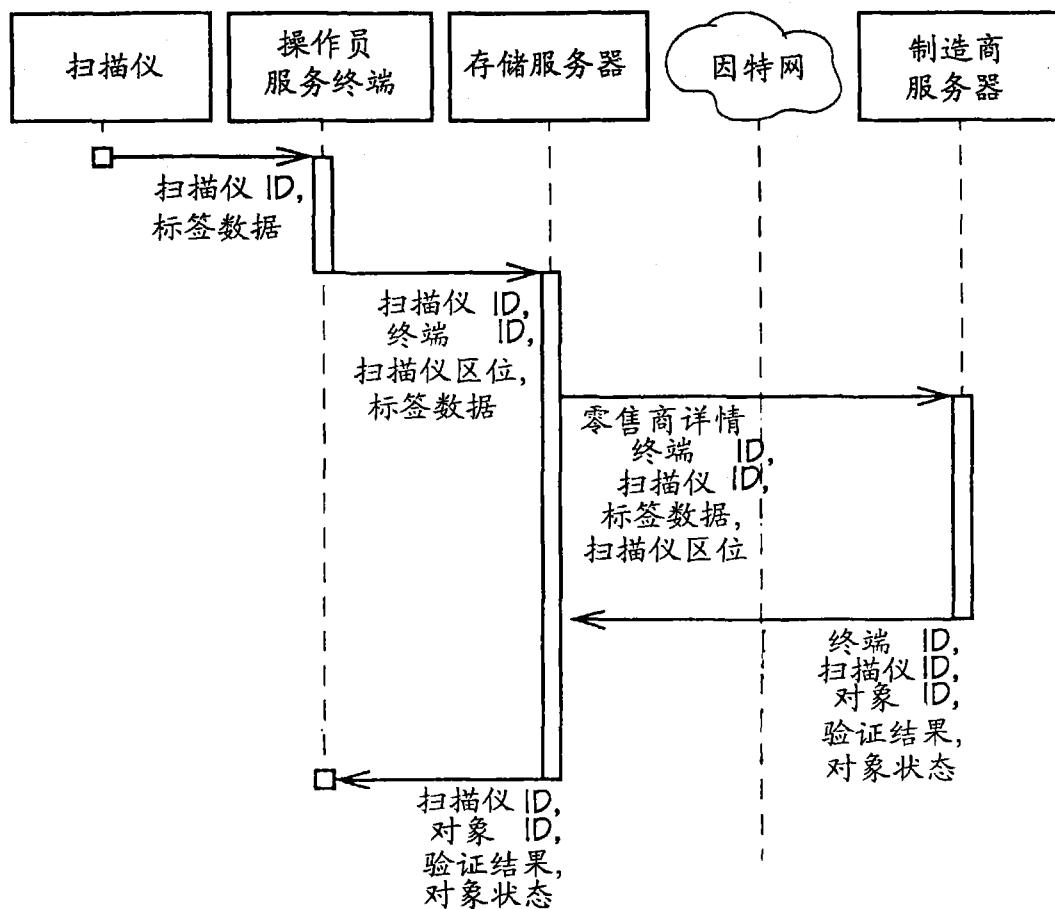


图 45

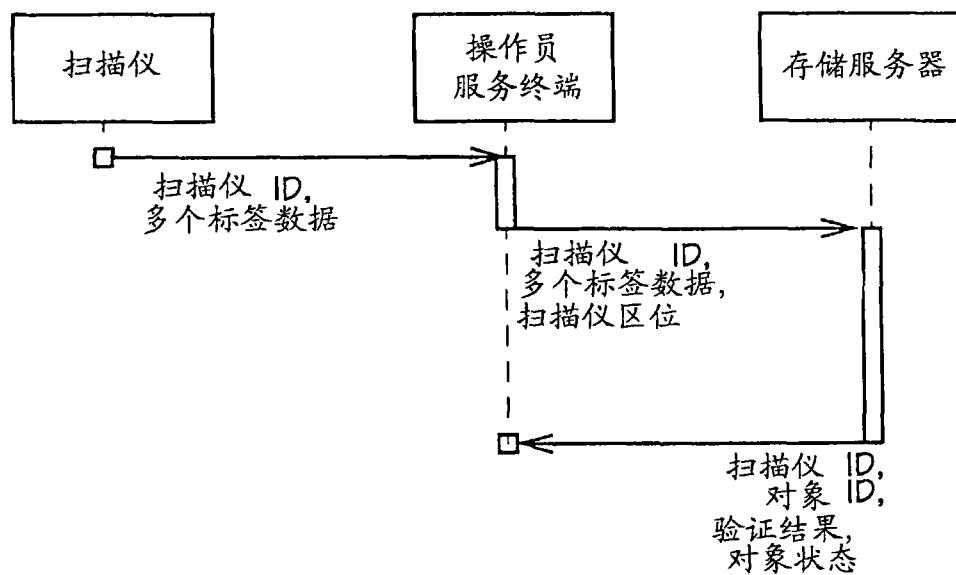


图 46

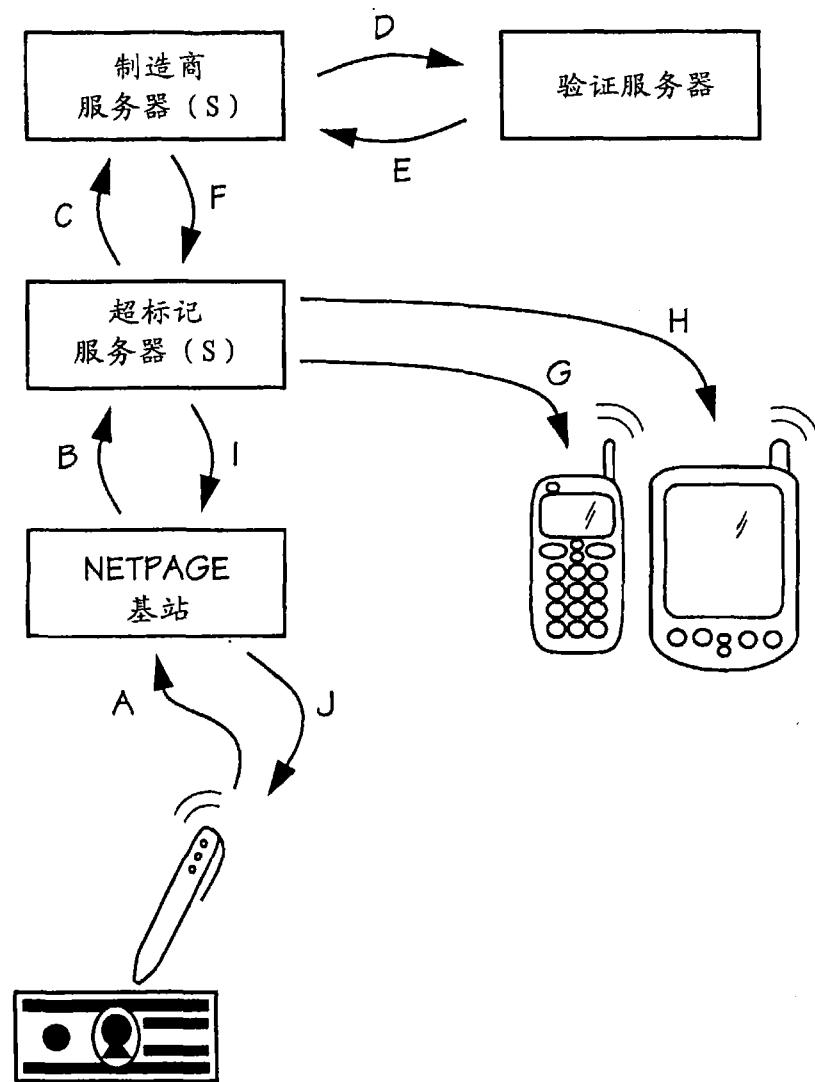


图 47

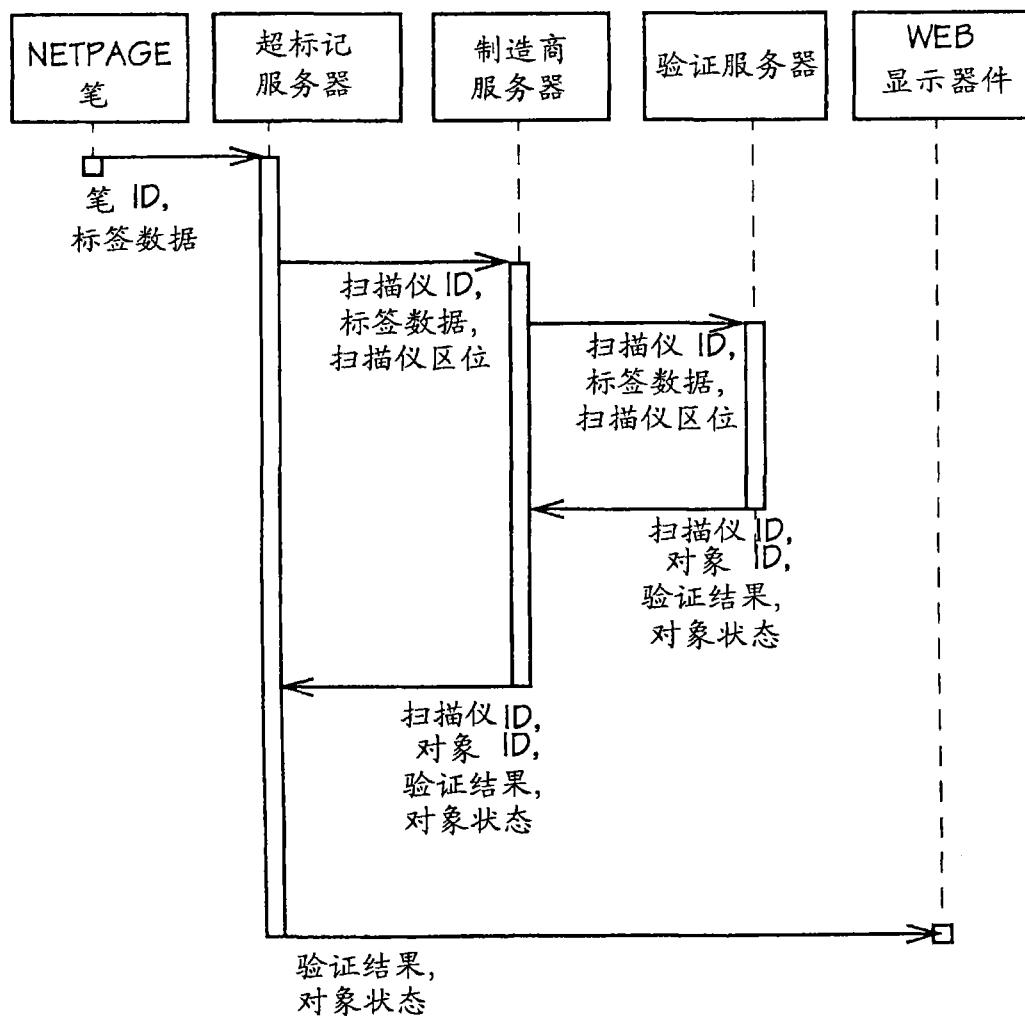


图 48

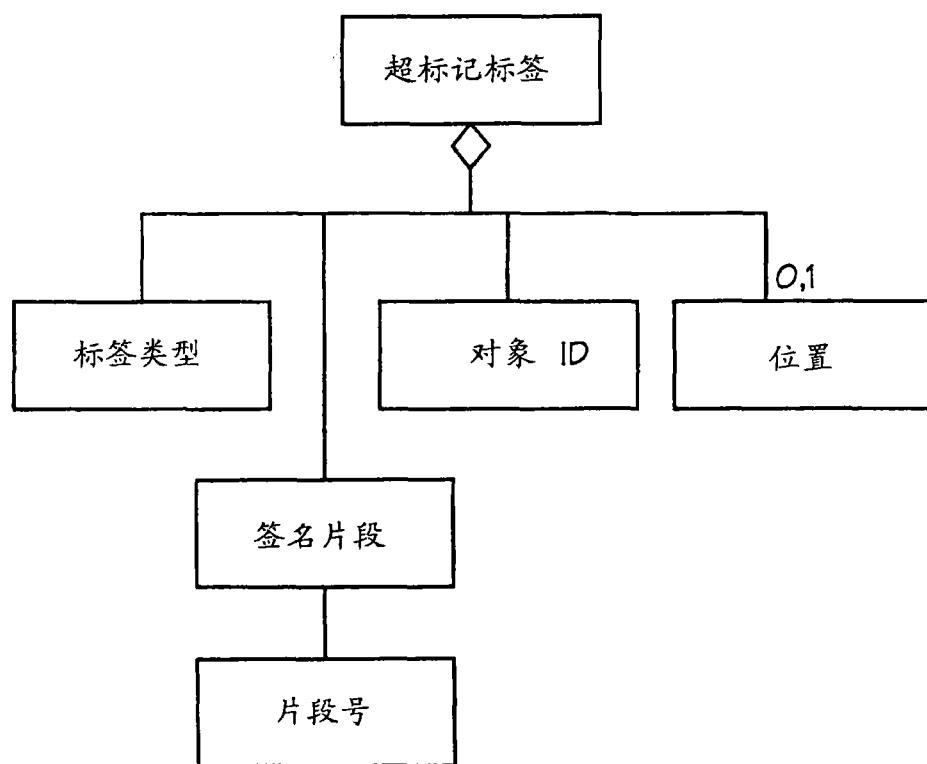


图 49

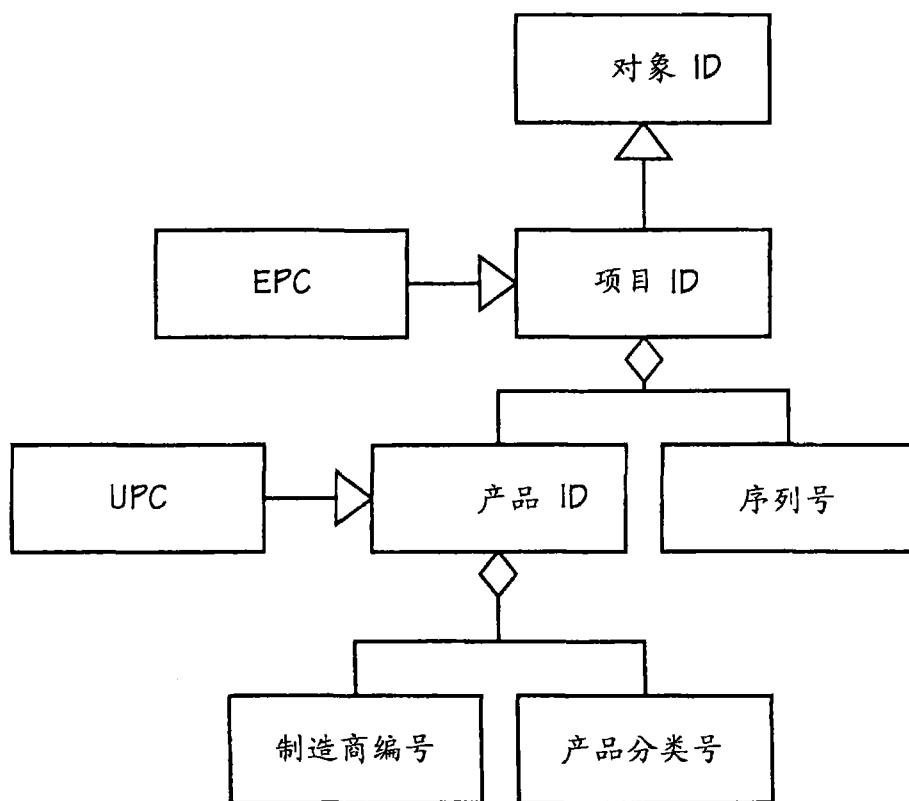


图 50

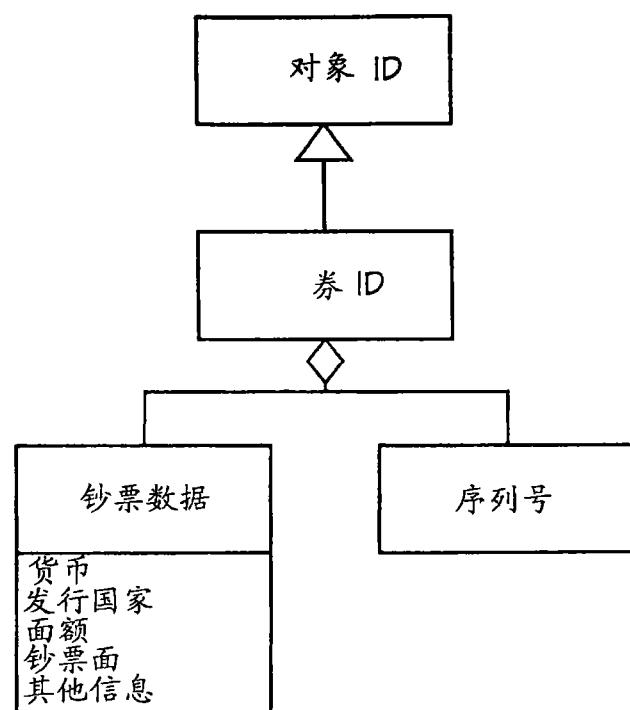


图 51

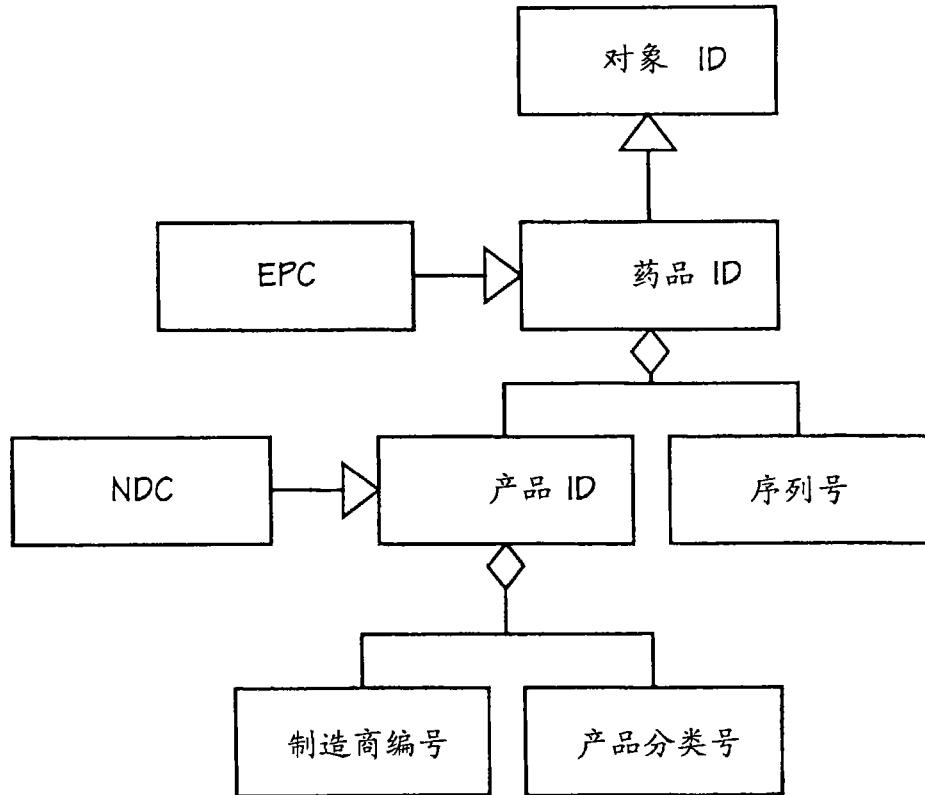


图 52

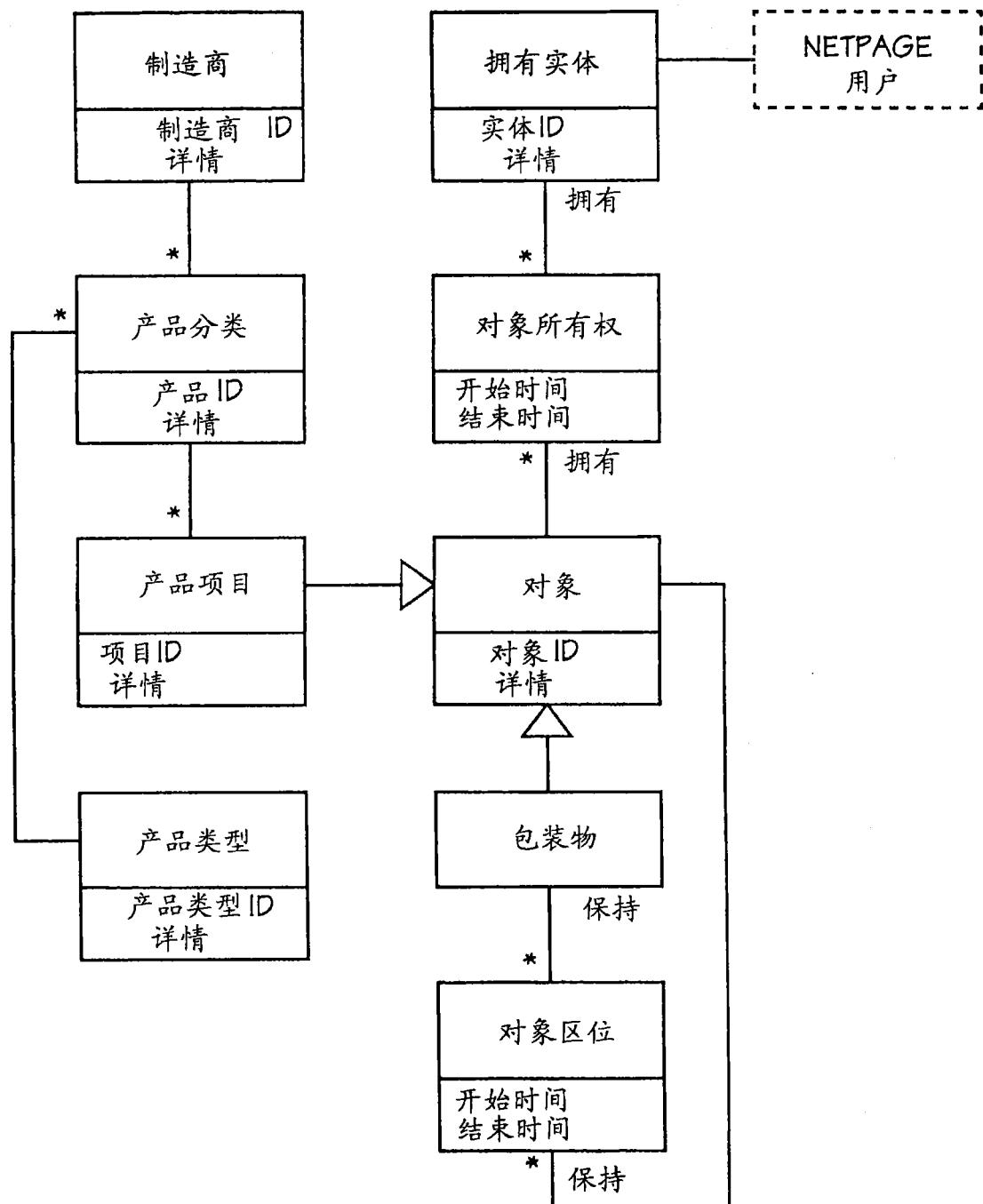


图 53

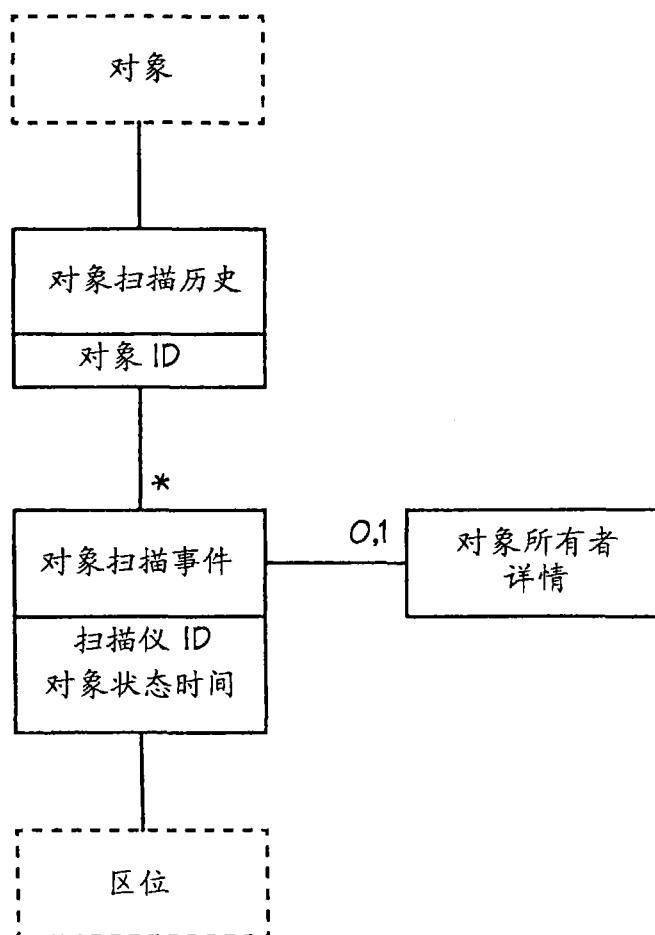


图 54

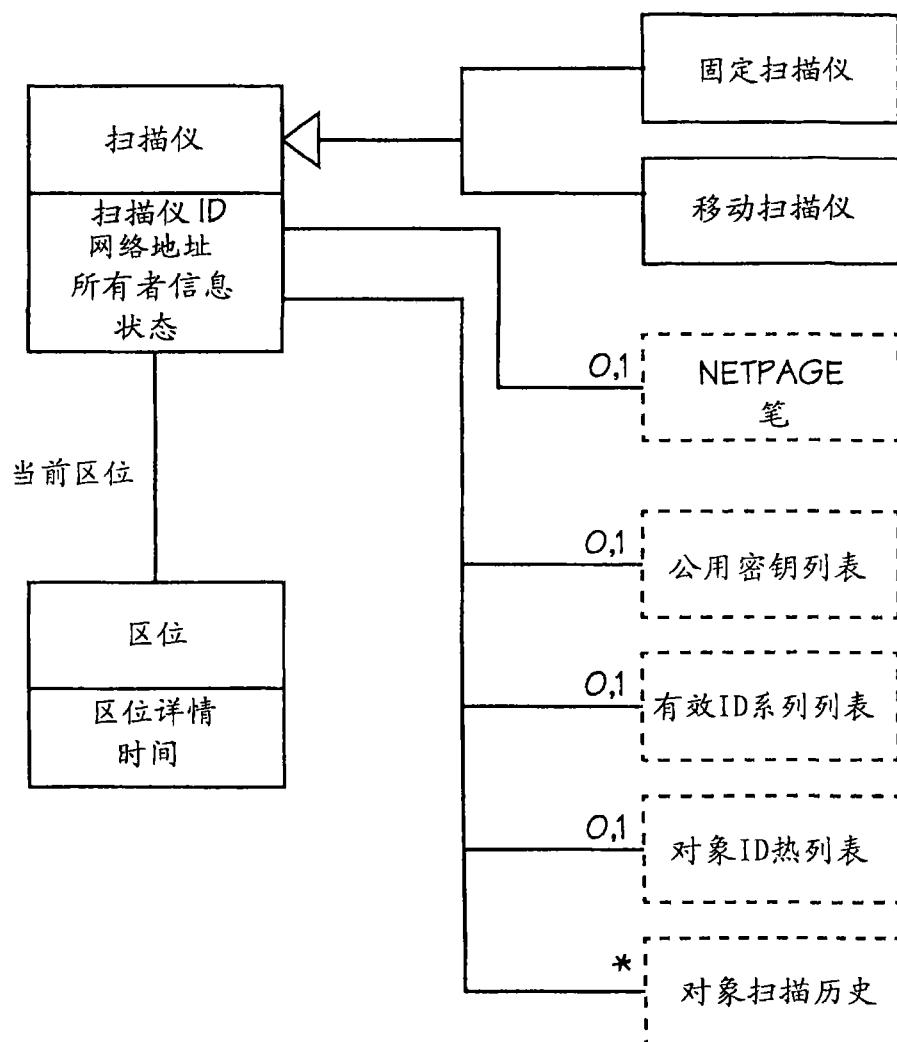


图 55

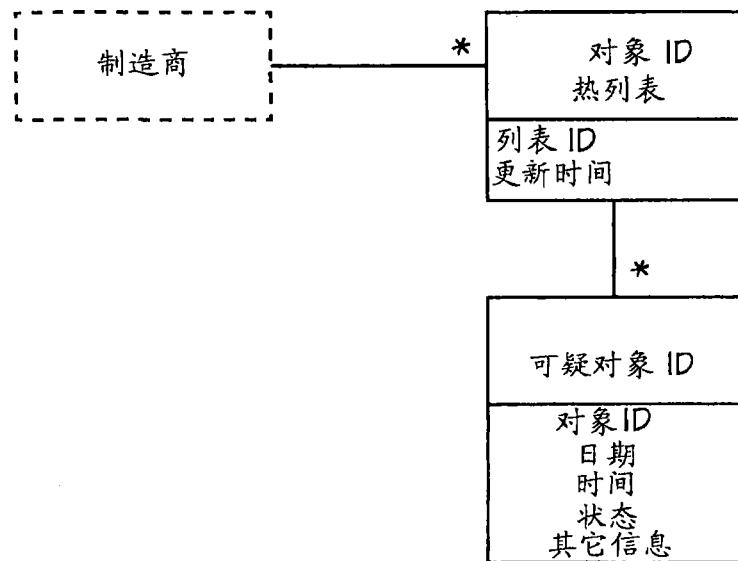


图 56

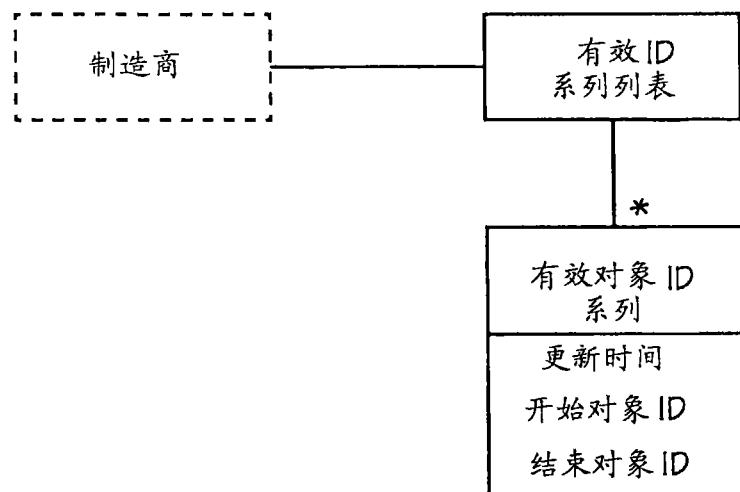


图 57

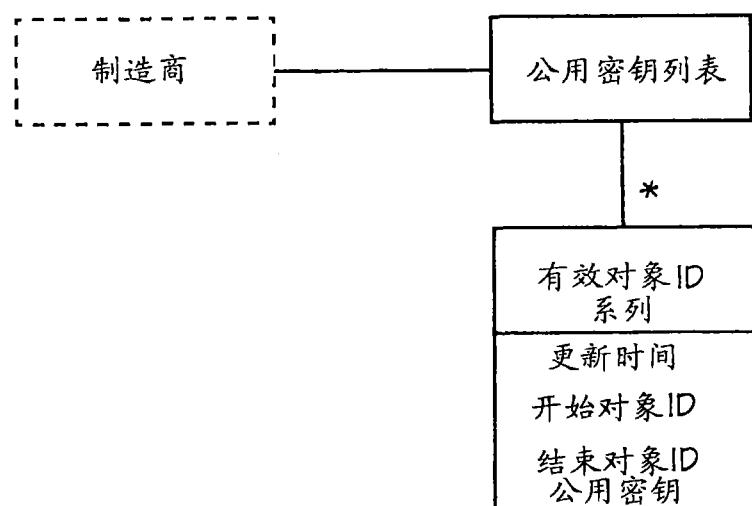


图 58

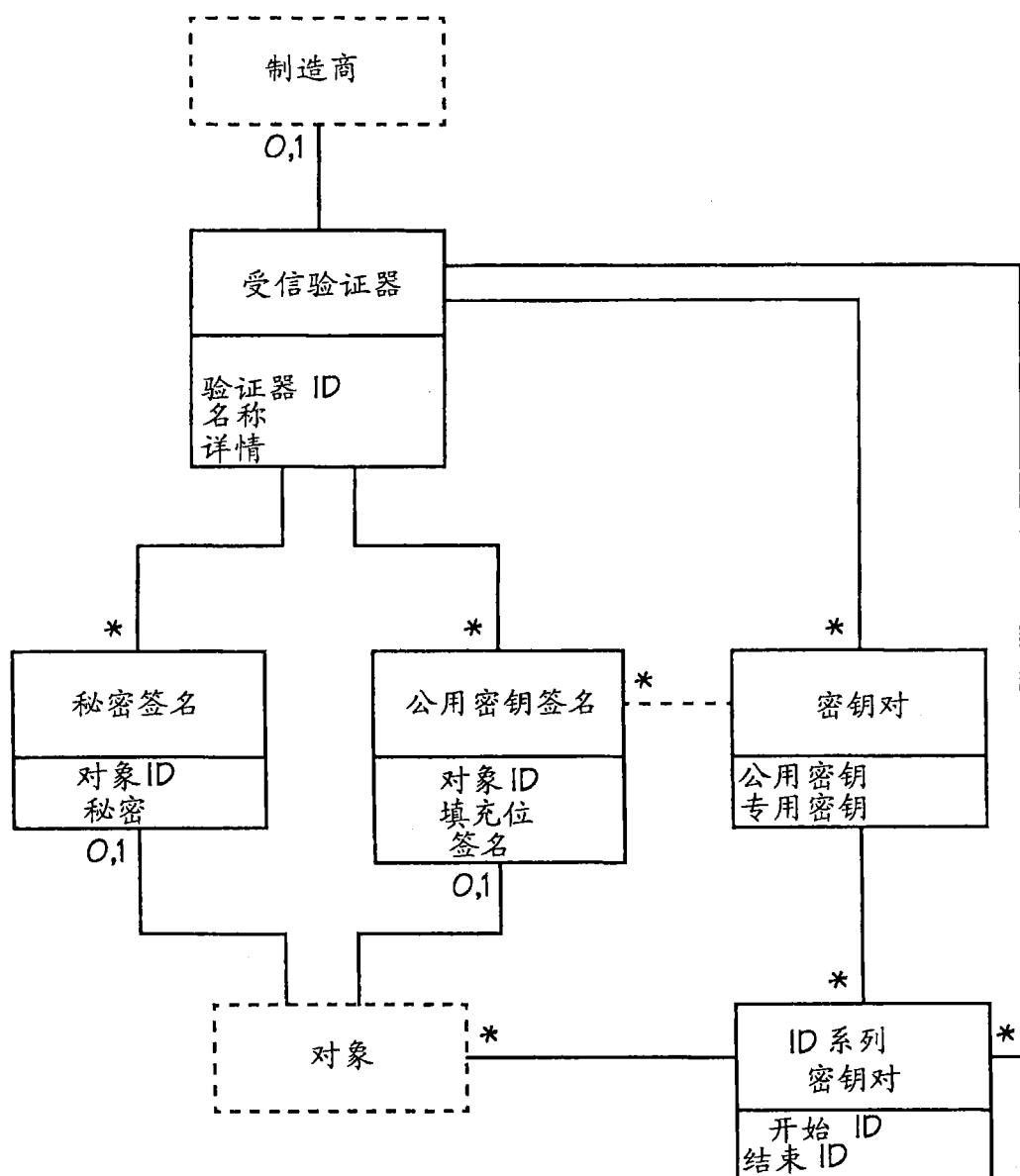


图 59

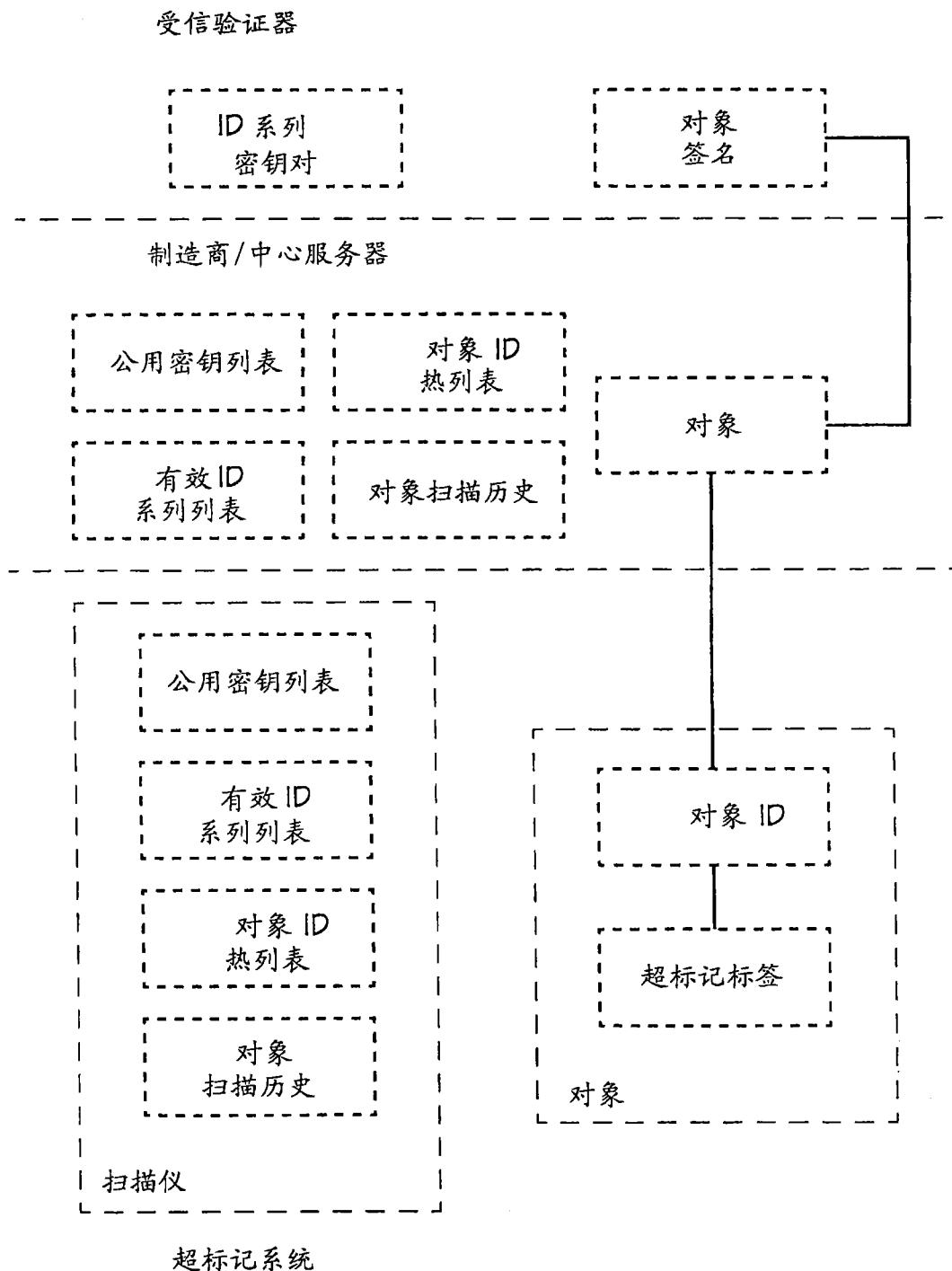


图 60