[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 3/12 (2006.01)
H04L 9/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 03818887.2

[45] 授权公告日 2007 年 7 月 11 日

[11] 授权公告号 CN 1326027C

[22] 申请日 2003.8.6 [21] 申请号 03818887.2

[30] 优先权

[32] 2002. 8. 6 [33] JP [31] 228950/2002

[32] 2003. 7.25 [33] JP [31] 280375/2003

[86] 国际申请 PCT/JP2003/010016 2003.8.6

[87] 国际公布 WO2004/013749 英 2004.2.12

[85] 进入国家阶段日期 2005.2.5

[73] 专利权人 佳能株式会社

地址 日本东京

[72] 发明人 皆川智德

[56] 参考文献

CN1332405A 2002.1.23

EP1100003A2 2001.5.16

审查员 徐 薇

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

代理人 董 莘

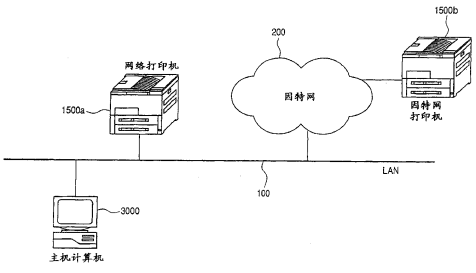
权利要求书 9 页 说明书 25 页 附图 23 页

[54] 发明名称

具有数据加密和解密的打印数据通信

[57] 摘要

本发明公开了一种打印控制装置，用于将包含打印数据的打印作业通过通信媒体传输到指定的成像装置，并且控制所述指定的成像装置以打印所述打印数据，所述打印控制装置包括：获取单元，用于在加密状态从所述成像装置获取关于邮件方法的目的地的信息，其中所述邮件方法是被远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；解密单元，用于解密所述获取单元获取的关于目的地的信息；以及传输单元，用于借助所述邮件方法，将所述打印数据传输到由所述解密单元解密的信息所指示的目的地，其中根据 HTTP 协议执行所述传输。



1、一种打印控制装置，用于将包含打印数据的打印作业通过通信媒体传输到指定的成像装置，并且控制所述指定的成像装置以打印所述打印数据，所述打印控制装置包括:

获取单元，用于在加密状态从所述成像装置获取关于邮件方法的目的地的信息，其中所述邮件方法是被远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程;

解密单元，用于解密所述获取单元获取的关于目的地的信息；以及

传输单元，用于借助所述邮件方法，将所述打印数据传输到由所述解密单元解密的信息所指示的目的地，其中根据 **HTTP** 协议执行所述传输。

2、根据权利要求 1 的打印控制装置，还包括:

特征数量计算单元，用于根据所述打印数据计算特征数量；以及

打印作业传输单元，用于将所述特征数量计算单元计算的特征数量包含在打印作业中，并且将所述特征数量通过所述通信媒体传输到所述指定的成像装置。

3、根据权利要求 1 的打印控制装置，其中由所述获取单元获取的关于目的地的信息是统一资源标识符（**URI**）。

4、根据权利要求 1 的打印控制装置，还包括打印数据加密单元，用于在打印所述打印作业时，以指定的加密方法加密所述打印数据，

其中所述打印数据加密单元用作基于公共密钥密码系统而执行加密的公共密钥加密单元，并且基于所述公共密钥密码系统，利用为打印所述打印数据而指定的成像装置的公共密钥，加密所述打印数据。

5、根据权利要求 4 的打印控制装置，还包括:

保密密钥产生单元，用于产生由为打印所述打印数据而指定的成像装置共同使用的保密密钥;

保密密钥加密单元，用于加密由所述保密密钥产生单元所产生的保密密钥；以及

打印作业传输单元，用于将由所述保密密钥加密单元所加密的保密密钥包含在所述打印作业中，并且将所述密钥传输到所述通信媒体，其中:

所述打印数据加密单元用作基于常规加密系统而执行加密的公共密钥加密单元，并且基于所述常规加密系统，利用所述保密密钥产生单元所产生的保密密钥，加密所述打印数据；以及

所述保密密钥加密单元用作基于所述公共密钥密码系统而执行加密的公共密钥加密单元，基于所述公共密钥密码系统执行加密，并且利用为打印所述打印数据而指定的成像装置的公共密钥，加密所述保密密钥。

6、根据权利要求 2 的打印控制装置，还包括:

数字签名产生单元，用于通过对于由所述特征数量计算单元所计算的特征数量执行基于公共密钥密码系统的加密，并且利用所述数字签名产生单元的专用密钥，加密所述特征数量，产生数字签名，其中:

所述打印作业传输单元将由所述数字签名产生单元所产生的数字签名、而不是将由所述特征数量计算单元计算的特征数量包含在所述打印作业中，并且将所述打印作业传输到所述通信媒体。

7、根据权利要求 4 的打印控制装置，还包括:

成像装置选择单元，用于通过向管理关于所述成像装置的信息的成像装置管理服务器发布查询，从包括多个成像装置的组中选择用于打印所述打印数据的成像装置；以及

成像装置信息获取单元，用于从所述成像装置管理服务器获取关

于为打印所述打印数据而指定的成像装置的信息。

8、根据权利要求 7 的打印控制装置，其中：

所述成像装置信息获取单元从所述成像装置管理服务器获取为打印所述打印数据而指定的成像装置的加密密钥和地址；以及

所述打印数据加密单元使用由所述成像装置信息获取单元获取的成像装置的密钥，加密所述打印数据，并且将所述加密后的打印数据直接传输到由所述成像装置信息获取单元获取的成像装置的地址。

9、根据权利要求 7 的打印控制装置，其中：

所述打印数据加密单元获取所述成像装置管理服务器的加密密钥，加密所述打印数据，并且将所述加密后的打印数据传输到所述成像装置管理服务器。

10、根据权利要求 7 的打印控制装置，其中：

通过所述成像装置信息获取单元将这样的必需条件传输给所述成像装置管理服务器，所述成像装置选择单元从包括多个成像装置的组中选择相应的成像装置，其中所述必需条件是所述成像装置选择单元从包括多个成像装置的组中选择相应的成像装置所必需的条件。

11、根据权利要求 7 的打印控制装置，其中：

通过所述成像装置信息获取单元将这样的必需条件传输给所述服务器，即所述必需条件是所述成像装置管理服务器从包括多个成像装置的组中粗略地选择相应的成像装置所必需的条件，所述成像装置管理服务器从包括多个成像装置的组中粗略地选择相应的成像装置，并且

已经从所述包括多个成像装置的组中粗略地选择相应成像装置的成像装置管理服务器与所述成像装置选择单元交互地通信，由此从所述包括多个成像装置的组中选择用于打印所述打印数据的成像装

置。

12、一种成像装置，用于打印包含在通过通信媒体接收的打印作业中的加密的打印数据，包括：

传输单元，用于加密和传输关于邮件方法的目的地的信息，所述邮件方法是远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；以及

设置单元，响应于关于目的地的信息的传输，设置所述成像装置可以接受来自远程源端的邮件方法的条件。

13、根据权利要求 12 的成像装置，还包括：

打印数据解密单元，用于解密所述加密的打印数据；

特征数量获取单元，用于从所述接收的打印作业中获取特征数量；

特征数量计算单元，用于根据由所述打印数据解密单元解密的打印数据，计算特征数量；以及

打印数据确认单元，用于比较由所述特征数量计算单元计算的特征数量与所述特征数量获取单元获取的特征数量，并且如果比较结果指示这两个特征数量彼此匹配，则确认所述加密并被接收的打印数据没有被改变。

14、根据权利要求 13 的成像装置，还包括：

保密密钥检索单元，用于从所述接收的打印作业中检索加密的保密密钥；以及

保密密钥获取单元，用于基于公共密钥密码系统，对从所述保密密钥检索单元中检索出的加密的保密密钥执行解密，利用所述保密密钥获取单元的专用密钥来解密所述加密的保密密钥，并且获得所述打印作业的保密密钥，其中：

所述打印数据解密单元用作基于常规加密系统而执行解密的公

共密钥解密单元，应用所述常规加密系统，以利用所述保密密钥来解密所述加密的打印数据，并且获得打印数据。

15、根据权利要求13的成像装置，还包括：

数字签名检索单元，用于从所述接收的打印作业中检索数字签名，其中：

所述特征数量获取单元通过基于公共密钥解密方法，利用所述打印作业的源端的公共密钥，解密由所述数字签名检索单元检索出的数字签名，从而获得特征数量；

所述打印数据确认单元比较根据所述打印数据解密单元解密的打印数据而计算出的特征数量与由所述特征数量获取单元获得的特征数量，确认这些特征数量相互匹配，由此确认所述源端是指定的成像装置驱动程序，并且所述加密并被接收的打印数据没有被改变。

16、一种打印控制方法，用于将包含打印数据的打印作业通过通信媒体传输到指定的成像装置，并且控制所述指定的成像装置以打印所述打印数据，所述打印控制方法包括：

获取单元在加密状态从所述成像装置获取关于邮件方法的目的地的信息，其中所述邮件方法是被远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；

解密单元解密所述获取单元获取的关于目的地的信息；以及

传输装置将所述打印数据传输到借助所述邮件方法由所述解密装置解密的信息所指示的目的地，其中根据HTTP协议执行所述传输。

17、根据权利要求16的打印控制方法，还包括：

特征数量计算单元根据所述打印数据计算特征数量；以及

打印作业传输单元将所述特征数量计算单元计算的特征数量包含在打印作业中，并且将所述特征数量通过所述通信媒体传输到所述指定的成像装置。

18、根据权利要求 16 的打印控制方法，其中关于由所述获取单元获取的目的地的信息是统一资源标识符（URI）。

19、根据权利要求 16 的打印控制方法，还包括:

打印数据加密单元在打印所述打印作业时，以指定的加密方法加密所述打印数据，

其中所述打印数据加密单元用作基于公共密钥密码系统而执行加密的公共密钥加密单元，并且基于所述公共密钥密码系统，利用为打印所述打印数据而指定的成像装置的公共密钥，加密所述打印数据。

20、根据权利要求 19 的打印控制方法，还包括:

保密密钥产生单元产生由为打印所述打印数据而指定的成像装置共同使用的保密密钥;

保密密钥加密单元加密由所述保密密钥产生单元所产生的保密密钥；以及

打印作业传输单元将由所述保密密钥加密单元所加密的保密密钥包含在所述打印作业中，并且将所述密钥传输到所述通信媒体，其中:

所述打印数据加密单元用作基于常规加密系统而执行加密的公共密钥加密单元，并且基于所述常规加密系统，利用所述保密密钥产生单元所产生的保密密钥，加密所述打印数据；以及

所述保密密钥加密单元用作基于所述公共密钥密码系统而执行加密的公共密钥加密单元，基于所述公共密钥密码系统执行加密，并且利用为打印所述打印数据而指定的成像装置的公共密钥，加密所述保密密钥。

21、根据权利要求 17 的打印控制方法，还包括:

数字签名产生单元通过对于由所述特征数量计算单元所计算的

特征数量执行基于公共密钥密码系统的加密，并且利用所述数字签名产生单元的专用密钥，加密所述特征数量，产生数字签名，其中：

所述打印作业传输单元将由所述数字签名产生单元所产生的数字签名、而不是将由所述特征数量计算单元计算的特征数量包含在所述打印作业中，并且将所述打印作业传输到所述通信媒体。

22、根据权利要求 19 的打印控制方法，还包括：

成像装置选择单元通过向管理关于所述成像装置的信息的成像装置管理服务器发布查询，从包括多个成像装置的组中选择用于打印所述打印数据的成像装置；以及

成像装置信息获取单元从所述成像装置管理服务器获取关于为打印所述打印数据而指定的成像装置的信息。

23、根据权利要求 22 的打印控制方法，其中：

所述成像装置信息获取单元从所述成像装置管理服务器获取为打印所述打印数据而指定的成像装置的加密密钥和地址；以及

所述打印数据加密单元使用由所述成像装置信息获取单元获取的成像装置的密钥，加密所述打印数据，并且将所述加密后的打印数据直接传输到由所述成像装置信息获取单元获取的成像装置的地址。

24、根据权利要求 22 的打印控制方法，其中：

所述打印数据加密单元获取所述成像装置管理服务器的加密密钥，加密所述打印数据，并且将所述加密后的打印数据传输到所述成像装置管理服务器。

25、根据权利要求 22 的打印控制方法，其中：

通过所述成像装置信息获取单元将这样的必需条件传输给所述成像装置管理服务器，所述成像装置选择单元从包括多个成像装置的组中选择相应的成像装置，其中所述必需条件是所述成像装置选择单

元从包括多个成像装置的组中选择相应的成像装置所必需的条件。

26、根据权利要求 22 的打印控制方法，其中：

通过所述成像装置信息获取单元将这样的必需条件传输给所述服务器，即所述必需条件是所述成像装置管理服务器从包括多个成像装置的组中粗略地选择相应的成像装置所必需的条件，所述成像装置管理服务器从包括多个成像装置的组中粗略地选择相应的成像装置，并且

已经从所述包括多个成像装置的组中粗略地选择相应成像装置的成像装置管理服务器与所述成像装置选择单元交互地通信，由此从所述包括多个成像装置的组中选择用于打印所述打印数据的成像装置。

27、一种成像方法，用于打印包含在通过通信媒体接收的打印作业中的加密的打印数据，包括：

传输单元加密和传输关于邮件方法的目的地的信息，所述邮件方法是远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；以及

设置单元响应于关于目的地的信息的传输，设置所述成像装置可以接受来自远程源端的邮件方法的条件。

28、根据权利要求 27 的成像方法，还包括：

打印数据解密单元解密所述加密的打印数据；

特征数量获取单元从所述接收的打印作业中获取特征数量；

特征数量计算单元根据由所述打印数据解密单元解密的打印数据，计算特征数量；以及

打印数据确认单元比较由所述特征数量计算单元计算的特征数量与所述特征数量获取单元获取的特征数量，并且如果比较结果指示这两个特征数量彼此匹配，则确认所述加密并被接收的打印数据没有

被改变。

29、根据权利要求28的成像方法，还包括：

保密密钥检索单元从所述接收的打印作业中检索加密的保密密钥；以及

保密密钥获取单元基于公共密钥密码系统，对从所述保密密钥检索单元中检索出的加密的保密密钥执行解密，利用所述保密密钥获取单元的专用密钥来解密所述加密的保密密钥，并且获得所述打印作业的保密密钥，其中：

所述打印数据解密单元用作基于常规加密系统而执行解密的公共密钥解密单元，应用所述常规加密系统，以利用所述保密密钥来解密所述加密的打印数据，并且获得打印数据。

30、根据权利要求28的成像方法，还包括：

数字签名检索单元从所述接收的打印作业中检索数字签名，其中：

所述特征数量获取单元通过基于公共密钥解密方法，利用所述打印作业的源端的公共密钥，解密由所述数字签名检索单元检索出的数字签名，从而获得特征数量；

所述打印数据确认单元比较根据所述打印数据解密单元解密的打印数据而计算出的特征数量与由所述特征数量获取单元获得的特征数量，确认这些特征数量相互匹配，由此确认所述源端是指定的成像装置驱动程序，并且所述加密并被接收的打印数据没有被改变。

具有数据加密和解密的打印数据通信

技术领域

本发明涉及打印控制装置、成像装置、成像装置管理服务器、打印处理系统、打印控制方法、计算机程序以及计算机可读记录媒体，尤其适于经由通信媒体，例如因特网和网络等打印数据。

背景技术

从主机计算机获取和打印打印机（成像装置的一个例子）上数据的方法包括：独立连接方法，其中主机计算机和打印机通过电缆直接连接；以及网络连接方法，其中主机计算机和打印机通过网络相互连接，使得网络连接允许使用远程打印机。

在这些方法中，用于通过使用上述网络连接的网络打印数据的网络打印优点在于在连接到网络（因特网）的其他打印机上打印。网络打印优点还在于允许多个终端设备共享大的高速打印机和昂贵的彩色打印机，以及如上所述在远程打印机上打印数据。这些优势使得网络打印的使用剧增。

发明内容

但是，只有有限数量的用户使用网络和因特网，并且如果第三方想，则第三方能够容易地窃取流过网络和因特网的打印数据。

例如，当在连接到以太网的客户端中打印机上打印重要数据，例如安全和保密数据时，或者当售货员使用访问端附近的打印机打印这样的数据时，不希望打印数据在到达打印机之前被窃取、篡改，或者打印数据在不是打印机驱动程序所指定的打印机的错误打印机上被打印。

但是，在现有技术中，已经存在这样的问题，即第三方能够在通

过通信媒体，例如网络、因特网等，打印数据时窃取和使用打印数据。

本发明用以解决上述问题。作为本发明的第一方面，即使打印数据在其通过通信媒体，例如网络、因特网等被打印时，也能够保护被窃取的数据，以防被第三方使用。另外，作为本发明的第二方面，即使打印数据在其通过通信媒体，例如网络、因特网等被打印时被窃取和篡改，也能够检测到窃取和篡改，以保护数据不被非法打印。

另外，作为本发明的第三方面，当通过网络和因特网从打印机管理服务器获得端口、URL、或作为打印机目的地的合适例子的其他信息时，保护关于打印目的地数据的信息，以防止被窃取。

根据本发明，提供了一种打印控制装置，用于将包含打印数据的打印作业通过通信媒体传输到指定的成像装置，并且控制所述指定的成像装置以打印所述打印数据，所述打印控制装置包括：

获取单元，用于在加密状态从所述成像装置获取关于邮件方法的目的地的信息，其中所述邮件方法是被远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；

解密单元，用于解密所述获取单元获取的关于目的地的信息；以及

传输单元，用于借助所述邮件方法，将所述打印数据传输到由所述解密单元解密的信息所指示的目的地，其中根据 HTTP 协议执行所述传输。

根据本发明，还提供了一种成像装置，用于打印包含在通过通信媒体接收的打印作业中的加密的打印数据，包括：

传输单元，用于加密和传输关于邮件方法的目的地的信息，所述邮件方法是远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；以及

设置单元，响应于关于目的地的信息的传输，设置所述成像装置可以接受来自远程源端的邮件方法的条件。

根据本发明，还提供了一种打印控制方法，用于将包含打印数据的打印作业通过通信媒体传输到指定的成像装置，并且控制所述指定

的成像装置以打印所述打印数据，所述打印控制方法包括:

获取单元在加密状态从所述成像装置获取关于邮件方法的目的地的信息，其中所述邮件方法是被远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程;

解密单元解密所述获取单元获取的关于目的地的信息；以及

传输装置将所述打印数据传输到借助所述邮件方法由所述解密装置解密的信息所指示的目的地，其中根据 **HTTP** 协议执行所述传输。

根据本发明，还提供了一种成像方法，用于打印包含在通过通信媒体接收的打印作业中的加密的打印数据，包括:

传输单元加密和传输关于邮件方法的目的地的信息，所述邮件方法是远程调用的、用于从远程源端向所述成像装置中的目的地输入打印数据的进程；以及

设置单元响应于关于目的地的信息的传输，设置所述成像装置可以接受来自远程源端的邮件方法的条件。

由以下描述结合附图将了解本发明的其他特征和优点，在附图中相同的附图标记表示系统或相似的部件。

附图说明

图 **1** 参考打印处理系统的配置例子表示本发明的第一实施例的构思;

图 **2** 是参考打印处理系统的配置例子的本发明的第一实施例的框图;

图 **3A** 和 **3B** 表示使用 **RAM** 内存图的第一实施例;

图 **4** 通过解释在打印处理系统中所使用的加密密钥而表示本发明的第一实施例;

图 **5** 参考打印机驱动程序过程流程图表示本发明的第一实施例;

图 **6** 参考打印机过程流程图表示本发明的第一实施例;

图 **7** 参考打印机驱动程序过程流程图表示本发明的第二实施例;

图 **8** 参考打印机过程流程图表示本发明的第二实施例;

图 9 参考打印机驱动程序过程流程图表示本发明的第三实施例;

图 10 参考打印机过程流程图表示本发明的第三实施例;

图 11 参考打印处理系统的配置例子表示本发明的第四实施例的构思;

图 12 是参考打印处理系统的配置例子的本发明的第四实施例的框图;

图 13A、13B 和 13C 表示使用 RAM 内存图的第四实施例;

图 14 通过解释打印处理系统中所使用的加密密钥而表示本发明的第四实施例;

图 15 参考打印机管理服务器过程流程图表示本发明的第四实施例;

图 16 参考打印机驱动程序处理流程图表示本发明的第四实施例;

图 17 参考打印机处理流程图表示本发明的第四实施例;

图 18 参考打印机管理服务器处理流程图表示本发明的第五实施例;

图 19 参考打印机驱动程序处理流程图表示本发明的第五实施例;

图 20 参考打印机驱动程序处理流程图表示本发明的第六实施例;

图 21 参考打印机管理服务器处理流程图表示本发明的第六实施例;

图 22 参考打印机处理流程图表示本发明的第六实施例;

图 23 参考对目的地信息的加密过程表示本发明的实施例。

具体实施方式

(第一实施例)

以下参考附图介绍根据本发明的打印控制装置、打印机、打印机管理服务器、打印处理系统、打印控制方法、计算机程序以及计算机可读记录媒体的第一实施例。

图 1 参考打印处理系统的配置例子表示本发明的第一实施例的构思。

在本发明的这个实施例中，用户运行来自作为打印控制装置安装的主机计算机 300 的打印指令，并考虑这样的情况，其中在共享于网络（LAN）100 中的网络打印机和通过因特网 200 连接的因特网打印机 1500b 上打印数据。除了打印机，成像装置的例子可以是扫描仪、传真机、数码相机、以及具有复印机、打印机、传真机、扫描仪等功能的组合机器（多功能外部设备）。

图 2 是参考打印处理系统的配置例子的本发明的第一实施例的框图。

除非另外指明，主机计算机 3000 通过 LAN、WAN、公共电路、因特网、以及其他任何方式（通信媒体）连接到打印机 1500（网络打印机 1500a 和因特网打印机 1500b）。

在图 2 中，主机计算机 3000 包括 CPU 1，CPU 1 用于根据存储在 ROM 3 的程序 ROM 或外部存储器 11 中的文档处理程序等，以混合方式处理包含图形、图像、字符、表格（包括电子数据表格等）等的文档，并且中央控制连接到系统总线 4 的设备 2 到 8 中的每一个。

ROM 3 的程序 ROM 3b 或者外部存储器 11 也存储作为 CPU 1 的控制程序的操作系统程序（OS）等。ROM 3 的字库 ROM 3a 或外部存储器 11 存储字库数据等，用于在上述文档处理中使用。另外，ROM 3 的数据 ROM 3c 或外部存储器 11 存储各种数据，用于在执行上述文档处理中使用。

RAM 2 作为 CPU 1 的主存储器、工作区等。

键盘控制器（KBC）5 控制来自键盘 9 或附图中未示出的点击设备的密钥输入。

CRT 控制器（CRTC）6 控制 CRT 显示器（CRT）10 的显示。

磁盘控制器（DKC）7 控制对存储引导程序、各种应用程序、字库数据、用户文件、编辑文件、打印机控制命令产生程序（以下称为打印机驱动程序）等的硬盘（HD）和外部存储器，例如软盘等的访问。

打印机控制器（PRTC）8 通过网络 100 连接到打印机 1500，并且执行对与打印机 1500 的双向通信的控制过程。打印机控制器 8 能够

在打印作业被传输到打印机 1500 时根据连接协议将命令添加到打印作业。命令也能够由操作系统程序（OS）自动添加。

CPU 1 对 RAM 2 中显示信息 RAM 组中的外形字型执行光栅化，并支持 CRT 10 上的 WYSIWYG。

CPU 1 打开在 CRT10 上根据附图中未标出的鼠标光标等所指示的命令所记录的不同窗口，并执行各种类型的数据处理。在执行打印处理之前，用户打开用于打印设置的窗口。然后，用户使用打开的窗口设置用于打印机驱动程序的打印过程，包括设置打印机、选择打印模式等。

在打印机 1500 中，打印机 CPU 12 具有根据存储在 ROM 14 的程序 ROM 中的控制程序等或存储在外部存储器 21 中的控制程序等，通过连接到系统总线 15 的打印单元接口（打印单元 I/F）16 将图像信号作为输出信息输出到打印单元 17（打印机机芯）的功能。

ROM 14 的程序 ROM 14b 存储打印机 CPU 12 的控制程序等。ROM 14 的字库 ROM 14a 存储字库数据等，用于生成输出信息。ROM 14 的数据 ROM 14c 存储由主机计算机 3000 在没有外部存储器 21，例如硬盘等，的打印机上使用信息等。

打印机 CPU 12 能够通过输入单元 18 与主机计算机 3000 通信，并且能够将打印机 1500 中的信息等通知主机计算机 3000。

从打印机驱动程序中所接收的数据被存储在 RAM 13 中，并由控制程序转换为图像信号。根据通信协议所添加的命令也由控制程序解释。

RAM 13 是作为打印机 CPU 12 的主存储器、工作区等的记录媒体，并且被配置，使得其存储能力能够由连接到附图中未标出的外部端口的可选 RAM 扩展。RAM 13 被用作输出信息扩展区、环境数据存储区、NVRAM（非易失性 RAM）等。

上述硬盘（HD）和外部存储器 21，例如 IC 卡等，由存储器控制器（MC）20 进行访问控制。外部存储器 21 作为可选单元连接，并存储字库数据、仿真程序、形式数据等。

操作面板 22 具有操作开关、LED 指示器、液晶面板等。另外，上述外部存储器 21 不限于一个单元，并且可以包括至少一个或多个存储单元。存储器也能够被配置为除了内部字库外，还具有可选的字库卡，以及存储用于解释不同类型打印机控制语言的程序的多个外部存储器单元。另外，存储器可以包括附图中未标出的 NVRAM，用于存储来自操作面板 22 的打印机模式设置信息。

图 3A 是表示控制程序的内存图，所述控制程序根据本发明的这个实施例存储在主机计算机 3000 的程序 ROM 3b 中，并在其被装入主机计算机 3000 的 RAM 2 中以后变为可执行的。

根据本发明的这个实施例，在主机计算机 3000 中使用的加密、数据特征数量计算功能作为与打印过程相关的程序 304 的一部分驻留。指派给打印的打印机公共密钥和打印机自身的专用密钥作为相关数据 303 的一部分驻留。

图 3B 是表示控制程序的内存图，根据本发明的这个实施例，所述控制程序被存储在打印机 1500 的程序 ROM 14b 中，并在其装入打印机 1500 的 RAM 13 中以后边为可执行的。

根据本发明的这个实施例，在打印机 1500 中使用的解密、数据特征数量计算功能等作为与打印过程相关的程序 313 的一部分驻留。特定打印机驱动程序的公共密钥和打印机自身的专用密钥作为相关数据 312 的一部分驻留。

图 4 表示根据本发明的这个实施例，在打印处理系统（参考图 5 中和后表示的流程图）中使用的加密密钥。在这个实施例中，由公共密钥密码系统和常规加密系统实现加密，并且每个信息设备具有其自己的公共密钥和专用密钥。因此，图 4 清楚地表示了各个密钥。

在图 4 中，表示与数据重叠的密钥的图片指示数据由相应密钥加密。

在根据本发明的这个实施例的打印处理系统中，不能通过传输在公共密钥密码系统中加密的打印数据而在不是所指定打印机的其他任何打印机上执行打印过程。

公共密钥密码系统是这样一种方法，其中在一个用户和所述用户的通信伙伴之间使用不同密钥（专用密钥和公共密钥）实现加密和解密，并且使用一个密钥加密的数据不能无需使用其他密钥就被解密。

在公共密钥密码系统中，公共密钥通常被公开，而专用密钥保密。在公共密钥密码系统中，不需要为每个通信伙伴准备特定密钥，公共密钥能够被公开。因此，可以由能够解密限于所述用户的密钥的个人很容易地将密钥传输到通信伙伴。

如果公共密钥密码系统被用于，例如根据本实施例的打印机1500，并且使用打印机的公开的公共密钥加密打印数据，则能够只在具有从任何打印机驱动程序传输的打印数据的目的地打印机上打印所述数据，由此使其他打印机不能打印所述数据。

以下参考图5中所示的过程流详细介绍打印机驱动程序生成加密打印作业的过程。

在从应用程序接收打印请求时，主机计算机3000的打印机驱动程序使用目的地打印机1500的公共密钥加密打印数据（步骤S501）。

然后，加密的打印数据作为打印作业被传输到打印机1500。

公开打印机1500的公共密钥，并且打印机驱动程序选择所使用的目的地打印机1500的公共密钥。

以下参考图6中所示的过程流详细介绍打印机1500从所接收的打印作业获得打印数据的过程。

打印机1500使用打印机1500的专用密钥解密所接收的打印作业中的打印数据（步骤S601），并获得打印数据。

如上所述，打印机1500的专用密钥被打印机1500作为未公开的密钥保持。

当未指定的打印机试图打印打印数据时，所述打印数据被加密，并且不能被解密或打印。另外，既然只有指定的打印机1500才具有解密所述加密数据的密钥，所以其他打印机不能解密所述数据。因此，在根据本发明的实施例的打印处理系统中，尽管打印数据在网络100中被窃取，但是能够保护打印数据不在其他打印机上被打印。

（第二实施例）

以下介绍根据本发明的打印控制装置、打印机、打印机控制服务器、打印处理系统、打印控制方法、计算机程序、以及计算机可读记录媒体的第二实施例。根据本发明的打印处理系统的硬件的配置与上述第一实施例相似。因此，与第一实施例中部件相同的部件的附图标记与图 1 到 6 中所示的附图标记相同，并且在这里省略了详细解释。

在第一实施例中，即使打印数据被窃取，打印处理系统也能够保护打印数据不在其他打印机上被打印。

但是，既然打印机 1500 的公共密钥被公开，所以当任何人窃取了原始打印数据，并且通过与图 5 中所示的过程相同的步骤将不同数据传输到打印机 1500 时，打印机 1500 不能确定打印数据是否已经被篡改。在打印数据是估价、安全等时，这可能引起严重的问题。

因此，在根据本实施例的打印过程中，能够通过接收具有添加到打印数据的数字签名的打印作业，由打印机检验是否存在篡改。

通过使用主机计算机 3000 的打印机驱动程序的专用密钥加密打印数据内容的被计算出的特征数量来获得数字签名。打印机具有特定打印机驱动程序的内部公共密钥，并且将其用于解密和检验数字签名。

用散列值、校验和等表示打印数据内容的特征数量。使用散列函数计算散列值，所述散列函数几乎不能从计算结果中获得，或者几乎不能被伪造以获得同样的散列值。

以下参考图 7 所示的过程流详细介绍根据本实施例的主机计算机的打印机驱动程序生成加密打印作业的过程。

当接收在来自应用的打印请求处的打印数据时，主机计算机的打印机驱动程序使用目的地打印机的公共密钥加密打印数据（步骤 S701）。

然后，使用特征数量计算函数从原始未加密的打印数据中计算特征数量（步骤 S702），并且使用打印机驱动程序的专用密钥加密特征数量（步骤 S703）。使用这个结果作为数字签名。然后，主机计算机将加密的打印数据和数字签名的组合作为打印作业传输到打印机，用

于打印所述打印数据。

以下参考图8中所示的过程流详细介绍根据本实施例的打印机从所接收的打印作业中获得打印数据的过程。

打印机使用打印机的专用密钥解密所接收的打印作业中的打印数据（步骤S801），以获得打印数据。然后，它使用源打印机设备的公共密钥解密打印作业中的数字签名（步骤S802），以获得所获得的打印数据的特征数量。

然后，打印机使用特征数量计算函数从所获得的打印数据计算特征数量（步骤S803），比较所述特征数量与所接收的打印数据的特征数量（步骤S804），并且如果特征数量相互匹配，则确认在步骤S801中所获得的打印数据没有被篡改。

如果打印机所计算的特征数量与步骤S804过程中所接收的打印数据的特征数量不匹配，则假设以下情况。

即，可能存在这样的情况，其中不能使用特定计算机驱动程序的公共密钥解密打印数据，并且所接收的打印数据的源与正确的主机计算机不同，还可能存在这样的情况，其中打印数据的计算出的特征数量与所接收的打印数据的特征数量不同，因此表示打印数据被篡改。在每种情况中，打印作业都没有被正确地传输。

在根据本实施例的打印处理系统中，打印机能够检测非法打印数据。当检测到非法打印数据时，在检测后不输出非法打印数据，并且将非法打印数据的接收通知主机计算机，这是有效的对策。

在本实施例中，打印机主体具有与打印机驱动程序共同的特征数量计算函数。另外，假设在打印机主体中已经提前记录特定打印机驱动程序（或主机计算机）的公共密钥。

特定于打印机驱动程序的加密密钥不限于打印机驱动程序，而是能够由特定于主机计算机3000或当前用户的加密密钥替代。

例如，当加密密钥特定于主机计算机3000时，能够在多用户模式中使用主机计算机3000，使得所有使用主机计算机3000的用户能够在相同条件下在打印机1500上打印打印数据。

当加密密钥特定于用户时，能够在相同条件下由公司内的桌上个人计算机或室外的笔记本个人计算机（PC）打印打印数据。

因此，在加密密钥特定于打印机驱动程序、主机计算机3000、或用户的任何情况下，在打印机中只记录一个公共密钥。

（第三实施例）

以下介绍根据本发明的打印控制装置、打印机、打印机管理服务器、打印处理系统、打印控制方法、计算机程序、以及计算机可读记录媒体的第三实施例。根据本实施例的打印处理系统的硬件配置与上述第一和第二实施例的配置相似。因此，与第一和第二实施例中部件相同的部件具有图1到8中所示相同的附图标记，并且这里省略了详细的解释。

在上述第一和第二实施例中，保护打印数据不被窃取或被窃取的打印数据不被篡改，使得能够具有改进的打印数据安全性地打印打印机驱动程序。

但是，既然在上述公共密钥密码系统中打印数据的加密和解密需要很长的处理时间，所以不希望将这种方法用于大量的打印数据。

因此，在本实施例中，介绍比公共密钥密码系统具有更高性能（需要短得多的处理时间）的常规加密系统。

常规加密系统是指在用户及其伙伴之间使用相同密钥（保密密钥）加密和解密数据的方法。实际上，通过根据保密密钥所代表的规则用其他比特串替代或移动句子的比特串来加密数据。

常规加密系统的处理被视为比具有以下特征的公共密钥密码系统的复杂过程快好几百倍，所述特征是在由乘以素数而得到的值时很难执行素因数分解，或者很难估计值已经被输入其中的椭圆曲线中的值。

但是，另一方面，需要用安全的方法将保密密钥传递给每个伙伴，并且准备特定于每个伙伴的保密密钥。

在本实施例中，公共密钥密码系统与常规加密系统组合，以使用保密密钥加密打印数据，并使用公共密钥将保密密钥传递到打印机。

以下参考图9中所示的过程流详细介绍打印机驱动程序生成加密打印作业的过程。

当根据来自应用的请求接收打印数据时，主机计算机的打印机驱动程序首先生成保密密钥（步骤S901），并使用所生成的保密密钥加密所接收的打印数据（步骤S901）。使用打印机的公共密钥加密所生成的保密密钥（步骤S903）。

然后，使用特征数量计算函数从原始未加密的打印数据中计算特征数量（步骤S904），并使用打印机驱动程序的保密密钥加密特征数量（步骤S905）。结果是数字签名。

然后，主机计算机将使用保密密钥加密的打印数据、使用打印机公共密钥加密的保密密钥、和数字签名的组合作为打印作业传输到打印机。

以下参考图10中所示的过程详细介绍打印机从所接收的打印作业中获得打印数据的过程。

打印机使用打印机的专用密钥解密打印作业中所接收的保密密钥（步骤S1001），并获得打印作业中的保密密钥。

然后，使用所获得（解密）的保密密钥解密打印作业中的打印数据（步骤S1002），并获得打印数据。

使用源打印机驱动程序的公共密钥解密打印作业的数字签名（步骤S1003），并获得打印数据的特征数量。

从所获得的打印数据中，打印机主体使用特征数量计算函数计算特征数量（步骤S1004），比较所计算出的特征数量与打印数据的所接收的特征数量（步骤S1005）。如果特征数量相互匹配，则确认在步骤S1002中所获得的打印数据没有被篡改。

因此，根据本实施例，消耗公共密钥密码系统的时间只用于加密和解密保密密钥，并且不需要为连接到网络和因特网的多个打印机的每一个都管理保密密钥。另外，既然主机计算机能够在每次建立通信时改变保密密钥，所以打印数据能够被更安全地传输到打印机。

（第四实施例）

以下介绍根据本发明的打印控制装置、打印机、打印机管理服务器、打印处理系统、打印控制方法、计算机程序、和计算机可读记录媒体的第四实施例。

在本发明的上述第一到第三实施例中，能够通过能够加密打印数据，借助于只能有指定的打印机解密所述数据，而保护打印数据不被窃取，并且能够通过将数字签名（通过打印数据的源使用其自己的专用密钥加密打印数据的特征数量而获得，并且能够通过确认使用源的公共密钥解密的内容而检测数据的篡改）添加到打印数据，而保护打印数据不被篡改。

但是，在上述第一到第三实施例中所描述的方法中，必须将能够被指定的所有打印机的公共密钥通知主机计算机（或打印机驱动程序）。类似地，在打印机主体中必须记录所有打印机驱动程序的公共密钥。

因此，能够使用大量主机计算机和打印机的大的打印处理系统需要费力的操作来记录和维持必需的信息。

在这种情况下，本实施例维持使用上述第一到第三实施例中所述的打印处理系统、通过因特网和网络安全地传输打印数据的系统，打印机管理服务器中央地管理关于打印机公共密钥等的必需信息，并且打印机驱动程序从打印机管理服务器获得必需的信息，由此消除管理关于每个打印机的信息的需要。以下介绍具有上述配置的打印处理系统。

因此，通过将打印机管理服务器添加到参考本发明的第一到第三实施例所述的打印处理系统来设计根据本实施例的打印处理系统的硬件配置。因此，第一到第三实施例中也包括的部件具有与图 1 到 3 中相同的附图标记，并且这里省略详细解释。

图 11 参考打印处理系统的配置例子表示本发明的第四实施例的构思。

假设，用户运行来自主机计算机 3000 的打印指令，并且在网络（LAN）100 上共享的网络打印机 1500a 和通过因特网 200 连接的打

印机 1500b 执行打印过程。

打印机管理服务器 4000（4000a，4000b）管理关于可能的打印机的信息（设置位置、地址、加密密钥等），并且主机计算机 3000 在打印期间从打印机管理服务器 4000 获得关于需要的打印机的信息，并将打印数据传输到相应打印机。

根据本实施例的打印处理系统也能够通过打印机管理服务器 4000 将打印数据传输到打印机 4000a 和 4000b。打印机管理服务器 4000 能够被连接到网络 100 或因特网 200。

图 12 是参考打印处理系统的配置例子的、本发明的第四实施例的框图。

除非特别说明，主机计算机 3000 通过任何 LAN、WAN、公共电路、因特网等连接到打印机 1500。

在图 12 中，打印机管理服务器 4000 包括用于执行存储在 ROM 33 或附图中未标出的外部存储器中的控制程序的 CPU 31，以及作为 CPU 31 的主存储器、工作区等的 RAM 32，并且 CPU 31 中央地控制连接到系统总线 35 的每个单元 32 和 33。

网络接口卡（NIC）34 执行与打印机驱动程序和打印机 1500 的双向通信过程。

图 13A 是表示控制程序的内存图，所述控制程序根据本发明的这个实施例被存储在主机计算机 3000 的程序 ROM 3b 中，并且在其被装入到主机计算机 3000 的 RAM 2 以后变为可执行的。

根据本发明的这个实施例在主机计算机 3000 中使用的加密、数据特征数量计算函数等作为与打印过程相关的程序 304 的一部分被驻留。

打印机管理服务器 4000 的公共密钥和打印机驱动程序自己的专用密钥作为相关数据 303 被驻留。

图 13B 是表示控制程序的内存图，所述控制程序根据本发明的这个实施例被存储在打印机管理服务器 4000 的程序 ROM 33（或附图中未标出的外部存储器）中，并且在其被装入到打印机管理服务器 4000

的 RAM 32 中以后变为可执行的。

根据本发明的这个实施例在打印机管理服务器 4000 中使用的加密/解密、数据特征数量计算函数、打印机检索过程等作为与打印过程相关的程序 313 的一部分被驻留。

由打印机管理服务器 4000 管理的打印机信息（设置位置和每个打印机的地址、每个打印机的公共密钥等）作为相关数据 312 的一部分驻留。

图 13C 是表示控制程序的内存图，所述控制程序根据本发明的这个实施例被存储在打印机 1500 的程序 ROM 14b 中，并且在其被装入到打印机 1500 的 RAM 13 中以后变为可执行的。

根据本发明的这个实施例的在打印机 1500 中使用的解密、数据特征数量计算函数等作为与打印过程相关的程序 323 的一部分被驻留。打印机管理服务器 4000 的公共密钥和打印机驱动程序自己的专用密钥作为相关数据 322 的一部分被驻留。

图 14 表示根据本发明的实施例的、在打印处理系统中使用的（参考图 15 中和后的流程图）密钥。在这个实施例中，由公共密钥密码系统实现加密，并且每个信息设备具有其自己的公共密钥和专用密钥。因此，各个密钥被单独表示。

在图 14 中，表示与数据重叠的密钥的图片指示由相应密钥加密的数据。

在根据本发明的这个实施例的打印处理系统中，打印机驱动程序以安全模式从打印机管理服务器 4000 获得关于打印机 1500 的信息，并且在公共密钥密码系统中加密的打印数据被传输到打印机 1500。

公共密钥密码系统是这样一种方法，其中在用户和用户的通信伙伴之间使用不同的密钥（专用密钥和公共密钥）来实现加密和解密，并且使用一种密钥加密的数据在不使用另一个密钥的情况下被解密。

在公共密钥密码系统中，公共密钥一般被公开，而专用密钥被保密。在公共密钥密码系统中，不需要为每个通信伙伴准备特定密钥，并且公共密钥能够被公开。因此，密钥能够由能够解密限于所述用户

的密钥的个人很容易地传输到通信伙伴。

如果公共密钥密码系统被用于例如根据本实施例的打印机 **1500**，并且使用打印机的公开的公共密钥加密打印数据，则数据只能在具有从任何打印机驱动程序传输的打印数据的目的地打印机上被打印，由此使其他打印机不能打印所述数据。

数字签名被用作打印机驱动程序安全地从打印机管理服务器 **4000** 中获得打印机信息的方法。

通过使用源专用密钥加密将被传输的数据内容的特征数量计算结果而获得数字签名。在这个例子中，使用打印机管理服务器 **4000** 的专用密钥加密打印机信息。

打印机驱动程序保持打印机管理服务器 **4000** 的公共密钥，使用公共密钥解密所加密的数字签名，并比较所解密的数字签名与从单独被传输的打印机信息中所计算出的特征数量，由此成功地确认源的识别和打印数据（打印作业）是否存在篡改。

特征数量可以由散列值、校验和等表示。使用散列函数计算散列值，所述散列函数几乎不能从计算结果中获得或者几乎不能被伪造而获得相同的散列值。

当用户在应用中执行打印操作时，所述应用将打印数据传递给打印机驱动程序，并且执行打印过程。打印机驱动程序确定输出数据的第一打印机，并将打印机信息搜索请求传输到打印机管理服务器 **4000**，以获得所述打印机的地址和密钥。

接收打印机信息搜索请求数据的打印机管理服务器 **4000** 中的打印机选择参考可以被请求：

“当用户在外时，在手边的打印机（例如，最近的便利店的）上打印估价等“；

“当用户不在家或办公室时，在离用户最近的打印机上打印数据”；

“在客户等的打印机上秘密地打印数据”。

为了确定数据将在哪个打印机上打印，用户提前或交互地执行打

印机选择操作。

以下详细介绍打印机管理服务器 4000 检索打印机信息并将信息返回到打印机驱动程序的过程。

打印机管理服务器 4000 根据从打印机驱动程序所接收的打印机信息搜索请求数据的内容（需要的打印机能力，例如打印机的位置、彩色/双面/装订等）从由服务器管理的打印机信息列表中选择适当的打印机，并检索关于相应打印机的打印机信息（步骤 S501）。

假设，上述打印机信息包括打印机的打印机地址、公共密钥等。

在打印机使用在 HTTP（超文本传输协议）上实现的 SOAP（简单对象接入协议）与主机通信数据时，有效地加密 URL。

图 23 参考对关于目的地信息的加密过程表示本发明的一个实施例。在图 23 的（1）中，在识别来自用户的打印指令时，主机计算机 2301 使用在 HTTP 上实现的 SOAP，并请求打印机 2305 将打印机数据的目的地信息（这个例子中是 URL）与设备 ID 和设备功能一起作为打印机数据传输。在图 23 的(2)和(3)中，打印机将包括 URL 2305 的打印机信息传输到已经传输获取打印机信息请求的主机计算机 2301。这时，使用主机的公共密钥 2302 加密 URL。同时，或加密后立即，等待从外部单元到传输者的 URL 的 HTTP 的邮件方法。在(4)中，主机计算机 2301 使用其自己的专用密钥 2303 解密 URL。使用 HTTP 的邮件方法，主机计算机 2301 输入将被打印的数据到指示打印机中预定存储区的解密的 URL。邮件方法在 HTTP 中规定，并且是用于石匠数据输入到预定存储区的、远程调用过程。参考例如由 IETF（因特网工程任务组）所发布的文档 RFC 2616。

这时，如果 URL 作为原始数据被传输则不安全，因为打印机等待上述步骤（2）中的外部邮件方法，并且易受外部攻击。即，如果 URL 作为原始数据被传输，则它将受到来自恶意非法创入者的攻击。如果恶意非法创入者了解 URL，他就能够发起攻击，例如使用所获得的 URL 在打印机中 URL 存储区中进行写操作，或者尝试非法访问。因此，希望 URL 在使用从主机计算机获得的公共密钥在打印机中被

加密以后再被传输。主机计算机使用其自己的专用密钥解密从打印机获得的主机计算机中的 URL，并使用在 HTTP 的邮件方法中的 URL 传输打印数据。

显然 URL 是 URI（统一资源标识符）的一个例子。以上描述的是 URL 作为优选例子，但是它在增强指示目的地打印机的识别信息（例如 IP 地址、NETBEUI 所规定的 SMB 标识符地址；即关于目的地的信息和关于成像数据的目的地信息等）的安全性也是有效的。

在步骤 S501 的打印机搜索步骤中，不是始终需要选择一个打印机。即，在步骤 S501 的打印机搜索步骤中，能够执行交互过程，使得打印机管理服务器 4000 能够根据某些条件（打印机信息的搜索请求数据的内容）概略地选择一些打印机，一次将关于概略选择的打印机的打印机信息返回到打印机驱动程序，并允许打印机驱动程序从概略选择的打印机中最后选择出希望的打印机。

另外，打印机管理服务器 4000 能够传输自己管理的所有打印机的打印机信息，而无需概略地选择打印机，并允许打印机驱动程序选择所希望的打印机。

于是，打印机管理服务器 4000 使用来自所检索的打印机信息的特征数量计算函数计算特征数量（步骤 S502），并使用打印机管理服务器 4000 的专用密钥加密特征数量（步骤 S503）。在步骤 S503 中所获得的结果是数字签名。最后，打印机信息和数字签名被返回到打印机驱动程序。

以下参考图 16 所示的过程流详细介绍打印机驱动程序将加密的打印作业传输到打印机的过程。

打印机驱动程序使用打印机管理服务器 4000 的公共密钥解密包含在数字签名和从打印机管理服务器 4000 所返回的打印机信息中的数字签名，并获得特征数量（步骤 S601）。假设打印机驱动程序保持打印机管理服务器 4000 的公共密钥。

然后，打印机驱动程序使用特征数量计算函数从所获得的打印机信息中计算特征数量（步骤 S602），将其与所接收的特征数量比较（步

骤 S603），并且，如果比较的结果是特征数量相互匹配，则确认打印机信息已经从所希望的打印机管理服务器 4000 中被传输，且打印数据还没有被篡改。

于是，打印机驱动程序检索包含在打印机信息中的公共密钥（步骤 S604），并使用所检索的公共密钥加密从应用传输的打印数据（步骤 S605）。最后，加密的打印数据作为打印作业被传输到打印机 1500。

以下参考图 17 所示的过程流详细介绍打印机从打印作业获得打印数据的过程。

打印机 1500 使用打印机 1500 的专用密钥解密所接收的打印作业中的打印数据，并获得打印数据。

在图 16 和 17 所示的每个步骤中，打印作业能够被从打印机驱动程序传输到打印机 1500，这保护打印作业不被所指定的打印机以外的其他打印机非法打印。

只必须将打印机管理服务器 4000 的保密密钥通知打印机驱动程序，以在安全方法中获得打印机信息，而无需单独管理目标打印机的地址、能力或保密密钥。即，只有打印机管理服务器 4000 必须被适当的维持，以容易地和安全地打印来自任何主机计算机的打印数据。

（第五实施例）

以下介绍根据本发明的打印控制装置、打印机、打印机管理服务器、打印处理系统、打印控制方法、计算机程序、和计算机可读记录媒体的第五实施例。根据本实施例的打印处理系统的硬件配置与上述第四实施例的配置相似。因此，与第四实施例中相同的部件具有与图 11 到 15 中所示的相同的附图标记，并且这里省略详细解释。

在上述第四实施例中，既然将数字签名添加到在获取打印机驱动程序请求的打印机信息处通信的信息中，所以数据不可能被篡改，但是数据能够被网络上的任何人查阅。因此，第三方能够跟踪随后的动作。

因此，本实施例表示加密由打印机管理服务器 4000 所返回的数据，以增强信息安全性的例子。

与第四实施例的不同在于打印机管理服务器和打印机驱动程序之间的通信，而在打印机侧打印被加密的打印数据的过程与图 17 中所示的过程相同。

如果用户在应用上执行打印操作，则应用将打印数据传递给打印驱动程序，以用于打印过程。打印机驱动程序将打印机信息搜索请求数据传输到打印机管理服务器 4000。这时，根据本实施例，也传输打印机驱动程序的公共密钥，以减少用于服务器管理的信息。在服务器管理将被管理的打印机驱动程序的公共密钥时，不要求传输。

以下参考图 8 中所示的过程流详细介绍打印机管理服务器 4000 检索打印机信息并将其返回到打印机驱动程序的过程。

打印机管理服务器 4000 根据从打印机驱动程序所接收的上述打印机信息搜索请求数据的内容从由服务器管理的打印机信息列表中检索适当的打印机（步骤 S801）。这个步骤的过程与上述参考第四实施例的步骤 S501 中的过程相同。

于是，打印机管理服务器 4000 使用所接收的打印机驱动程序的公共密钥加密所检索的打印机信息（步骤 S802）。然后，打印机管理服务器 4000 使用来自原始打印机信息的特征数量计算函数计算特征数量（步骤 S803），并使用打印机管理服务器 4000 的专用密钥加密特征数量（步骤 S804）。

在步骤 S804 中所获得的结果是数字签名。最后，将加密的打印机信息和数字签名返回到打印机驱动程序。

以下参考图 19 所示的过程流详细介绍打印机驱动程序将加密的打印作业传输到打印机的过程。

打印机驱动程序使用打印机驱动程序的专用密钥解密从打印机管理服务器 4000 所接收的打印机信息（步骤 S901），并获得打印机信息。

打印机驱动程序使用打印机管理服务器 4000 的公共密钥解密从打印机管理服务器 4000 所接收的数字签名，并获得打印机信息的特征数量（S902）。假设打印机驱动程序保持打印机管理服务器 4000 的公

共密钥。

然后，打印机驱动程序使用特征数量计算函数从所获得的打印机信息中计算出特征数量（步骤 S903），将其与所接收的特征数量比较（步骤 S904），并且如果比较的结果是特征数量相互匹配，则确认已经从所希望的打印机管理服务器 4000 传输所获得的打印机信息，且打印数据还没有被篡改。

然后，打印机驱动程序检索包含在打印机信息中的公共密钥（步骤 S905），并使用所检索的公共密钥加密从应用所接收的打印数据（步骤 S906）。最后，加密的打印数据作为打印作业被传输到打印机 1500。

在上述步骤中，从打印机管理服务器 4000 所返回的打印机信息只能够被已经发出请求到打印机管理服务器 4000 的打印机驱动程序访问，由此成功地增强安全性。

既然打印机驱动程序传输其自己的公共密钥，所以打印机管理服务器不需要管理相应的打印机驱动程序。既然公共密钥是公开的，所以不存在将其传递到打印机管理服务器 4000 的问题。

在本实施例的这个例子中，加密打印机信息。但是，用于将打印机驱动程序的公共密钥从打印机驱动程序传输到打印机管理服务器 4000、并将使用公共密钥加密的信息返回到打印机驱动程序的单元也能够用于其他数据。

因此，在加密除打印机信息以外的其他数据时，能够提供不管理打印机驱动程序的打印机管理服务器 4000 的系统。

在本实施例的上述例子中，使用打印机驱动程序的保密密钥。但是，可用的保密密钥不限于打印机驱动程序的保密密钥，而是能够使用主机计算机 3000 的密钥，或者显然能够使用当前用户的密钥。

例如，当使用主机计算机 3000 的保密密钥时，能够在多用户模式中使用主机计算机 3000，使得主机计算机 3000 上的任何人都能够在相同的条件下在打印机 1500 上打印打印数据。

另外，当使用用户的保密密钥时，用户能够在相同的条件下从室内桌上个人计算机（PC）或任何室外笔记本个人计算机（PC）打印

打印数据。

（第六实施例）

以下介绍根据本发明的打印控制装置、打印机、打印机管理服务器、打印处理系统、打印控制方法、计算机程序、和计算机可读记录媒体的第六实施例。根据本实施例的打印处理系统的硬件配置与上述第四和第五实施例的配置类似。因此，与第四实施例中部件相同的不见具有图 11 到 19 中相同的附图标记，并且在这里省略详细解释。

在本发明的第四和第五实施例中，打印数据不能在指定的打印机之外的其他打印机上打印。

但是，如果任何人窃取了原始打印数据，并通过与第四和第五实施例相同的步骤将不同数据传输到目标打印机，则打印机不能确定所接收的打印数据是否已经被篡改。

这个问题能够通过将数字签名指定给打印数据而解决。但是，为了解决这个问题，目标打印机驱动程序的公共密钥将被记录在打印机中。

另外，公共密钥将被记录在打印处理系统的所有打印机中。如果增加目标主机计算机，则所有打印机必须被相应地维持。因此，以这种方法确定打印机驱动程序是否已经被篡改需要费力的操作。

这里，根据本实施例，通过打印机管理服务器 4000 传输打印数据，使得能够保护打印数据不被篡改，并且几乎能够消除对打印机 1500 的维护。

以下参考图 20 所示的过程流详细介绍打印机驱动程序将打印数据传输到打印机管理服务器的过程。

当用户在一个应用上执行打印操作时，所述应用将打印数据传递到打印机驱动程序，由此执行打印过程。

为了首先确定目的地打印机，打印机驱动程序产生请求数据到打印机管理服务器 4000，或者通过与打印机管理服务器 4000 的交互通信指派打印机（S1001），并产生将被传输到打印机管理服务器 4000 的、指定打印机的请求。

然后，打印机驱动程序使用打印机管理服务器 4000 的公共密钥加密从所述应用接收的打印数据（步骤 S1002）。最后，它将加密的打印数据和打印机指派请求传输到打印机管理服务器 4000。

以下参考图 21 所示的过程流详细介绍打印机管理服务器 4000 将加密的打印机驱动程序传输到打印机 1500。

响应于从打印机驱动程序所接收的打印机指派请求，打印机管理服务器 4000 从服务器所管理的打印机信息列表中选择适当的打印机，并检索相应的打印机信息（步骤 S1101）。假设打印机信息包括打印机的地址、公共密钥等。

然后，打印机管理服务器 4000 使用打印机管理服务器 4000 的专用密钥解密从打印机驱动程序所接收的打印数据（步骤 S1102），并获得打印数据。在这个步骤以后，除了打印机管理服务器 4000 之外的其他信息设备不能窃取打印数据。

于是，打印机管理服务器 4000 使用包含在打印机信息中的打印机公共密钥加密所获得的打印数据（步骤 S1103）。

打印机管理服务器 4000 然后从所获得的打印数据计算特征数量计算函数（步骤 S1104），并使用打印机管理服务器 4000 的专用密钥加密所计算的特征数量（步骤 S1105）。所得到的结果是数字签名。

最后，打印机管理服务器 4000 将加密的打印数据和数字签名的组合作为打印作业传输到包含在打印机信息内的打印机地址。

以下参考图 22 所示的过程流详细介绍打印机 1500 从所接收的打印作业中获得打印数据的过程。

打印机 1500 使用打印机 1500 的专用密钥解密所接收的打印作业中的打印数据（步骤 S1201），并获得打印数据。在这个步骤之后，除了指定的打印机之外的其他信息设备不能窃取打印数据。

于是，打印机 1500 使用源的打印机管理服务器 4000 的公共密钥解密所接收的打印作业中的数字签名（步骤 S1202），并获得打印数据的特征数量。

然后，打印机 1500 使用来自所获得的打印数据的特征数量计算

函数计算特征数量（步骤 S1203），将结果与所接收的特征数量比较（步骤 S1204），并且，如果特征数量相互匹配，则确认步骤 S1201 中所获得的打印数据还没有被篡改。

因此，根据本实施例，不仅能保护打印数据不被窃取，而且也能保护打印数据不被篡改。

另外，每个信息设备所保持的其他信息设备的公共密钥只是用于打印机驱动程序和打印机的打印机管理服务器 4000 的公共密钥。打印机管理服务器 4000 只必须管理服务器所管理的打印机的公共密钥。因此，尽管打印处理系统的配置被改变，但是只维护打印机管理服务器 4000。

（本发明的其他实施例）

本发明也包括为系统中连接到不同设备和计算机的装置提供用于实现上述实施例的功能的软件程序代码，从而使得能够操作不同设备实现上述实施例的功能、并且根据存储在系统的计算机（CPU 或 MPU）或装置中的程序操作不同设备的实施例。

在这种情况下，上述软件程序代码实现上述实施例的功能，程序代码本身以及为计算机提供程序代码的单元，例如存储程序代码的存储媒体，配置本发明。存储这种程序代码的记录媒体可以是例如软盘、硬盘、光盘、磁光盘、CD-ROM、磁带、非易失性存储卡、ROM 等。

不仅在执行所提供的程序代码的计算机实现上述实施例的功能时，而且在与在计算机上运行的 OS（操作系统）或其他应用软件协作实现上述实施例的功能时，本发明的实施例也包括程序代码。

另外，在所提供的程序代码被存储在计算机功能扩展板或连接到计算机的功能扩展板的存储器中时，在功能扩展板和功能扩展单元中提供的 CPU 在程序代码指令下执行部分或全部实际过程，并且由过程实现上述实施例的功能。显然这个过程也包括在本发明中。

如上所述，根据本发明，包含打印数据的打印著作业通过通信媒体被传输到指定的打印机，并且控制所指定的打印机打印所述打印数据。这时，以加密方法加密打印数据，其中只有指派打印所述打印作

业的打印机能够执行解密。因此，尽管包含打印数据的打印作业被窃取，但是能够保护打印数据不被其他打印机非法打印，并且能够保护被窃取的打印数据不被第三方非法使用。

另外，根据本实施例的其他特征，能够加密从打印数据计算出的特征数量，以产生数字签名，并且所产生的数字签名能够被包含在打印作业中并被传输。因此，能够指派打印作业的源，并且能够保证打印作业不被篡改。所以，尽管通过通信媒体打印打印数据，但是如果发生窃取和篡改，能够检测到打印数据的被窃取和篡改。因此，能够反之错误的打印，并且能够安全地打印重要的打印数据。

根据本实施例的另一个特征，能够由打印机管理服务器选择地管理连接到通信媒体的打印机。因此，打印机控制装置和打印机只必须保持打印机管理服务器的公共密钥，并且打印机管理服务器只必须保持由服务器所管理的打印机的公共密钥，由此明显减少包括多个打印控制装置和大量打印机的大系统中维护所需要的费力的操作。

图1

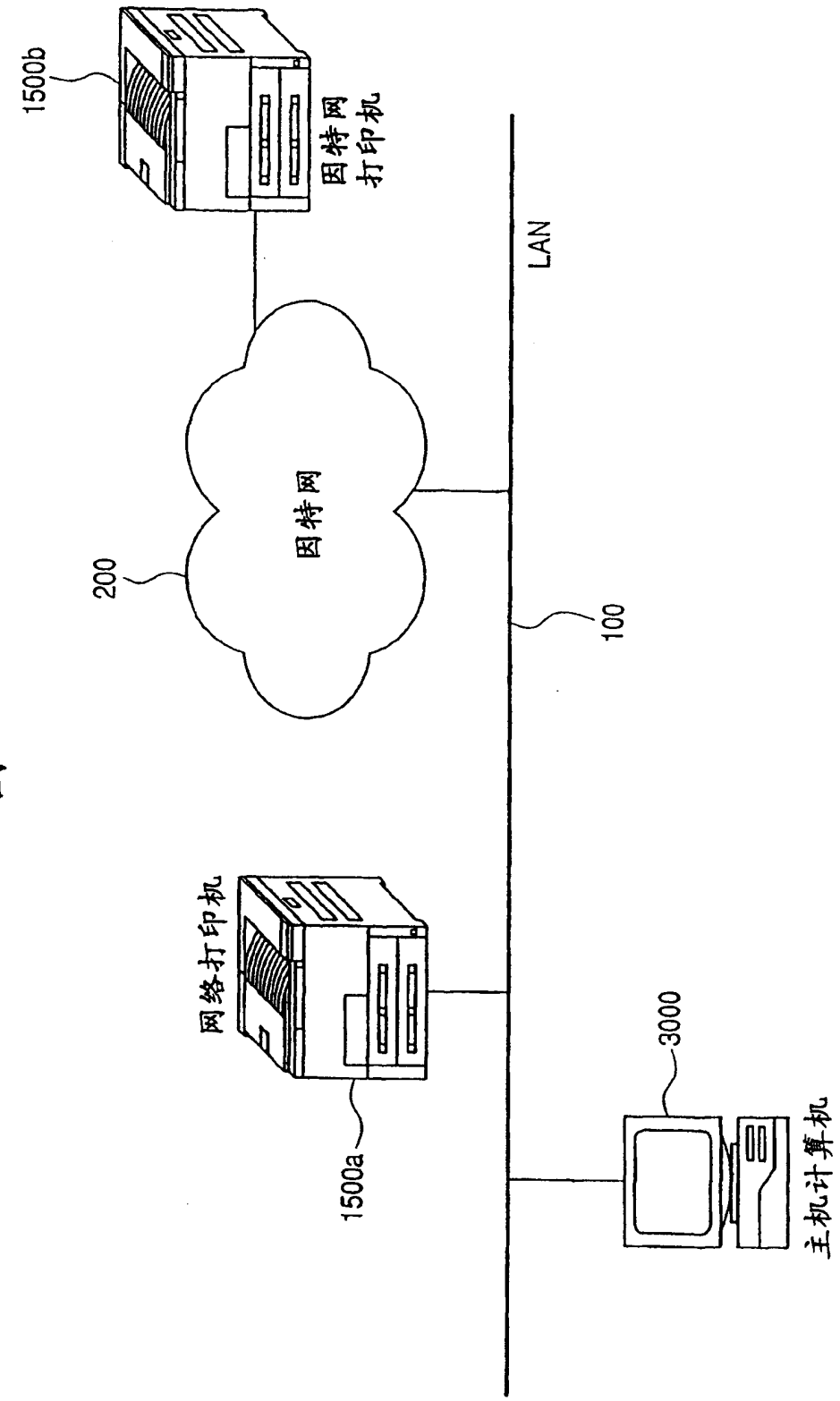


图2

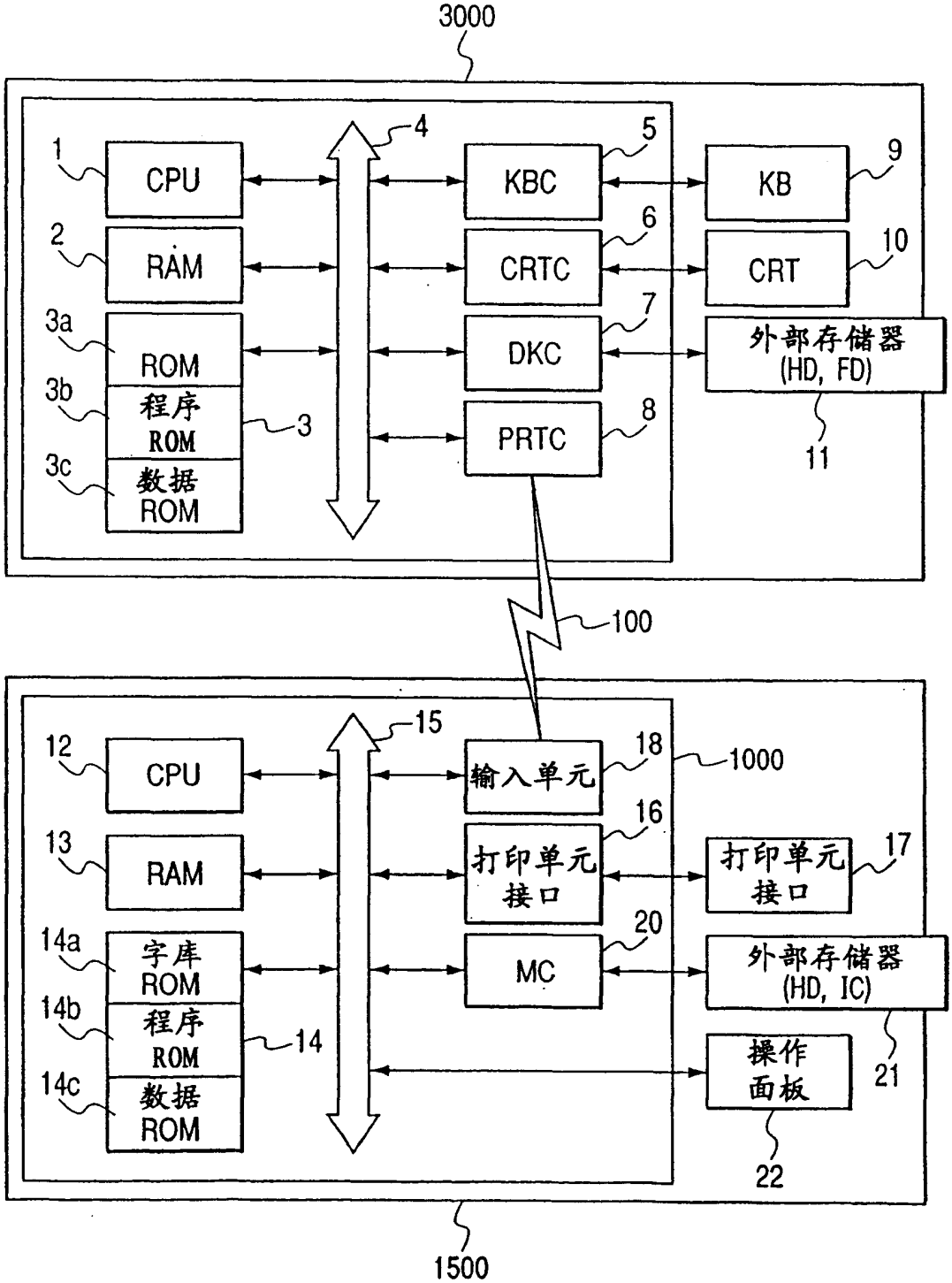

3000
1
CPU
2
RAM
3a
ROM
3b
程序 ROM
3c
数据 ROM
3
4
5
KBC
6
CRTC
7
DKC
8
PRTC
9
KB
10
CRT
外部存储器 (HD, FD)
11
100
12
CPU
13
RAM
14a
字库 ROM
14b
程序 ROM
14c
数据 ROM
14
15
18
输入单元
16
打印单元接口
20
MC
1000
打印单元接口
17
外部存储器 (HD, IC)
21
操作面板
22
1500

图 3A

主机计算机

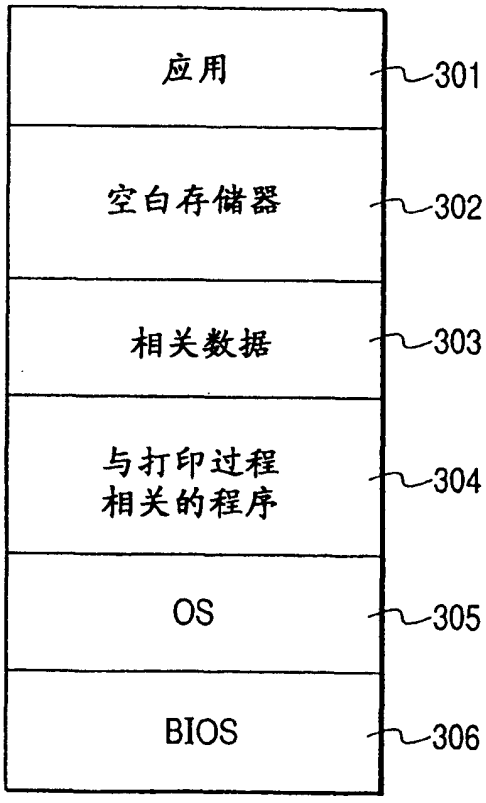


图 3B

打印机

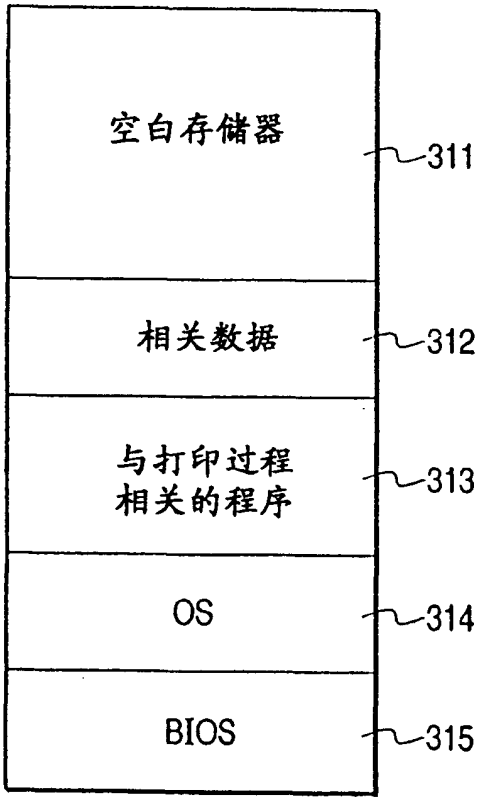
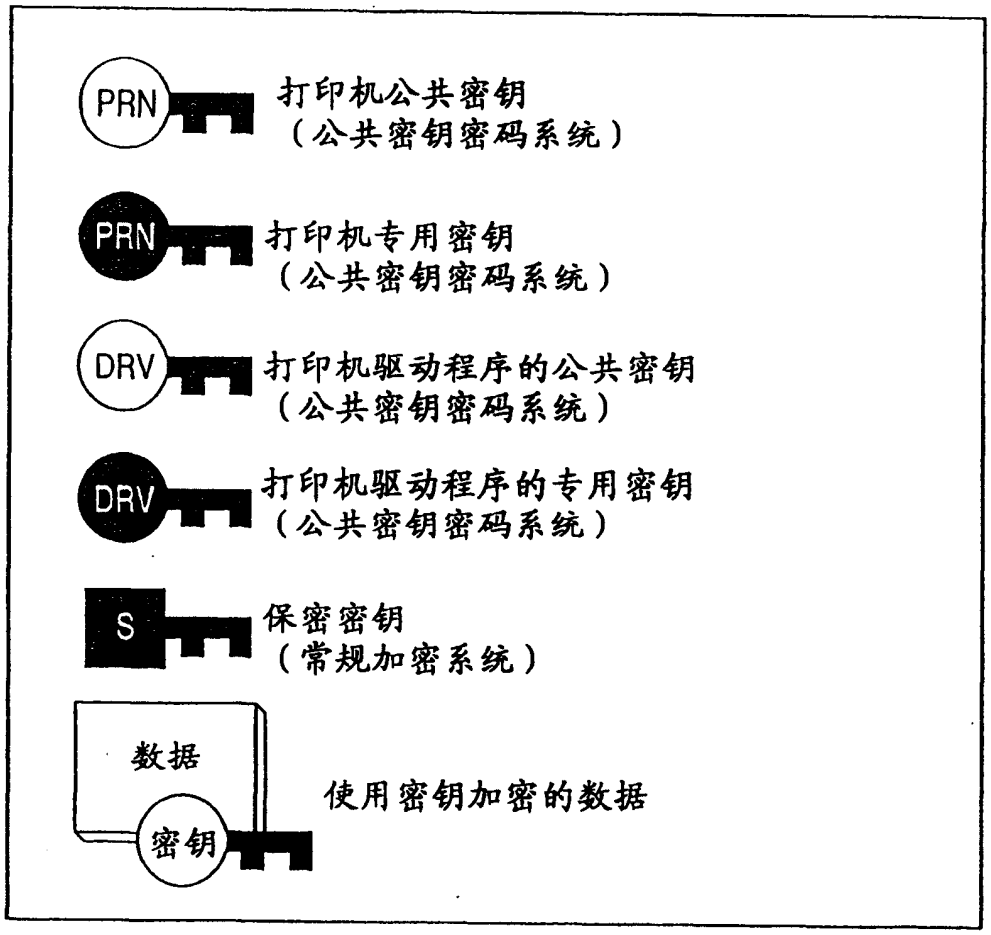


图4


PRN
打印机公共密钥
（公共密钥密码系统）
PRN
打印机专用密钥
（公共密钥密码系统）
DRV
打印机驱动程序的公共密钥
（公共密钥密码系统）
DRV
打印机驱动程序的专用密钥
（公共密钥密码系统）
S
保密密钥
（常规加密系统）
数据
密钥
使用密钥加密的数据

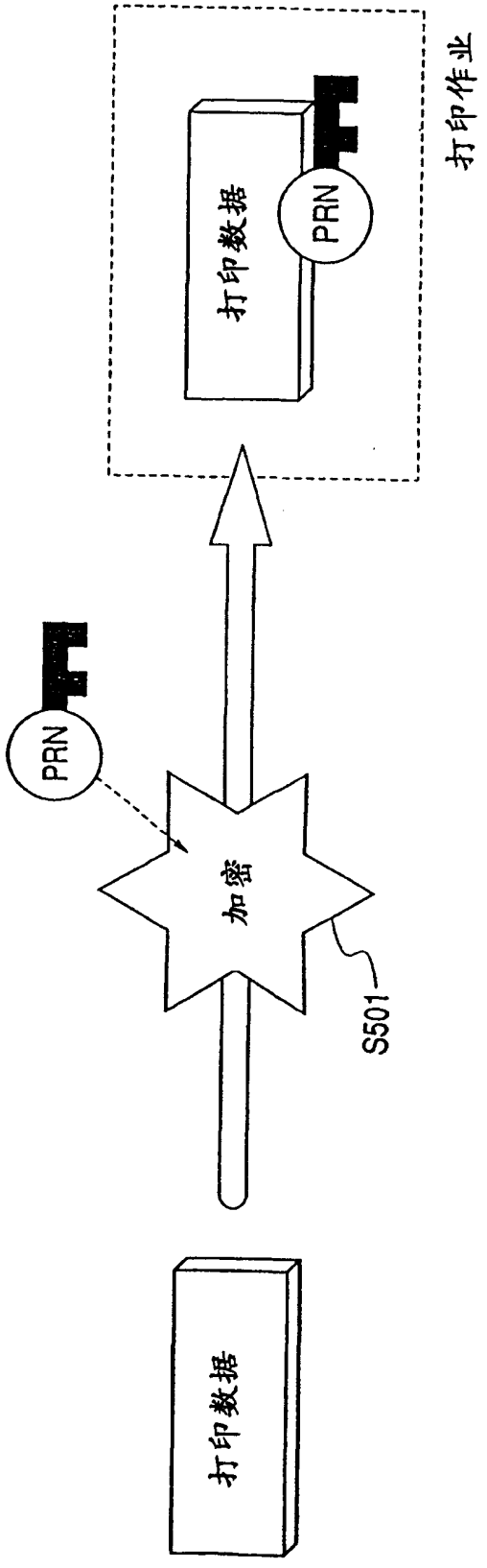
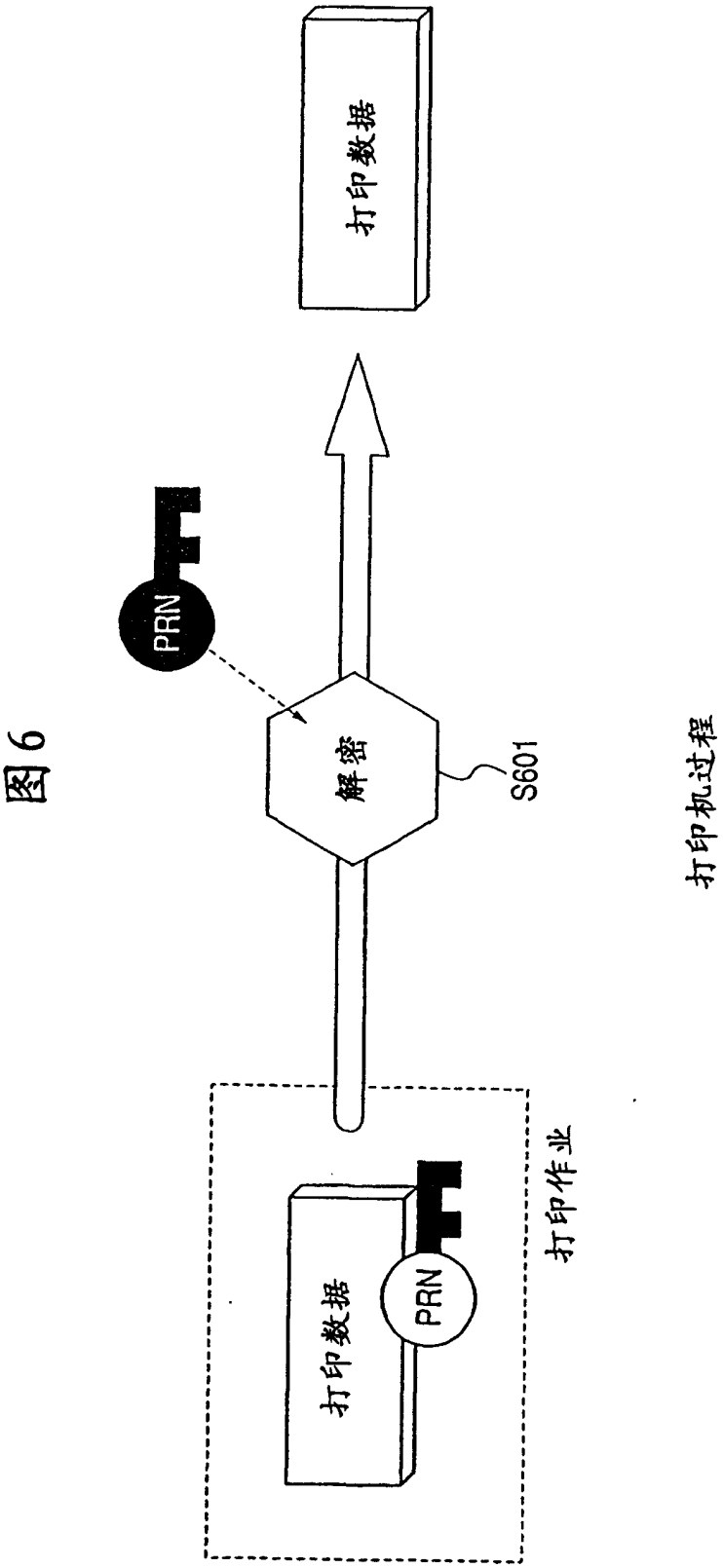


图5

图6



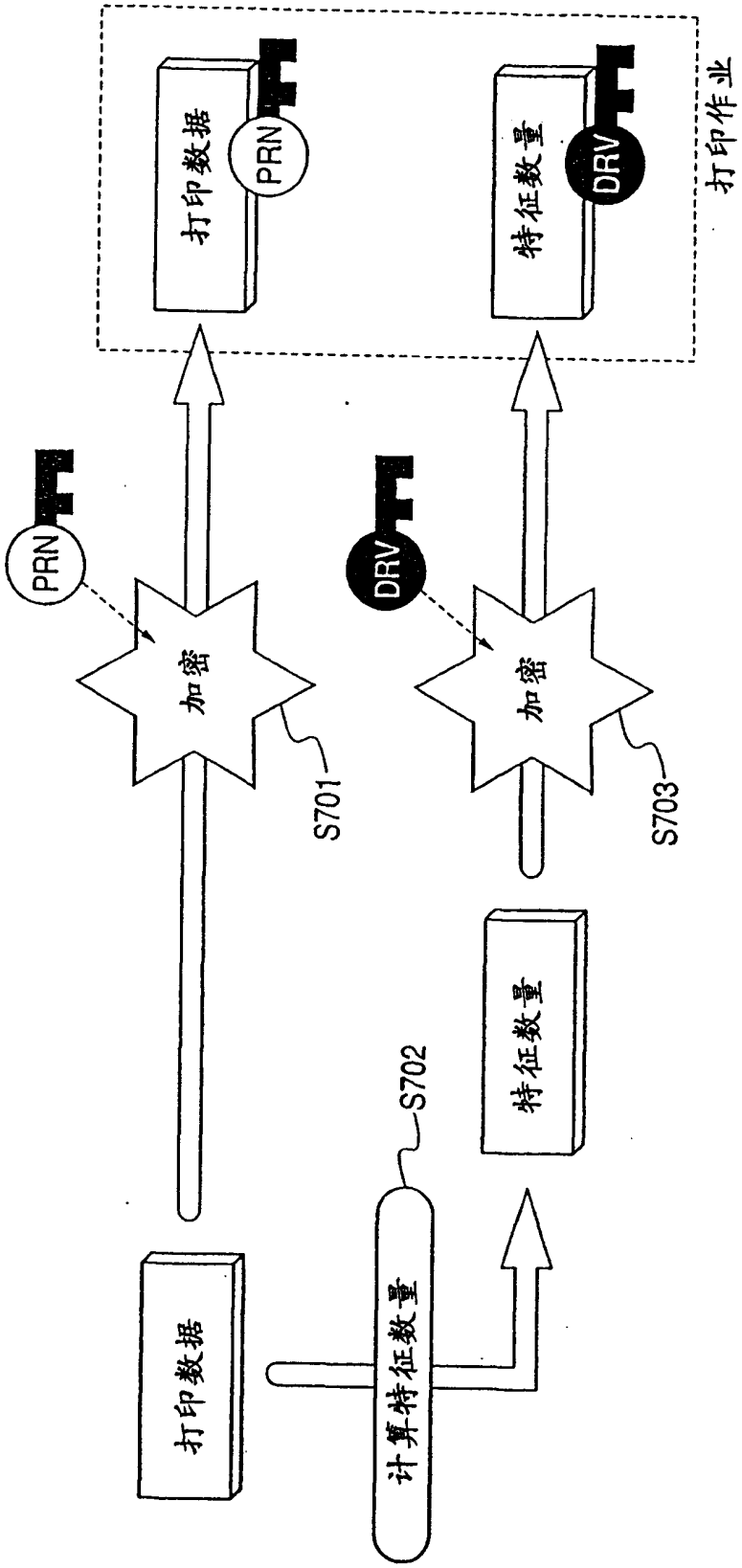


图 7

打印机驱动程序的过程

图8

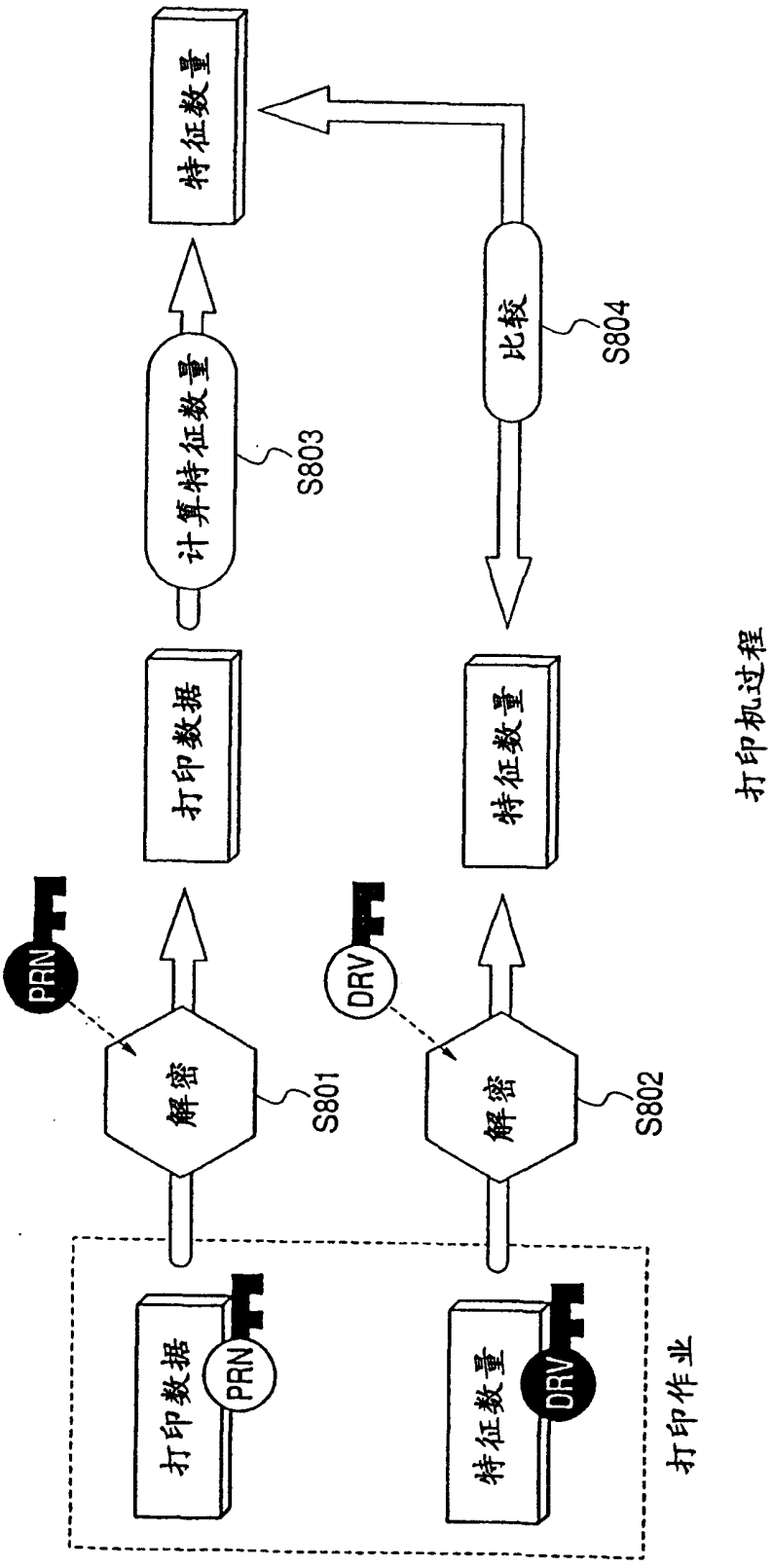

打印数据
PRN
特征数量
DRV
解密
S801
解密
S802
打印数据
特征数量
计算特征数量
S803
比较
S804
特征数量
打印作业
打印机过程

图 9

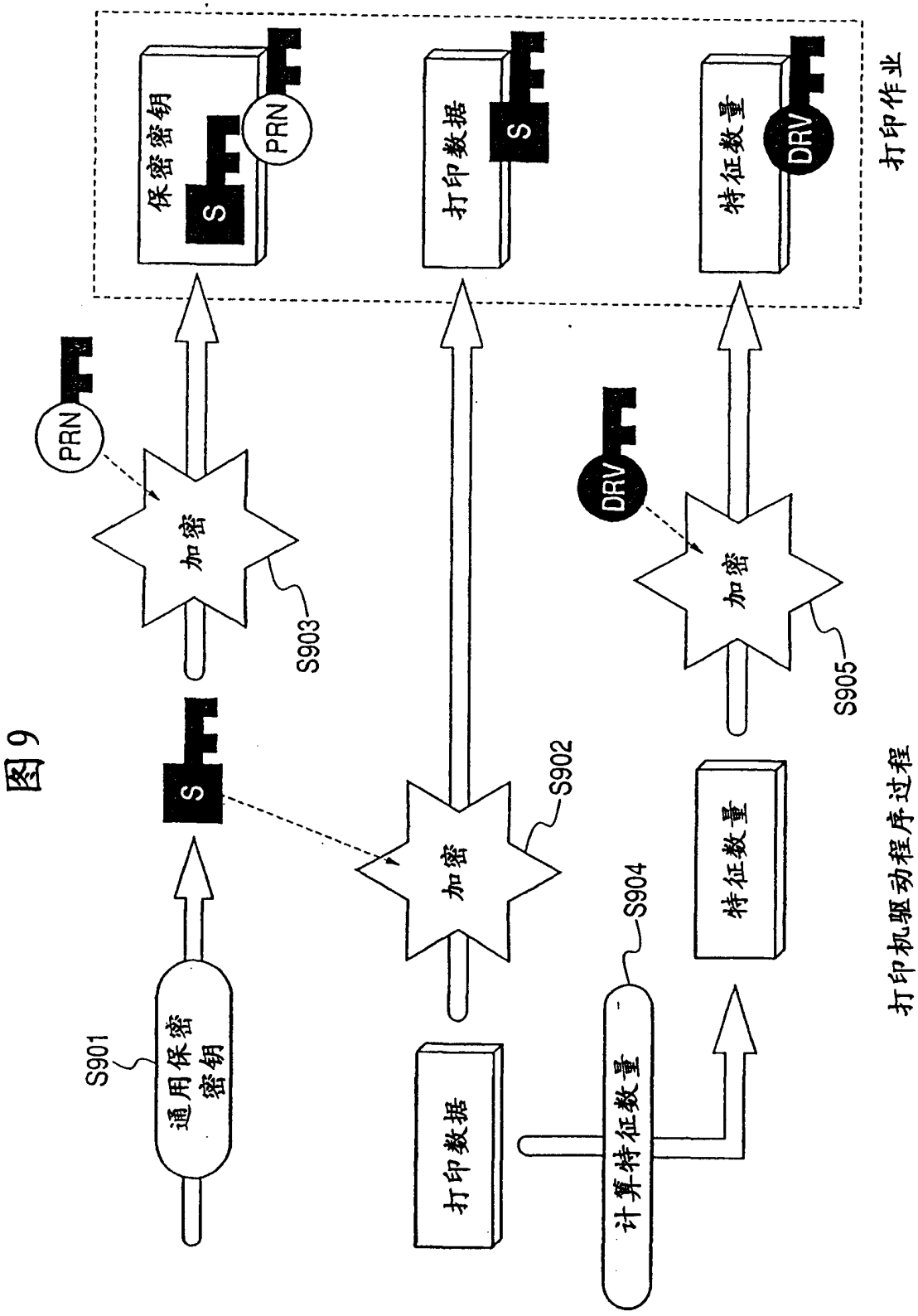

打印作业
保密密钥
S
PRN
打印数据
S
特征数量
DRV
PRN
加密
S903
S
加密
S902
DRV
加密
S905
S901
通用保密密钥
打印数据
S904
计算特征数量
特征数量
打印机驱动程序过程

图10

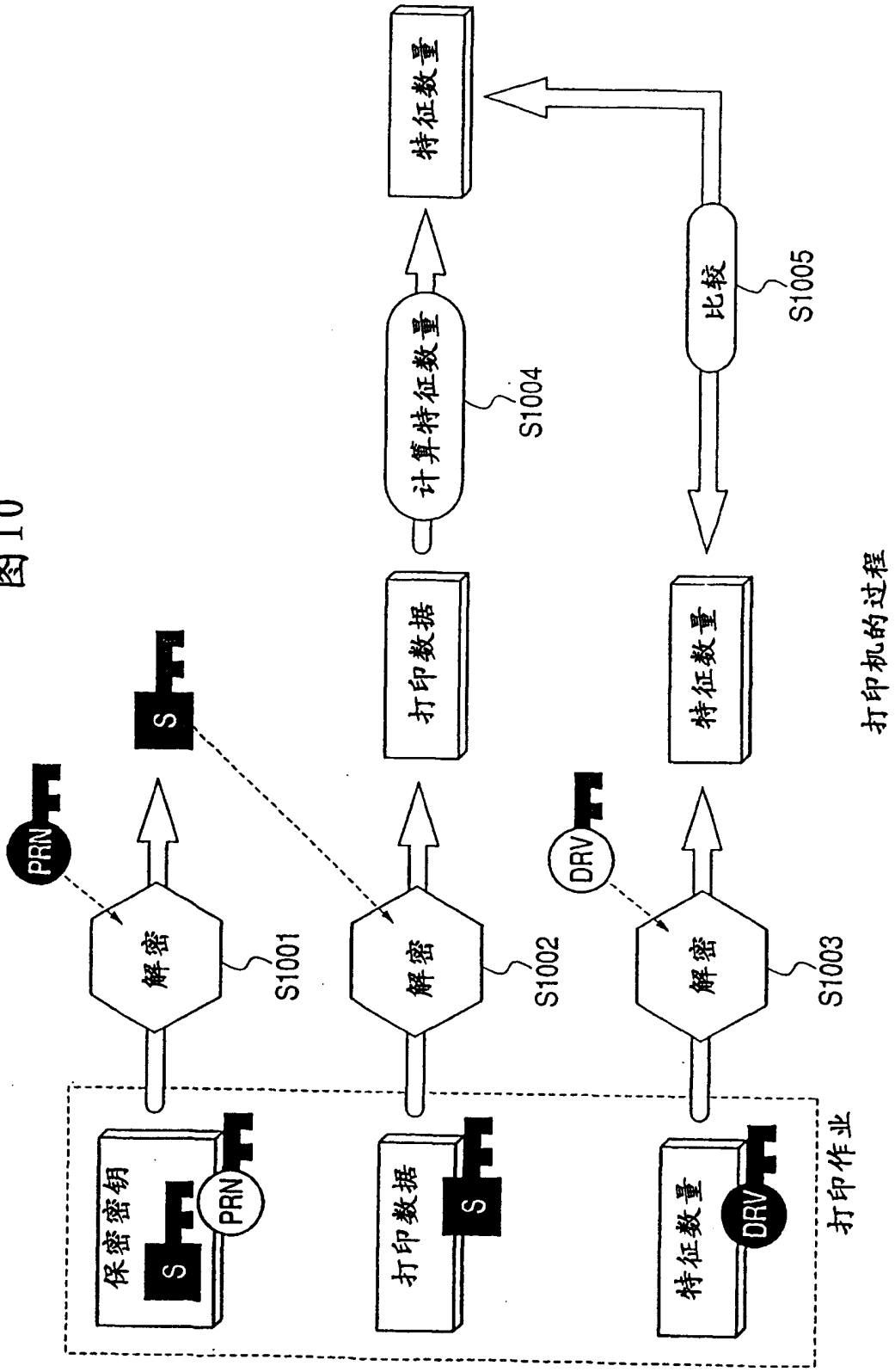

保密密钥
S
PRN
PRN
解密
S1001
S
打印数据
S
解密
S1002
打印数据
计算特征数量
S1004
特征数量
DRV
DRV
解密
S1003
特征数量
比较
S1005
特征数量
打印作业
打印机的过程

图11

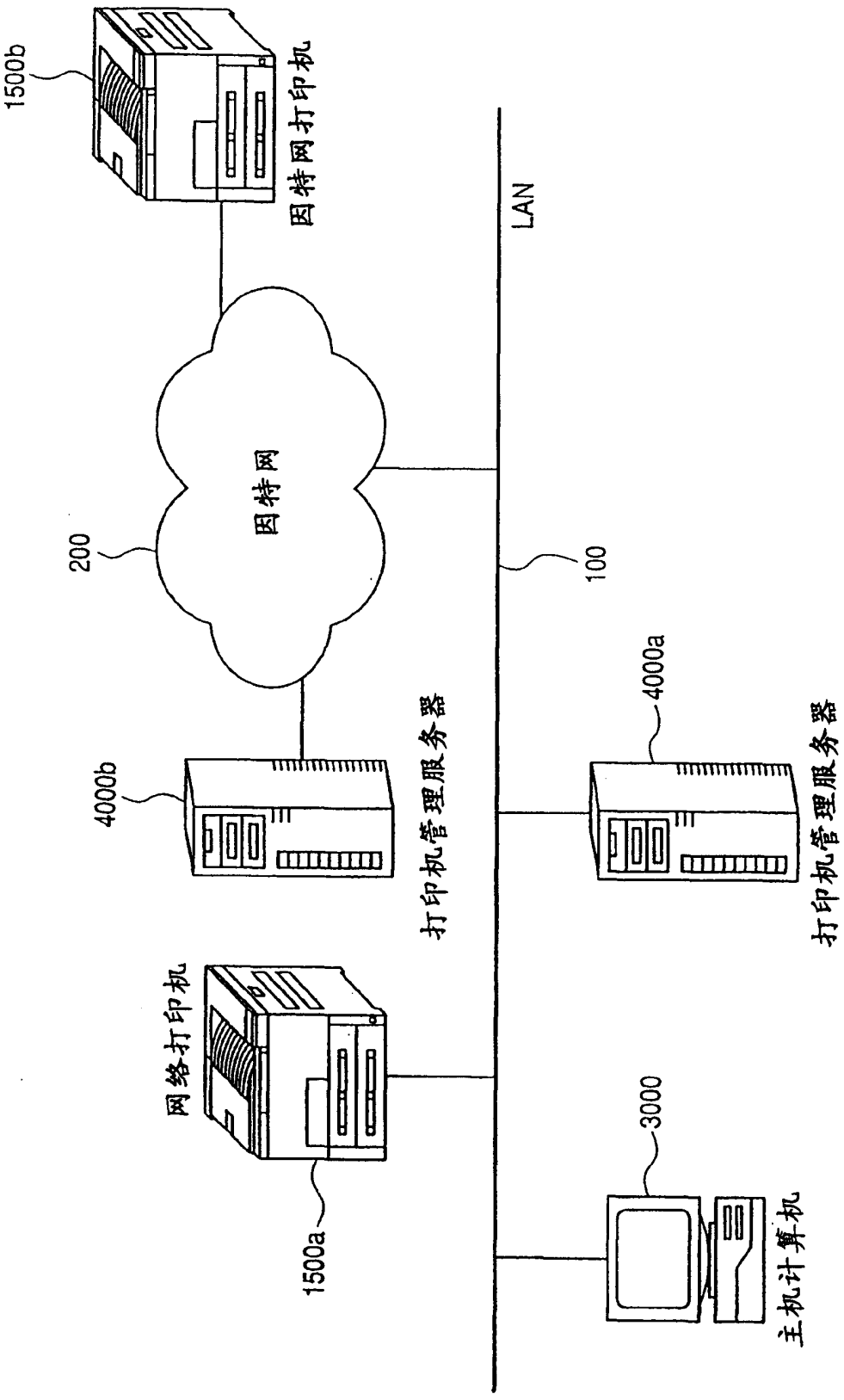

1500b
因特网打印机
LAN
因特网
200
100
4000b
打印机管理服务器
4000a
打印机管理服务器
网络打印机
1500a
3000
主机计算机

图12

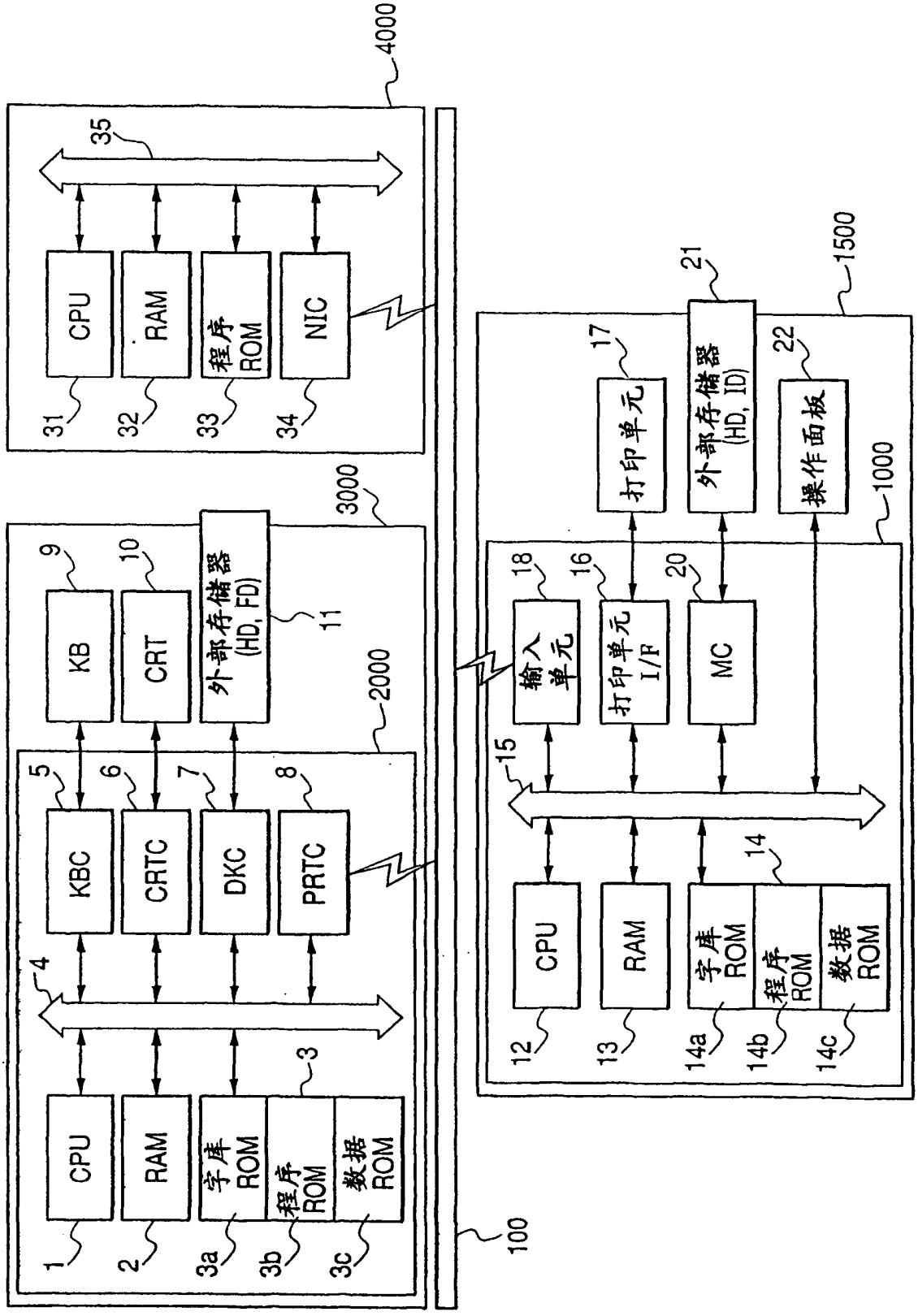

4000
35
CPU
RAM
程序 ROM
NIC
31
32
33
34
3000
9
10
KB
CRT
外部存储器 (HD, FD)
11
2000
5
6
7
8
KBC
CRTC
DKC
PRTC
4
CPU
RAM
字库 ROM
程序 ROM
数据 ROM
3
1
2
3a
3b
3c
100
1500
21
17
22
打印单元
外部存储器 (HD, ID)
操作面板
1000
18
16
20
输入单元
打印单元 I/F
MC
15
CPU
RAM
字库 ROM
程序 ROM
数据 ROM
14
12
13
14a
14b
14c

图13A

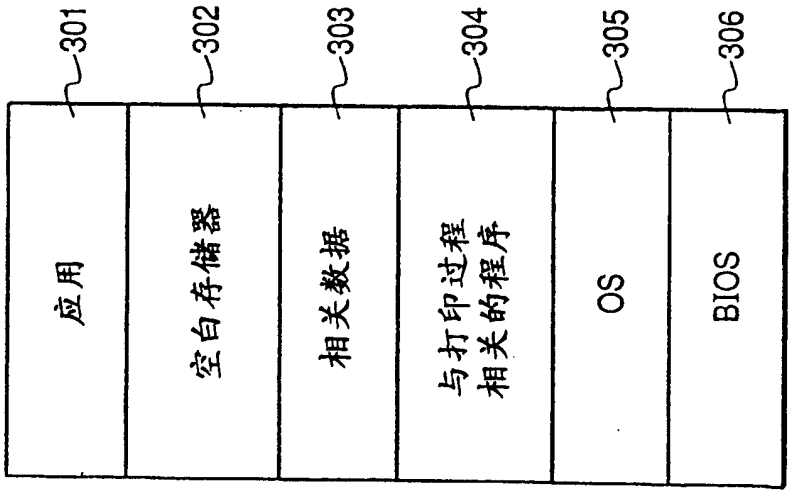


图13B

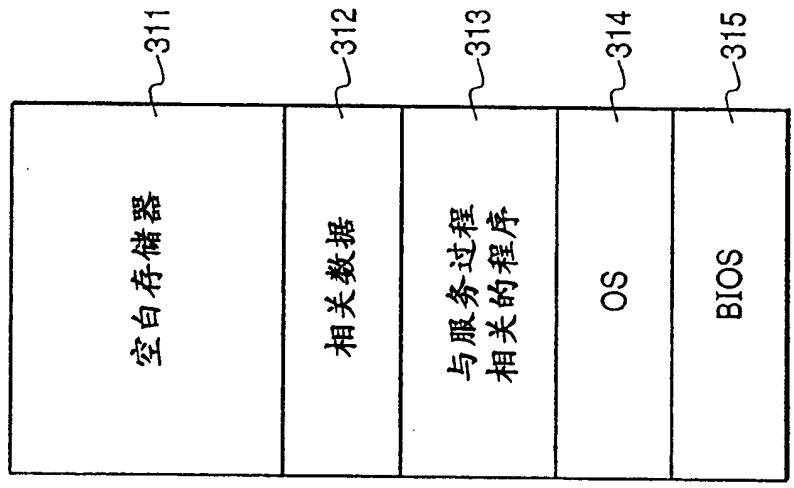


图13C

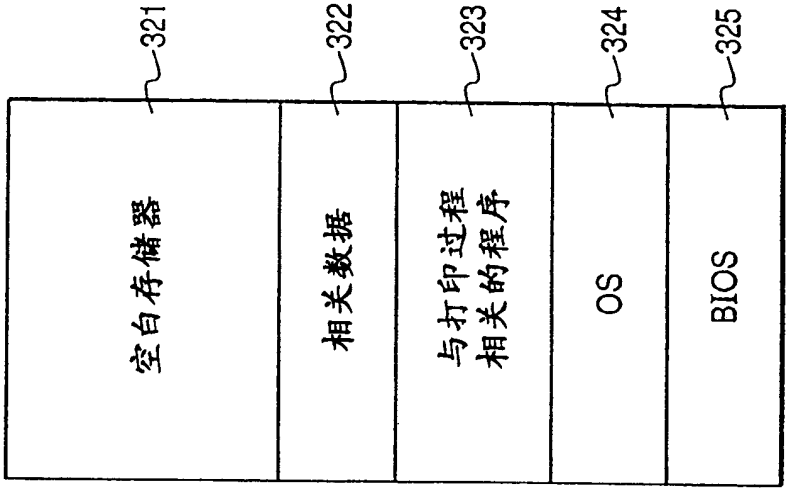


图14

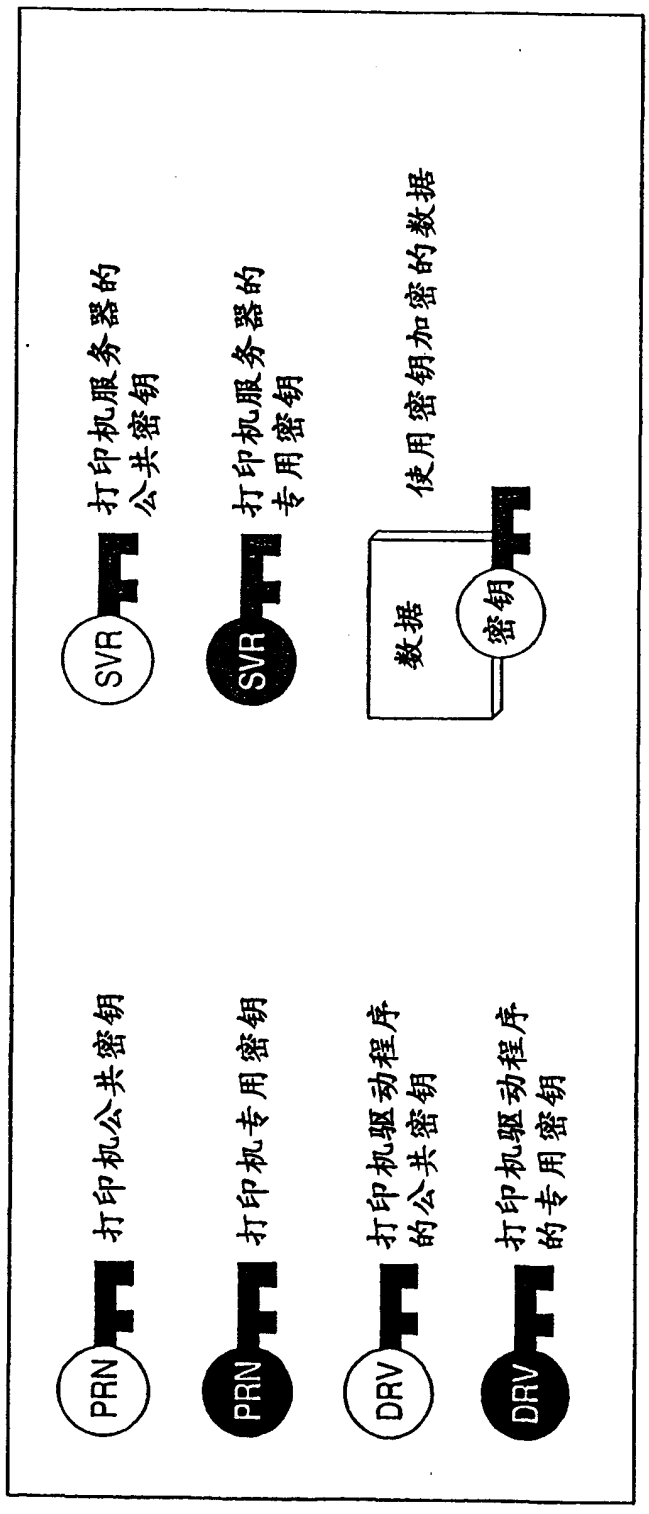

PRN
打印机公共密钥
PRN
打印机专用密钥
DRV
打印机驱动程序的公共密钥
DRV
打印机驱动程序的专用密钥
SVR
打印机服务器的公共密钥
SVR
打印机服务器的专用密钥
数据
密钥
使用密钥加密的数据

图15

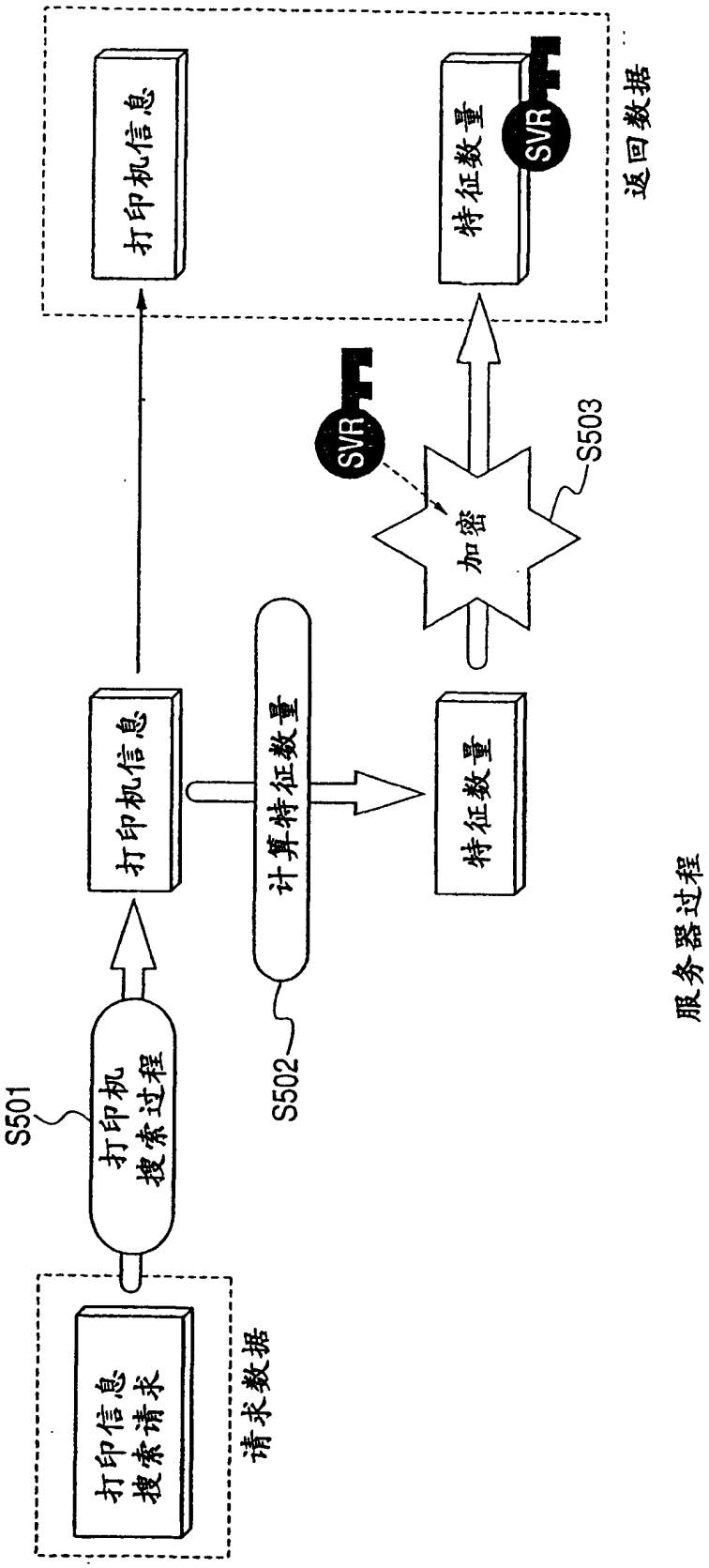

打印信息
搜索请求
请求数据
S501
打印机
搜索过程
打印机信息
计算特征数量
S502
特征数量
加密
SVR
S503
SVR
打印机信息
特征数量
返回数据
服务器过程

图 16

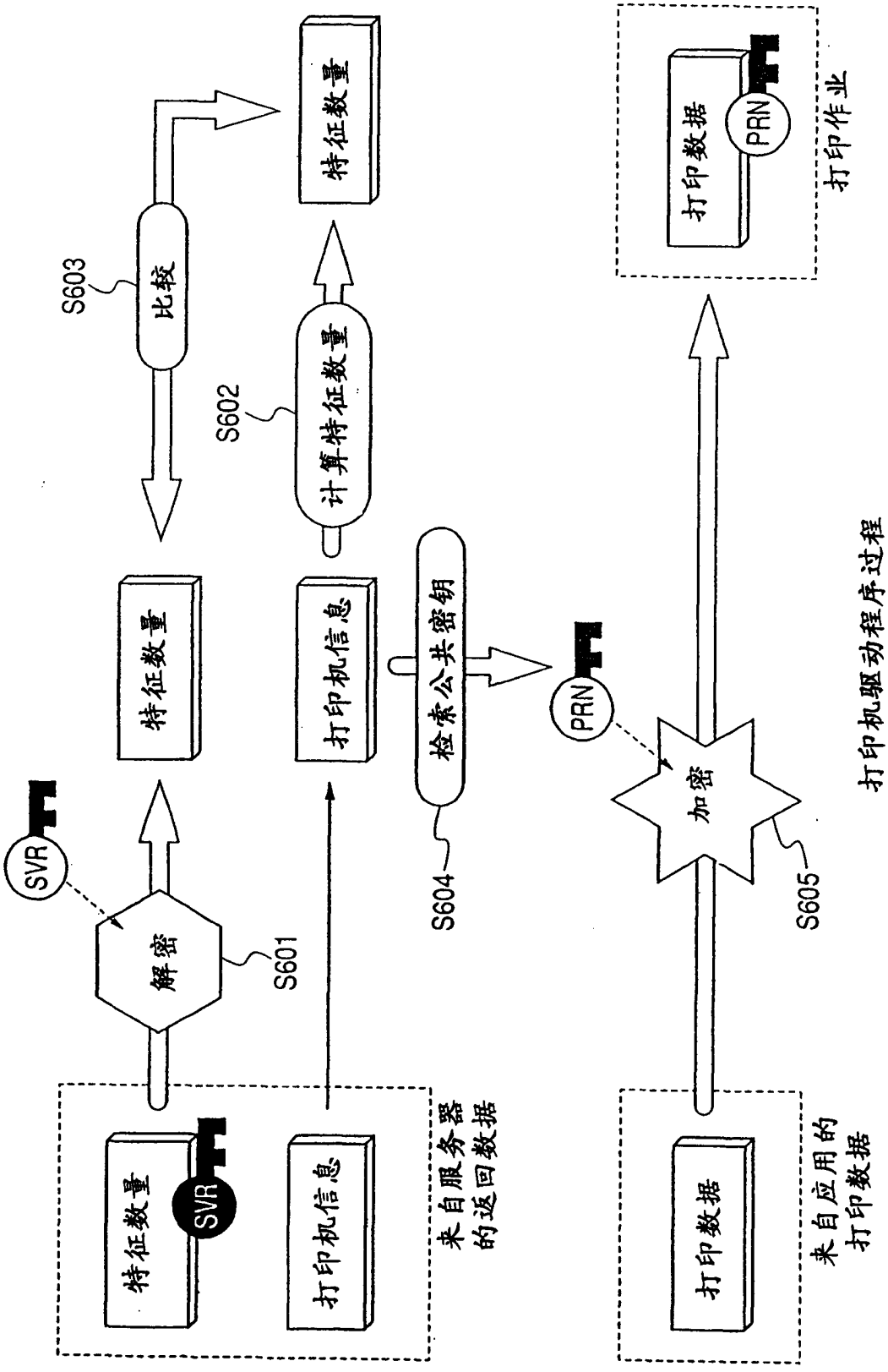

来自服务器的返回数据
特征数量
SVR
打印机信息
SVR
解密
S601
特征数量
打印机信息
S602
计算特征数量
S603
比较
特征数量
检索公共密钥
S604
来自应用的打印数据
打印数据
PRN
加密
S605
PRN
打印数据
打印作业
打印机驱动程序过程

图17

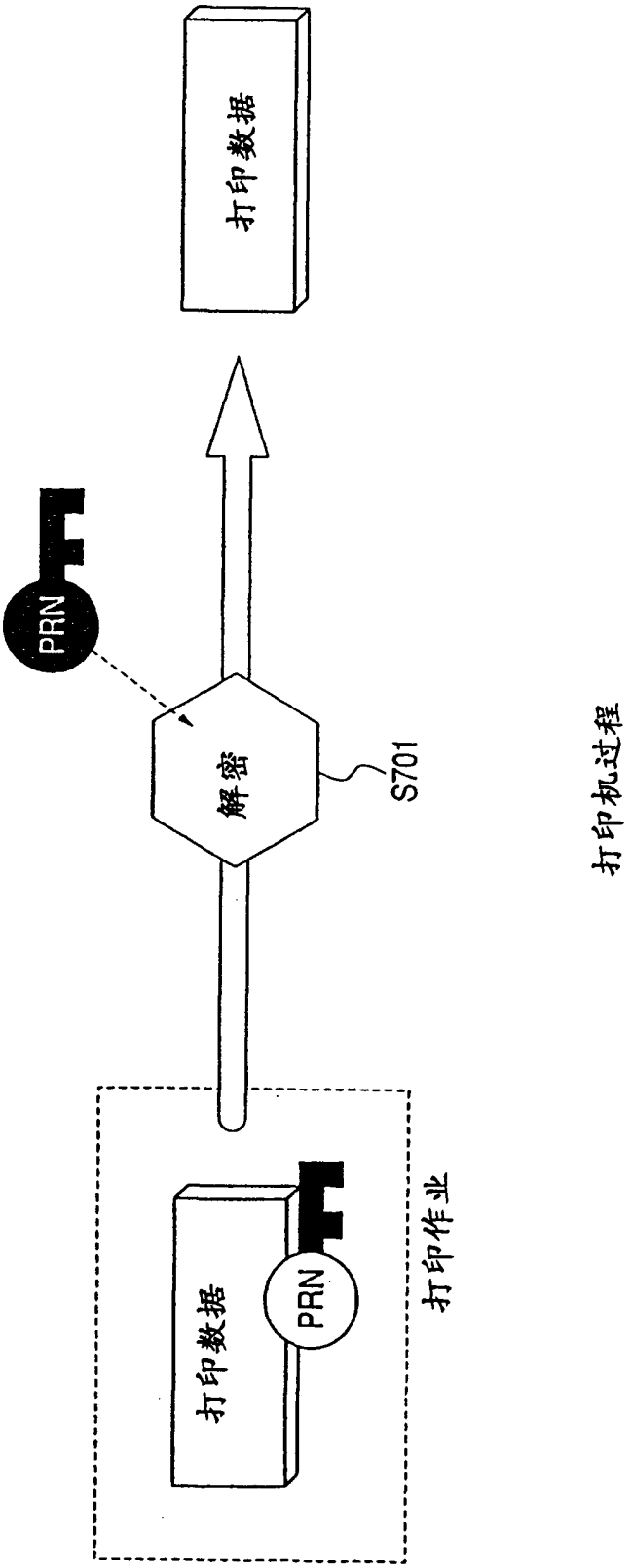


图18

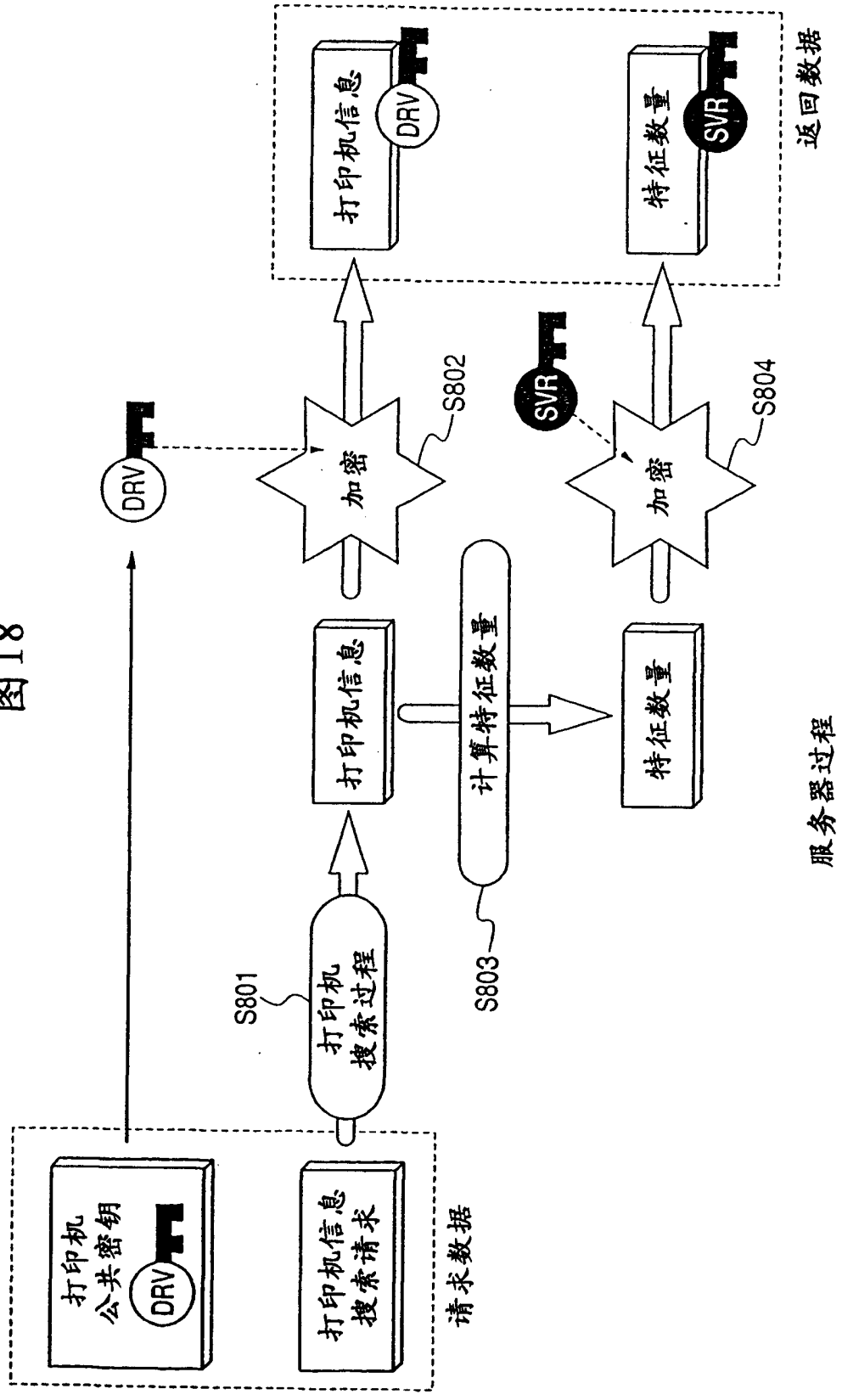

打印机
公共密钥
DRV
打印机信息
搜索请求
请求数据
S801
打印机
搜索过程
打印机信息
计算特征数量
S803
特征数量
DRV
加密
S802
SVR
加密
S804
打印机信息
DRV
特征数量
SVR
返回数据
服务器过程

图19

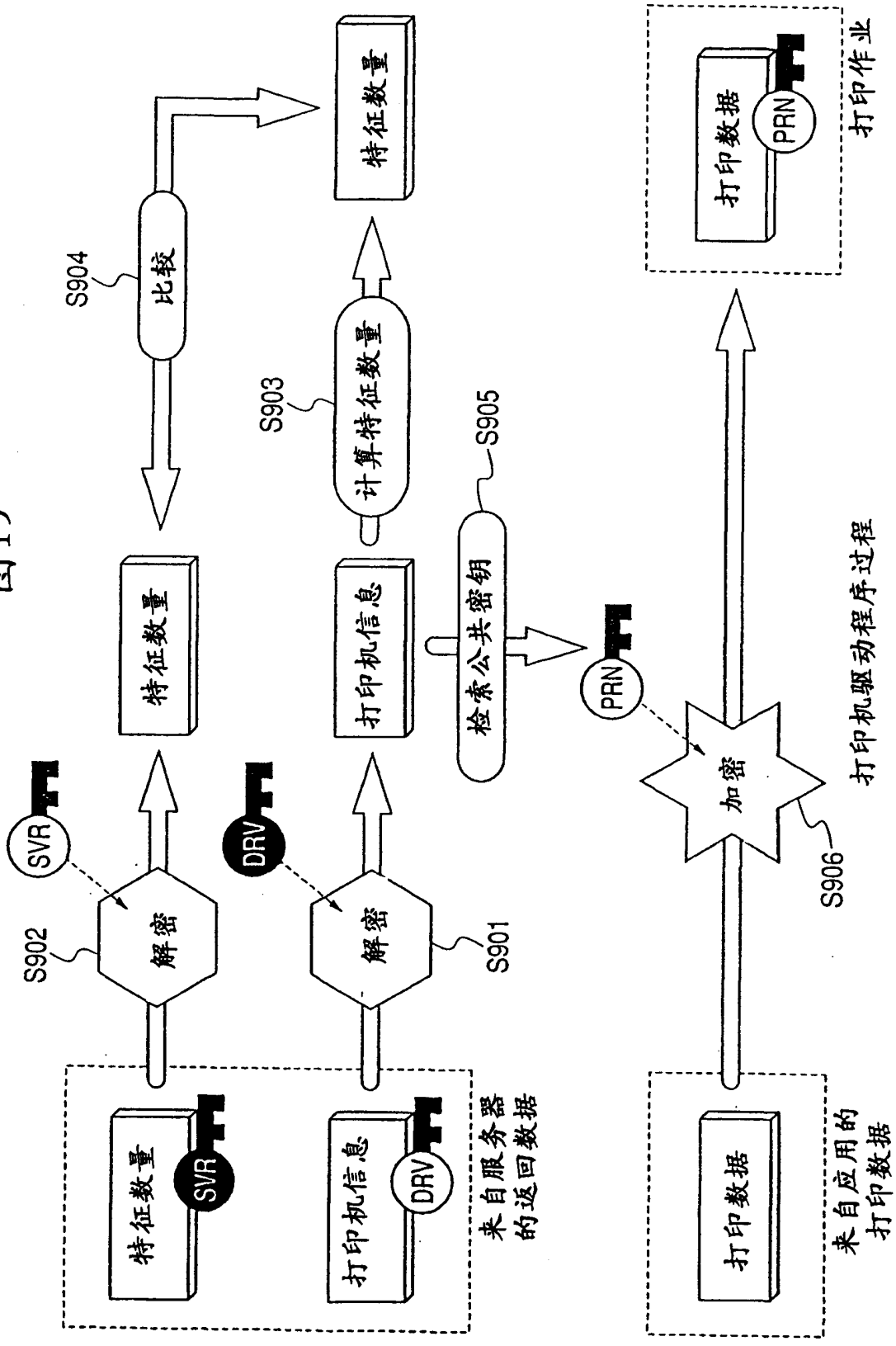

来自服务器的返回数据
来自应用的打印数据
打印机驱动程序过程
打印作业
特征数量
打印机信息
打印数据
SVR
DRV
PRN
解密
加密
检索公共密钥
计算特征数量
比较
S901
S902
S903
S904
S905
S906

图20

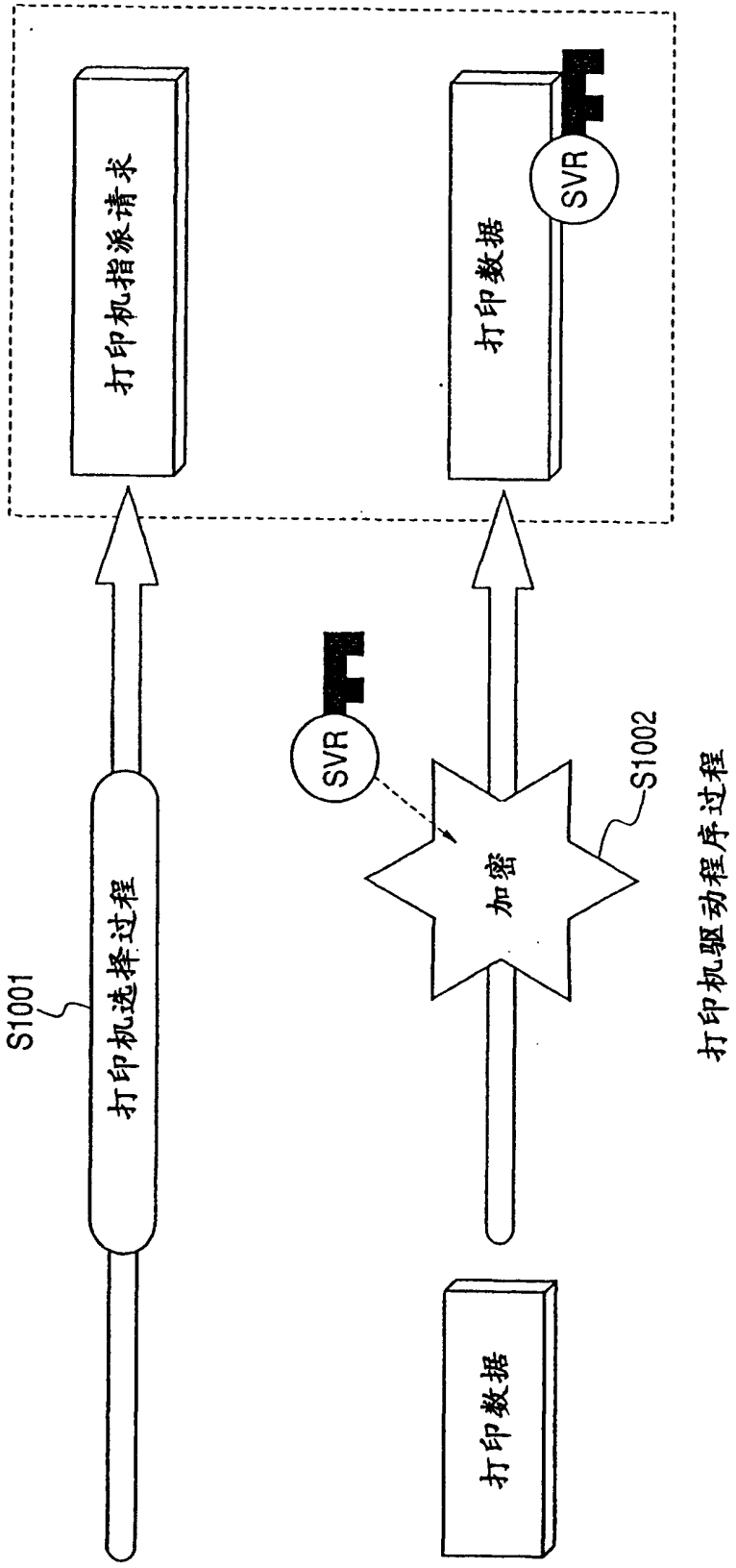


图21

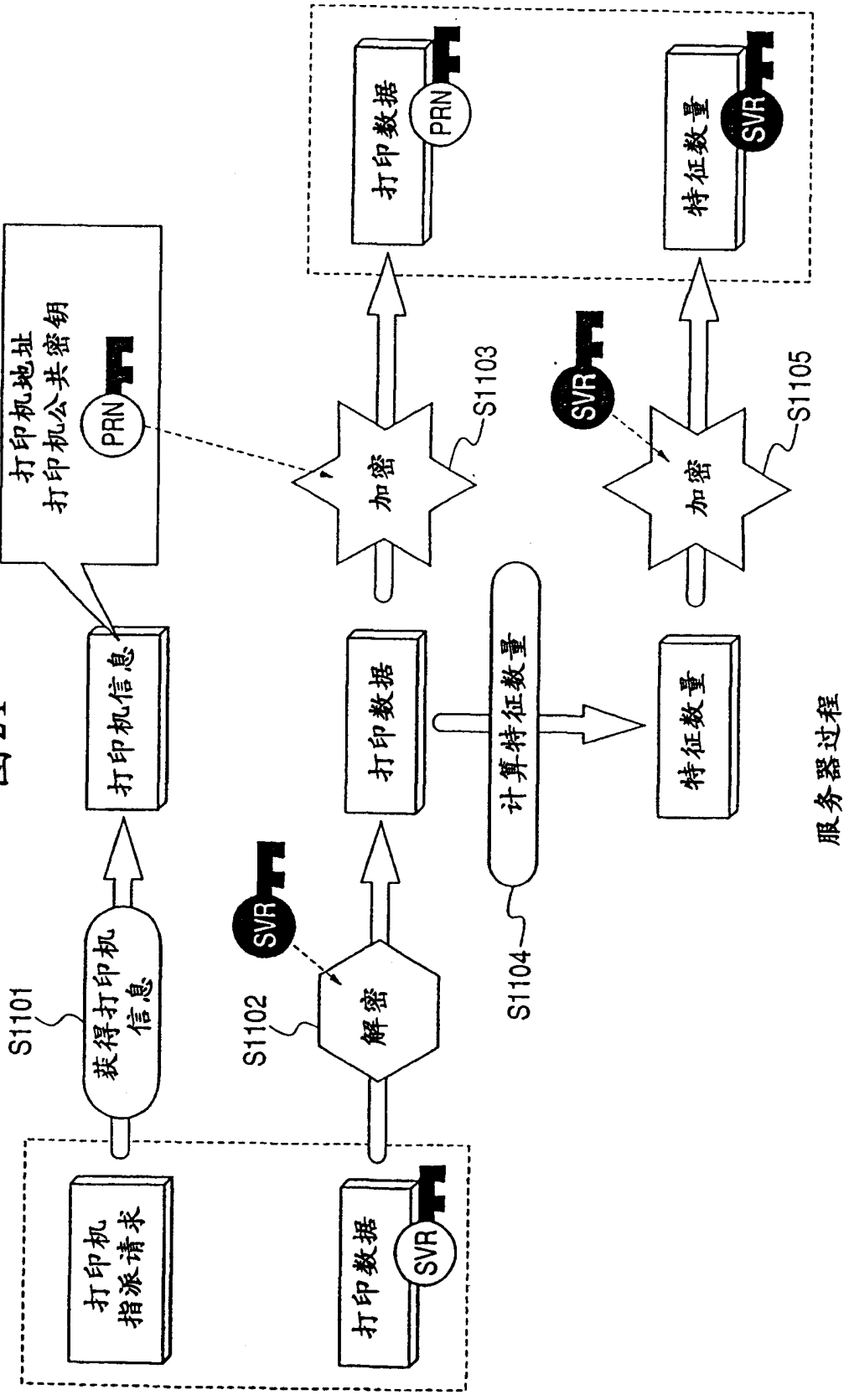

打印机指派请求
获得打印机信息
S1101
打印机信息
打印机地址
打印机公共密钥
PRN
SVR
打印数据
解密
S1102
计算特征数量
S1104
加密
S1103
打印数据
PRN
特征数量
SVR
加密
S1105
服务器过程

图22

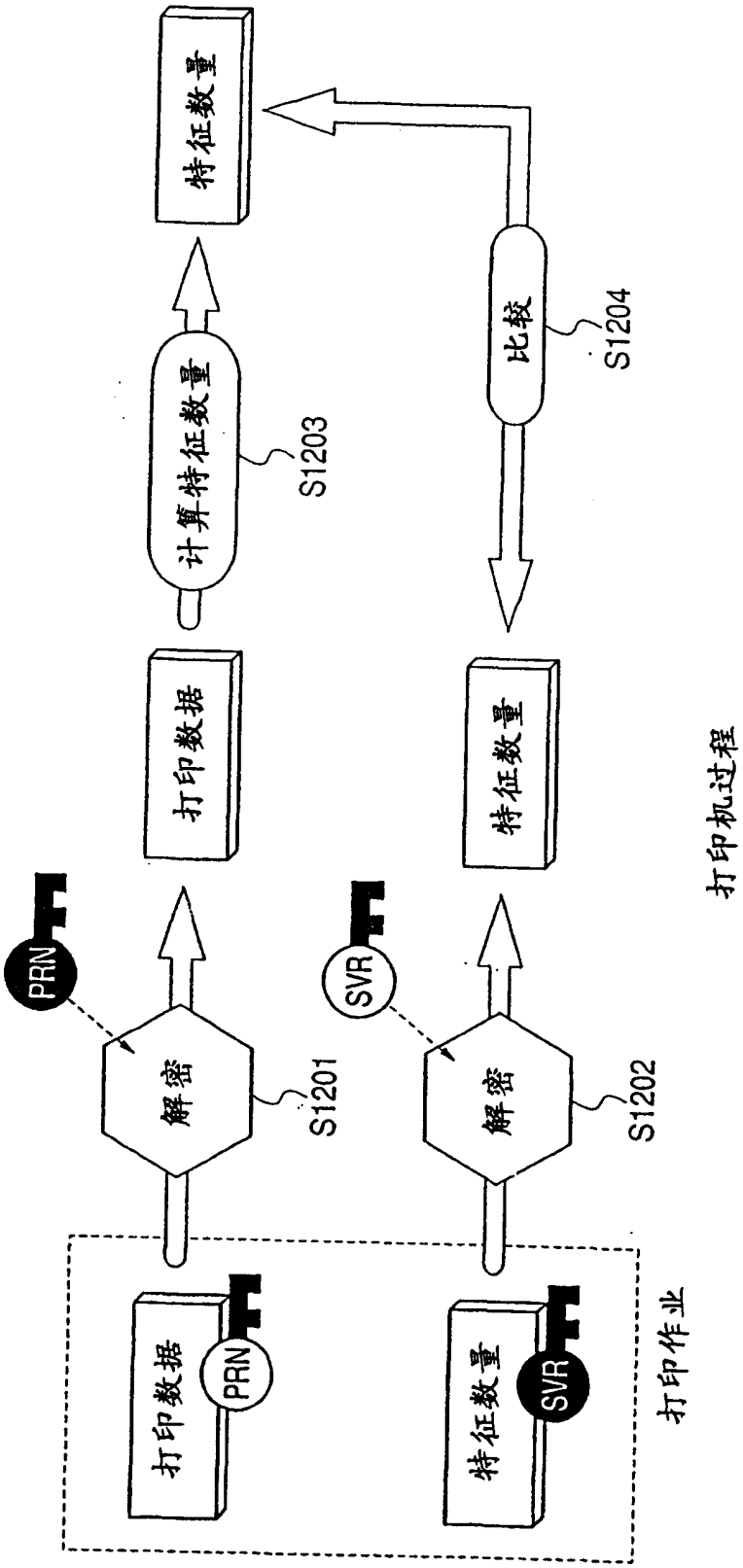
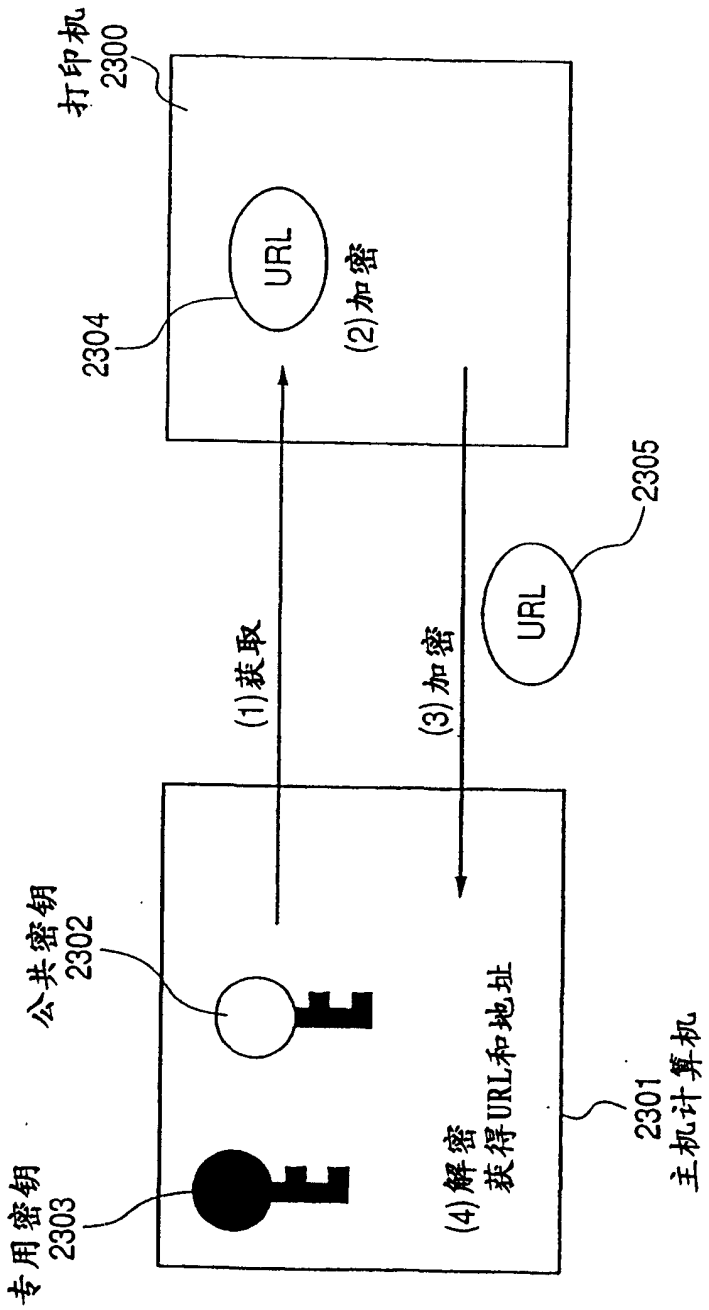

打印数据
PRN
特征数量
SVR
解密
S1201
解密
S1202
打印数据
特征数量
计算特征数量
S1203
比较
S1204
特征数量
打印机过程
打印作业

图23


打印机
2300
URL
2304
(2)加密
(1)获取
(3)加密
URL
2305
公共密钥
2302
专用密钥
2303
(4)解密
获得URL和地址
2301
主机计算机