(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105144189 A
(43)申请公布日 2015.12.09

(21)申请号 201380064100.4
(22)申请日 2013.12.06
(30)优先权数据
13/708,396 2012.12.07 US
(85)PCT国际申请进入国家阶段日
2015.06.08
(86)PCT国际申请的申请数据
PCT/US2013/073736 2013.12.06
(87)PCT国际申请的公布数据
WO2014/105395 EN 2014.07.03
(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 R·拉玛姆蒂 K·H·叶古罗
R·文卡特桑
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨丽
(51)Int.Cl.
*G06F 21/62*(2006.01)
*G06F 21/77*(2006.01)
*H04L 9/28*(2006.01)

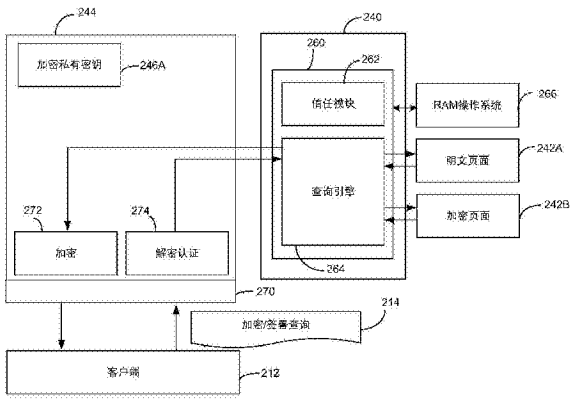
权利要求书2页 说明书13页 附图7页

(54)发明名称

安全云数据库平台

(57)摘要

一种用于在数据库上安全地处理查询的云计算服务。还公开了安全设备以及操作方法。安全设备可以置备有云服务的订户的私有密钥，并且可以具有使用该密钥的处理硬件，从而在硬件上隔绝密钥和加密处理使得包括云服务的操作人员的其他人无法容易地访问。安全设备内的处理可以解密接收自订户的查询并且可以加密响应以供在公共网络上传递。设备可以对明文执行函数，藉此限制云平台上处理的明文数据量，同时限制与订户的通信中消耗的带宽。此类处理可包括格式化由云平台使用的安全协议中的数据（包括查询中的自变量）。




CN 105144189 A

1. 一种被适配成用于提供云计算服务的计算设备，所述计算设备包括：

物理外壳；

置于所述外壳内的至少一个处理器，所述至少一个处理器被适配成在数据库上执行查询；

置于所述外壳内的网络接口，所述网络接口被适配成提供至网络的接口并且包括安全电路系统，所述安全电路系统包括：

解密组件，被适配成：

在网络上接收加密查询，所述查询接收自所述云计算服务的订户的设备，

处理加密查询以生成经处理查询，所述处理包括解密所述查询，以及

提供经处理查询以供由所述至少一个处理器执行；

加密组件，被适配成：

在所述至少一个处理器执行之后接收解密查询的结果，

加密结果，以及

在网络上向所述订户的设备传送加密结果。

2. 如权利要求 1 所述的计算设备，其特征在于：

所述网络接口包括连接到所述计算设备的总线的网络接口卡。

3. 如权利要求 2 所述的计算设备，其特征在于，所述网络是因特网并且所述总线是 PCI 总线。

4. 如权利要求 1 所述的计算设备，其特征在于：

所述安全电路系统进一步包括被配置有用于解密所述查询以及加密所述结果的至少一个加密密钥的硬件存储。

5. 如权利要求 1 所述的计算设备，其特征在于：

所述安全电路系统进一步包括查询转换组件，所述查询转换组件被适配成通过对解密查询执行转换来生成经转换的查询；以及

经转换的查询作为解密查询来提供以供由所述至少一个处理器执行；

所述安全电路系统进一步包括聚集组件，所述聚集组件被适配成：

解密所述查询的结果；以及

对解密结果执行聚集功能以产生经聚集的结果；

经聚集的结果作为解密查询的解密的结果被提供给加密组件。

6. 一种操作云数据库服务的方法，所述方法包括：

在提供非安全网络与数据库服务之间的接口的硬件组件内，所述数据库服务被配置成提供云数据库服务：

与所述云数据库服务的订户的计算设备交换查询和查询结果，所述查询和查询结果用第一加密格式来交换；以及

处理所述查询和查询结果以解密所述查询和加密所述查询结果；以及

与至少一个查询引擎交换经处理的查询以及由所述查询引擎对所述查询执行的结果，经处理的查询和执行的结果用至少第二加密格式来交换。

7. 如权利要求 6 所述的方法，其特征在于，进一步包括：

标识来自所述查询的以供在加密数据库上执行的一部分以及所述查询的其余部分；

在加密数据库上执行所述查询的所述一部分；以及

在明文数据库上执行剩余部分。

8. 如权利要求 7 所述的方法，其特征在于，进一步包括：

通过解密加密数据的至少一部分来生成明文数据库。

9. 如权利要求 8 所述的方法，其特征在于，进一步包括：

在所述查询的执行之后删除所述明文数据库。

10. 如权利要求 6 所述的方法，其特征在于：

所述查询的执行结果是加密数据；

所述方法进一步包括在所述硬件组件内对所述加密数据执行聚集函数。

# 安全云数据库平台

[0001] 背景

[0002] 在许多计算应用中，期望保持数据安全。例如，在医疗背景中，规定要求使用安全措施来阻止病人数据被未经授权方访问。如果财务数据（诸如企业顾客的信用卡号或社保安全号）被恶意方获得，则可能发生大量财务损失。

[0003] 为了保护数据，企业可以使用各种安全技术来维护他们自己的计算机系统以阻止对数据的未经授权的访问。企业可以使用物理和电子技术来控制对安全数据的访问。保护数据的一种替换办法（即便无法在所有情形中阻止对数据的访问）是在将数据存储在计算机系统中时对数据加密。

[0004] 已经被加密的数据或者以其他方式被如此处理从而即便未经授权方访问了该数据该未经授权方也无法确定数据的意义的数据有时被称为“密文”。在公司网络中，机密数据可以被存储为密文，除了在实际被处理时。通过控制能够将密文转换成“明文”的安全信息（诸如加密秘钥），可以通过限制数据在明文中的存在（除非在安全的高度限制的背景中）来维护数据安全。

[0005] 最近，数据正被存储在“云”中或者在“云”中被处理。云服务供应商（不是有数据要处理的企业）提供计算资源，包括处理和数据库存储。云服务供应商使得计算资源对顾客可用，每一个顾客与云服务供应商签订服务级协定（SLA）以能够访问对某一级别的计算资源。企业通过在因特网上提交作业来访问这些资源以在从云服务供应商“租赁”的计算机资源上进行处理。

[0006] 用于维护数据安全的传统技术在云环境中并不适用。尽管数据可以作为密文在因特网上传送，但一旦数据被云服务供应商接收，对于许多操作而言数据就被转换成明文。结果，（固有地在企业外部的）云服务供应商的雇员能够访问明文数据并且可能能够访问用于将密文转换成明文的安全信息。

[0007] 概述

[0008] 可以通过提供基于对订户唯一的安全信息对数据执行安全功能的硬件组件在云计算环境中提供安全数据库操作。结果，能够限制可访问明文数据的物理位置。数据可以仅对云环境的数据库节点内部可用，或者在一些实施例中，可以仅在安全设备内可用。在一些实施例中，安全设备具有适配成用于插入到数据库服务器中的标准槽的形状因子以使得明文数据的通信被限于内部服务器总线。

[0009] 此类安全设备可以在因特网或其他公共网络上接收加密的数据库命令。安全设备可以解密命令并且将它们提供给数据库服务器以供处理。当操作为查询时，查询结果可以被返回至安全设备，在安全设备处查询结果被加密以在公共网络上传输。

[0010] 在其他实施例中，数据库服务器可以接收采用与用于在公共网络上通信的加密格式不同的加密格式的命令。在这一实施例中，安全设备可以将查询从用于在公共网络上通信的加密格式转换成由数据库服务器使用的加密格式。由数据库服务器生成的结果可以被逆向转换。在一些实施例中，逆向转换可包括执行对命令处理的各部分。处理的该部分可包括聚集操作或任何其他合适类型的操作。

[0011] 在一些实施例中，转换命令可包括将命令拆分成各子命令。不同的子命令可具有不同的加密格式。一个子命令可以被格式化成用于至纯文本数据库的应用，而另一子命令可以被格式化成用于至加密数据库的应用。

[0012] 以上是对由所附权利要求定义的本发明的非限定性的概述。

[0013] 附图简述

[0014] 附图不旨在按比例绘制。在附图中，各个附图中示出的每一完全相同或近乎完全相同的组件由同样的附图标记来表示。出于简明的目的，不是每一个组件在每张附图中均被标号。在附图中：

[0015] 图 1 是利用安全计算设备的云计算平台的一示例性实施例的略图；

[0016] 图 2 是纳入安全设备的云数据库节点的一示例性实施例的功能框图；

[0017] 图 3 是纳入安全设备的云数据库节点的第二示例性实施例的功能框图；

[0018] 图 4 是纳入安全设备的云数据库节点的第三示例性实施例的功能框图；

[0019] 图 5A-5D 是由如本文所述的安全设备处理的数据库命令的示意性解说；以及

[0020] 图 6 是可用于实现本发明的一些实施例的示例性计算设备的功能框图。

[0021] 详细描述

[0022] 发明人已经认识和领会到，云数据库平台的利用可以通过用安全设备来装备云数据库平台来延伸。安全设备可以充当网络和一个或多个计算设备之间的接口，在该网络上订户访问云数据库平台，该一个或多个计算设备在云数据库平台内为该订户提供数据存储和检索资源。

[0023] 安全设备可以置备有对订户唯一的密码信息，诸如私有秘钥。这一置备可以至少部分地由订户或某一受信第三方来执行。结果，即使是云数据库平台的运营者也无法访问密码信息。这一密码信息可用于解密订户提交的查询和 / 或加密数据以响应于查询而返回至订户。

[0024] 安全设备可被配置成充当在其上交换查询和响应的非安全网络与订户之间的接口。安全设备可以与在其上可以执行查询的云数据库平台内的计算设备对接。

[0025] 虽然事实是安全计算设备被云数据库平台的操作者所有和 / 或在其控制之下，但仍然可以维护安全。可使用一个或多个技术来维护安全。在一些实施例中，可以通过将安全设备置于离在云数据库平台内执行查询的处理器紧密临近度的安全区域内来维护安全。虽然查询以及响应于该查询生成的数据的明文版本可以在安全设备与处理器之间交换，但将那些设备保持在紧密临近度的安全区域中可以使得难以访问该信息。在一些实施例中，安全设备可被安装在容纳该处理器的同一物理外壳中，并且可以通过计算设备的内部总线（诸如 PCI 总线）耦合至该处理器。对未经授权个体要访问云数据库平台内的计算设备内部的信息所提出的困难进一步增强了安全。

[0026] 在一些实施例中，云数据库平台可以用加密格式来存储数据。因而，即便未经授权个体获得对在安全设备与处理查询的处理器之间传递的信息的访问，该信息可能被加密。这一信息可以用与用于在不安全网络上传送信息的形式不同的形式来加密。尽管如此，即便未经授权个体获得对此形式的信息的访问，安全也不必受损。

[0027] 在此类实施例中，安全设备可在公共网络上接收加密查询。安全设备可以解密信息并且将其转换成第二形式以应用于云数据库平台内被配置成在加密数据库上执行查询

的计算设备。此类查询的结果可以被返回至安全设备以供处理以及在公共网络上传输至订户。

[0028] 在一些实施例中，安全设备内的处理可能需要解密加密结果。替换地或附加地，安全设备内的处理可包括对加密结果的操作。结果，经处理的查询结果可以被返回至订户，从而减少在公共网络上传递的信息量和／或为了访问查询结果由订户使用的客户端计算设备上要求的处理量。

[0029] 作为可以在安全设备内执行的处理的具体示例，安全设备可以执行聚集功能。聚集功能的示例包括对数据库中匹配查询的值和记录求和或者对数据库中匹配查询的记录数目进行计数。

[0030] 在一些实施例中，云数据库平台可以将数据部分地作为明文而部分地作为加密数据来存储。安全设备上的处理可能需要拆分查询以使得各个部分一些部分可以被应用于能够访问明文数据的处理器而其他部分被应用于能够访问受保护数据的处理器。用安全设备来处理结果可能需要将从明文数据生成的结果与从加密页面生成的结果相组合。此类处理可涉及解密加密页面以使得它们可以与明文页面相组合。

[0031] 此类云数据库平台可用于存储和访问任何合适类型的数据。例如，安全的云数据库平台可用于实现对关于个体的敏感医疗信息的处理。在这一示例中，医疗信息（无论是查询的一部分还是响应于执行查询而返回的结果的一部分）可以作为密文来传送。即便这一传输在公共网络上进行，传输中的数据安全可以通过对数据的加密来维持。

[0032] 在云数据库平台处接收到查询之际，这一查询可以在安全设备内被解密。数据安全可以使用本文描述的任何一个或多个技术来维持。应当领会，处理健康信息仅仅是可以在云计算平台上执行同时维持数据安全的处理的一个示例。本文所述的平台可用于任何合适的数据处理。在一些实施例中，安全设备可被配置成用于执行如由该安全设备已经被分配给其的订户所指定的操作，并且那些操作可以生成数据以供云中的进一步处理或以供加密和传输给订户。

[0033] 在一些实施例中，安全设备可以用阻止对作为安全计算设备的正常操作的一部分正在设备内部被处理的明文数据的访问的物理安全措施来实现。安全设备的物理构造可以通过显示对明文数据和／或用于设备内的安全处理的安全信息的访问来阻止或者至少极大地妨碍旨在获得对明文数据的访问的恶意活动而无需对设备的物理修改。如果未经授权的访问要求对设备的物理修改，该未经授权的访问可以被容易地检测到并且可以采取纠正措施来维持安全。

[0034] 相应地，在一些实施例中，安全设备可具有如此的架构以使得明文数据仅在安全设备内部的半导体设备内部可用。可以采用已知技术来构造这些半导体设备以确保无法使用电磁、热和／或其他非破坏性感测技术来检测到明文数据。例如，可以采用半导体设备的封装中的金属屏蔽板和／或确保承载明文数据的导体被嵌入在设备中的架构来确保那些导体上的信号无法容易地从半导体设备的外部检测到。可以替换地或附加地采用已知技术来妨碍对安全设备的操作的更改，这些更改可能导致安全设备揭露它用于对敏感数据的安全处理的密码信息。作为另一示例，明文数据可能出现在其外部的半导体设备封装外部的任何线缆可以被包裹在环氧树脂或不得不被物理更改以获得对明文数据的访问的其他材料中。

[0035] 用于实现安全设备的合适的半导体设备可以是可编程逻辑设备，诸如场可编程门阵列 (FPGA)。一些已知的 FPGA 设备包括促进仅由授权方进行安全编程的加载的特征。在此可以使用此类特征来允许云数据库平台的订户控制安全设备执行的程序，即便安全设备位于云数据库平台的操作者的场所处。相应地，FPGA 可以无需修改地使用或者在一些实施例中可以纳入除了常规 FPGA 设备中的那些特征之外的特征来支持安全计算设备的附加功能。

[0036] 安全设备可以采用一个或多个技术来保护安全。此类技术可能需要仅在安全设备的内部组件内对敏感明文数据执行处理，以使得即使云数据库平台的管理员也无法访问敏感明文数据。

[0037] 在其中安全设备是可编程的实施例中，可以通过在用要对设备编程的指令配置设备之前验证那些指令来维持安全。可以使用任何合适的技术来验证指令集。在一些实施例中，指令集可以用加密、密码签署、或者以其他方式用安全信息处理的格式被加载到安全设备中。安全设备可以对指令集执行密码处理以确保它们用对应于受信源的安全信息来处理。

[0038] 在一些实施例中，不同类型的信息可以被不同地处理以维持安全。在一些实施例中，安全设备可以使用引导进程来加载已知是安全的信息。引导进程例如可依赖于在设备的操作之前加载到安全计算设备中的与受信源相关联的密钥安全信息（诸如密钥）。

[0039] 与受信源相关联的这一预先加载的安全信息可由安全设备用来验证设备的操作期间所提供的信息。在一些实施例中，安全信息可由安全设备用来验证将设备配置成为具体订户执行安全操作的配置信息。该配置信息可包括与具体顾客相关联的进一步的安全信息，该安全信息可以解密和 / 或加密查询和 / 或与为该具体顾客执行的操作相关联的数据。替换地或附加地，配置信息可包括加载器程序，加载器程序可以加载由顾客提供的指令集以执行安全操作。加载器程序可以被适配成用与具体订户相关联的安全信息来操作以使得对安全设备的编程被限于该具体顾客。

[0040] 此种办法提供了配置安全设备方面的极大灵活性，而云数据库平台的操作者无法访问任何安全信息。为了允许云平台用于针对具体订户的安全处理，云数据库平台的操作者可以分配供具体订户使用的安全设备。之后，该安全设备可自动地与受信授权方和 / 或它被分配给的具体订户交互。

[0041] 转向图 1，解说了一示例性计算环境 100。环境 100 包括云数据库平台 130。如在常规云数据库环境中的那样，云数据库平台 130 包括处理和数据存储资源。在这一示例中，那些处理资源由计算设备 140 和 150 解说。存储资源由数据库 142 和 152 解说。

[0042] 在这一示例中，数据库 142 可以是明文数据库。计算设备 140 可以被配置有查询引擎以对照数据库 142 执行明文查询。数据库 152 可以是加密数据库，存储在数据库中的一些或全部数据以加密形式被存储。计算设备 150 可以被配置有查询引擎以对照数据库 152 执行加密查询。

[0043] 作为一具体示例，数据库 152 可以存储健康信息。与健康信息相关联的任何个人可标识信息可以用加密形式被存储在数据库 152 中。因而，如果数据库 152 包含关于名为 John Smith 的病人的信息，则姓名“John Smith”将不会出现在数据库 152 中。相反，姓名“John Smith”的加密形式将会出现。作为示例，姓名“John Smith”的加密形式可能作为

“AGF$#*%”出现。相应地，寻找关于 John Smith 的信息的查询引擎将在数据库 152 中搜索包含加密姓名“AGF$#*%”的记录。

[0044] 尽管图 1 仅示出云数据库平台 130 内的两个计算设备和两个数据库，但应当领会，云数据库平台可以具有许多计算设备和许多数据库，这些计算设备和数据库在操作中被分配给从云数据库平台 130 的操作者获得数据库服务的订户。相应地，应当领会，为了简明起见，云数据库平台 130 的许多细节从图 1 中被略去。

[0045] 图 1 示出可以通过相应的客户端计算设备 112A、112B 和 112C 访问云数据库平台 130 的多个订户 110A、110B 和 110C。如在常规云数据库平台中的那样，客户端计算设备通过网络 120（可以是因特网）连接到云数据库平台 130。

[0046] 因为网络 120 可以是公共网络或其他非安全网络，订户可以为与云数据库平台 130 交换的信息使用加密。以此方式，明文信息可以仅存在于订户场所 109 内以及拥有云数据库平台 130 的组件的设施内。那些设施之间的通信行经可以被加密成使得即便通信由未经授权的第三方截取，该第三方也可能无法使用该通信中包含的信息。

[0047] 为了支持这一加密功能，订户（诸如订户 110B）可以具有密钥 114。当订户 110B 向客户端计算设备 112B 输入查询时，在客户端计算设备 112B 上执行的加密程序可以在密码计算中使用密钥 114 来生成加密查询 116。加密查询 116 代替由订户 110B 生成的查询的明文版本可以在网络 120 上传递。

[0048] 在云计算平台 130 处，对应的密钥可以被应用以解密加密查询 116。在这一示例中，密钥 146A 可以与密钥 114 互补，以使得云计算平台 130 内的计算设备可以使用密钥 146A 来解密查询。这一查询一旦被解密就可被查询引擎应用来搜索数据库 142 和 / 或 152。在其中查询要被应用以搜索加密数据库 152 的实施例中，可能要求对查询的某种转换，以使得该查询尽管最初使用明文将指定如它们出现在加密数据库 152 中那样的值。

[0049] 在一些实施例中，这一解密和转换的部分或全部可以在计算设备 140 和 / 或 150 内进行。然而，在图 1 解说的实施例中，云计算平台装备有安全设备 144。出于安全理由在云计算平台 130 处执行的与加密 / 解密以及对查询的转换有关的处理的部分或全部可以在安全设备 144 内执行。安全设备 144 可以是如本文所述的由云计算平台的操作者所有的且被分配给订户的计算设备。尽管图 1 仅示出了在这一示例中单个安全设备 144 被分配给订户 110B，但支持多个订户的云计算平台可以包含多个安全设备（为简明起见并未明确解说）。

[0050] 可在安全设备 144 内执行任何合适的处理。在一些实施例中，所执行的具体处理可以由在订户 110B 的控制之下加载的程序来指定。该处理可以使用同样在订户 110B 的控制之下被加载的密钥。此外，安全设备 144 可以按照如此方式被配置和封装以使得安全设备 144 内的数据无法使用容易获得的工具来访问。以此方式，即便是云计算平台 130 的操作者的人员也无法容易地访问安全设备 144 内的编程和密钥或其他安全信息。

[0051] 在图 1 的示例中，密钥 146A 和 146B 被解说。这些密钥解说了可以为不同的安全功能使用不同的密钥。例如，可以使用密钥 146A 来解密订户 110B 发送的加密查询和 / 或加密返回至订户 110B 的执行那些查询的结果。密钥 146B 可用于与访问加密数据库 152 中的数据的安全功能相关联。例如，密钥 146B 可以在转换解密查询以应用于加密数据库 152 中被使用。替换地或附加地，密钥 146B 可以在解密通过查询加密数据库 152 返回的加密结

果中被使用。具有用于解密来自加密数据库 152 的结果的密钥可允许安全设备 144 内的安全处理以包括对从加密数据库 152 中的加密信息中导出的明文数据的操作。

[0052] 安全设备 144 提供的安全处理可以用多种方式中的任一种来使用。所执行的具体处理可取决于期望的安全级别。图 2 是提供第一安全级别的实施例的示例。图 2 示出被配置有在操作系统环境 260 内执行的查询引擎 264 的计算设备 240(诸如数据库服务器)。同样在操作系统环境 260 中执行的是信任模块 262。信任模块 262 可确保计算设备 260 引导进入已知状态,该已知状态例如可以是未被病毒破坏的状态。另外,信任模块 262 可允许计算设备 240 以加密形式将信息维持在块存储中。

[0053] 相应地,图 2 的示例包括加密页面 242B。为了处理查询,加密页面 242B 的某一部分可以被信任模块 262 转换成明文页面 242A。操作系统环境 260 可以控制哪些加密页面被转换成明文页面 242B 以及何时删除明文页面 242A。操作系统进行的这一处理可以访问 RAM 266。

[0054] 在这一示例中,查询引擎 264 被配置成执行纯文本查询。当查询被应用于查询引擎 264 时,对照明文页面 242A 来应用该查询是可能的。此类查询的结果以明文形式被返回。这样的处理可以使用本领域已知的技术来执行。尽管计算设备 240 内的此类处理可以用任何合适的方式来执行。

[0055] 为了提供安全,即便在与客户端 212 交换查询和结果时可以在公共网络上传送查询和结果,但安全设备也可被纳入云计算平台的场所。在这一示例中,该安全设备可以被实现为网络接口组件 244 的一部分。

[0056] 安全设备可包括物理网络接口 270,以允许安全设备直接连接到通过其可以与客户端 212 交换通信的网络。在这一示例中,收到的通信可以采用由客户端 212 上的密码处理加密和 / 或签署的查询 214 的形式。同样地,结果可以在通过物理网络接口 270 被传送到客户端 212 之前被加密和 / 或签署。

[0057] 为了支持加密和 / 或签署以及解密和 / 或验证签署通信所必要的密码处理,安全设备可被配置有密钥 246A。该密钥可以是加密私有密钥或者可以用任何合适的形式来存储。如上所述的技术或任何其他合适的技术可用于以安全的方式用密钥 246A 来配置安全设备。

[0058] 在图 2 的示例中,密钥 246A 在组件 274 中被使用来解密和认证接收自客户端 212 的查询。得到的明文查询可以被应用于查询引擎 264。作为查询引擎 264 执行查询的结果所返回的明文结果可以在组件 272 中被处理。组件 272 中的处理可以加密执行查询的明文结果以供通过物理网络接口 270 传输回客户端 212。

[0059] 在这一示例中,组件 272 和 274 可以通过对作为安全设备的一部分的 FPGA 编程来实现。此类编程可以按照如此方式来完成以使得私有密钥 246A 的未加密版本在没有破解进入到 FPGA 的内部处理中的极端措施的情况下无法被访问。但是,应当领会,用于执行安全设备内的密码处理的具体技术和硬件对于本发明并非是关键性的,并且可以使用任何合适的技术和硬件。

[0060] 图 3 解说了其中可以提供附加安全的替换实施例。图 3 示出被配置有查询引擎 364 的计算设备 340。如关于图 2 中示出的实施例那样,加密页面 342B 可以用团块形式的被存储。类似地,RAM 366 可用于由操作系统环境 360 的各组件使用。

[0061] 然而，在这一实施例中，代替解密页面，加密页面 342A 可以从团块加密页面 342B 中被选出并且被复制到更快的存储器中。查询引擎 364 可以对照加密页面 342A 来执行查询。因为页面被加密，查询引擎 364 可以处理为应用于加密页面而格式化的查询。

[0062] 相应地，安全设备可以接收查询并且将查询转换成由查询应用 364 应用于加密页面的格式。如对于图 2 中的实施例那样，安全设备可以被实现为网络接口组件的一部分。在图 3 的具体示例中，该网络接口组件可以是通过计算设备的其他内部总线的 PCI 总线连接到计算设备 340 的处理组件的网络接口卡。

[0063] 相应地，图 3 示出网络接口组件 344 在与为计算设备 340 执行处理的组件相同的外壳 330 中。外壳 330 例如可以是服务器机架的外壳。但是，应当领会，可以使用任何合适的外壳来包裹安全设备和计算设备 340 的处理组件两者。在一些实施例中，外壳可以是服务器的壳体。无论包裹安全设备、处理组件以及将其互连的总线的外壳的具体构造如何，此类安排可以提供减少未经授权的第三方访问数据的机会的物理安全。相应地，此类外壳可以在本文描述的任何实施例中使用。

[0064] 在所解说的示例中，客户端 312 生成加密 / 签署查询 314。查询 314 可以在公共网络（诸如因特网）上传送。该查询可以在物理接口 370 处接收，物理接口 370 可以是网络接口卡 344 的一部分。同样实现在网络接口卡 344 上的可以是用于执行安全功能的组件。另外，加密私有密钥 346A 可以被存储在网络接口卡 344 上。如图 2 中解说的实施例中那样，加密密钥可按照如此方式被存储以使得它在安全设备内执行安全处理的组件外部不被使用。

[0065] 在所解说的实施例中，那些组件可包括解密和认证查询 314 的组件 374。可以采用纯文本的解密查询可以被提供给转换查询的组件 378。

[0066] 组件 378 内的转换可能需要将查询格式化成应用于查询引擎 364。在这一示例中，查询引擎 364 将查询应用于加密数据库。相应地，组件 378 内的转换可能需要将查询中的项格式化以使得它们匹配加密页面 342A 中的对应项。此类处理可以使用密钥（诸如密钥 146B（图 1）或用于处理技术的任何其他合适的密钥）来执行。以此方式，查询内包含的敏感数据可以仅在安全设备内可用。

[0067] 在转换组件 378 和安全设备内的其他组件内执行的处理可以由订户基于用于存储在加密页面 342A 中的数据的加密形式来指定。例如，组件 378 可以被编程为标识与数据库中对其使用加密的字段相对应的值。这一信息可以是在编程时先验地已知的或者组件 378 可以被编程为动态识别对其使用加密的字段。

[0068] 可以为从查询返回的结果使用类似的办法。查询引擎 364 可以响应于查询返回从加密页面 342A 中导出的数据。此类数据可以包含仅采用加密形式的敏感值。这一数据同样地可被解密以将其从用于加密页面 342A 的格式中转换出。

[0069] 为了减少传送给客户端 312 的数据量，安全数据可以对数据执行聚集功能。聚集功能可以用某种方式聚集从匹配指定查询的多条数据中返回的值。作为一具体示例，聚集功能可以对来自匹配查询的多个记录的值求和。作为一具体示例，加密页面 342A 可以包含关于作出的购买的信息。所应用的查询可以请求关于由具体个体作出的所有购买的信息。聚集可能需要对这些购买的量求和。

[0070] 然而在所解说的实施例中，如果对直接从加密页面 342A 取得的加密值执行聚集

功能，则聚集功能将不会返回恰适的结果。相应地，查询引擎 364 将查询结果传递给安全设备内的解密组件 380。解密组件 380 可以解密查询结果中的任何加密值。解密组件 380 中的处理可以使用与转换组件 378 中使用的相同密钥或其他安全信息。但是，可以使用任何合适的处理来解密加密结果中的值。

[0071] 解密结果可以被传递至聚集组件 376。聚集组件 376 可以被编程为执行任何期望的聚集功能。该具体功能可取决于对数据的具体使用以及从客户端 312 发出的查询的本质。如对于安全设备内的其他组件那样，对聚集组件 376 的编程可以由安全设备已被指派给其的订户来指定。

[0072] 无论组件 376 内执行的具体聚集功能如何，该功能的结果被传递至组件 372。在组件 372 处，所得数据可以被加密。加密数据随后可以通过物理网络接口 370 来传递以供在因特网上传输回到客户端 312。

[0073] 在这一实施例中，应当认识到，不同的加密格式被用于因特网上的通信以及云数据库平台内加密数据的存储。此类架构允许对在公共网络上传送的信息的强加密以及私有云数据库环境中维持的数据的更快速的处理。然而，应当领会，任何合适的加密技术（无论其强度如何）可用于这些功能中的一者或两者。

[0074] 转向图 4，示出了可对响应于查询而检索到的结果上执行的处理操作的类型方面提供更大灵活性的附加实施例。在这一实施例中，如图 2 和 3 中的实施例那样，安全设备被实现为网络接口 444 的一部分。网络接口 444 具有可以连接到公共网络（诸如因特网）的物理网络接口 270。尽管未在图 4 中示出，但一个或多个客户端设备可以通过物理网络接口 470 来发送收到的查询。

[0075] 为了安全，可对收到的查询加密。相应地，图 4 的安全设备包括解密 / 认证组件 474，它可执行与如上所述的组件 374 或 274 类似的功能。同样地，图 4 的安全设备包括加密组件 472，它可执行与如上所述的组件 272 和 372 类似的功能。为了支持这些功能，安全设备可以被配置有被破坏的私有密钥 446A，被破坏的私有密钥 446A 也可以与上文结合图 2 和图 3 描述的私有密钥类似。

[0076] 同样如上结合图 3 所描述的，数据可以被存储在加密团块页面 442B 中。这些页面的某一部分可以被选中并且被复制到加密页面 442A，加密页面 442A 可以被临时存储在更快速的存储器中以供查询引擎 464B 将查询更快地应用于那些页面。

[0077] 同样如上结合图 2 所描述的，来自加密团块页面 442B 的一些页面可以被选中、解密、且临时地存储为明文页面 442C。明文查询可以被应用于明文页面 442C。

[0078] 相应地，图 4 解说了其中可以在相同的数据库节点中处理加密和明文查询两者的实施例。在这一示例中，为了支持对加密和明文查询两者的处理，解说了各自具有查询引擎的两个计算设备。计算设备 440 被示为包含查询引擎 464A。在这一示例中，查询引擎 464A 对照明文页面 442C 来执行明文查询。计算设备 450 被示为包含查询引擎 464B。查询引擎 464B 对照加密页面 442A 来执行加密查询。

[0079] 应当领会，为了简明起见，示出了具有两个查询引擎的两个计算设备。在一些实施例中，可以使用更多的计算设备和 / 或更多的查询引擎。或者，在一些实施例中，一个查询引擎可以被配置成执行明文查询和加密查询两者。或者，多个查询引擎可以在一个计算设备上执行。

[0080] 无论数据库节点以何种方式被架构以支持对明文查询和加密查询的执行，安全设备可以被配置成基于从客户端接收的查询来生成那些查询。在图 4 解说的示例中，安全设备包括查询拆分组件 478。一旦查询被接收并被解密和认证，组件 474A 将该查询传递至查询拆分组件 478。

[0081] 查询拆分组件 478 处理查询以生成明文查询和未加密查询。明文查询可以被提供给查询引擎 464B。加密查询可以被提供给查询引擎 464B。

[0082] 安全设备还可包含用于将处理经拆分查询的各部分的结果相组合的组件。出于这一目的，安全设备可包括组合组件 476。组合组件 476 从查询引擎 464A 接收明文结果。从查询引擎 464B 接收加密结果。

[0083] 可以执行任何合适的处理来组合查询结果。在所解说的实施例中，来自查询引擎 464B 的加密结果可以在组合组件 476 内被转换成明文格式。结果，在安全设备内，全部的结果可以以明文格式存在并且可以被容易地组合。

[0084] 一旦被组合，结果可以被提供给加密组件 4724 以供传输给生成该查询的客户端。

[0085] 图 5A、5B、5C 和 5D 解说了各个查询格式。图 5A 解说了明文查询 510。查询 510 包括聚集函数，此处被示为求和函数 :sum(l_extendprice*(1.0 - l_discount)。这一函数指示数据库记录内要在数字上被组合的字段并且提供用于该组合的公式。查询的其他部分指定要从数据库中选择哪些记录以在求和函数中进行处理。

[0086] 在这一示例中，查询是明文的，以使得查询中的任何敏感信息是可辨别的。例如，值 512 可能是姓名。维持这一查询可被应用的数据库的实体可能不想要揭露它正在存储关于有名字个体的信息。出于这一理由，查询 510 可以用加密形式在公共网络上传递。

[0087] 图 5B 解说了完全加密查询 520。在完全加密查询 520 中，查询的函数或者具体的姓名或其他值都是不可标识的。然而，采用这种格式，将难以或者不可能将查询中指定的准则与数据库存储的数据相匹配。

[0088] 图 5C 解说了可以被容易地应用于数据库的加密查询。在查询 530 中，表示敏感信息的值可被加密。然而，查询的其他部分被保留为明文。相应地，通过将图 5C 与图 5A 作比较，可以看到明文值 512 已经被加密值 532 代替。但是，在查询的上下文中都可以看出这两个值是数据库中的字段“o_clerk”的值。如果数据库中对应的字段“o_clerk”的所有值也用相同的破坏方案来加密，则加密值 532 将仍然匹配数据库中的恰适记录。以此方式，查询可以用加密形式被应用于数据库。

[0089] 图 5D 解说了查询拆分的一个示例。查询 540 已经被拆分成部分 550 和 560。部分 550 是明文查询，指定了要从明文数据库检索的信息。相反，部分 560 包含加密值 562，指定了用于从加密数据库检索信息的准则。

[0090] 在图 4 解说的系统中，收到的查询可以被拆分成各个部分，诸如部分 550 和 560。这些部分可以被相应地应用于查询引擎 464A 和 464B。在图 3 解说的系统中，以查询 530 为形式的经转换的查询可被应用于查询引擎 364。在图 2 解说的系统中，明文查询（如图 5A 所解说的）可被应用于查询引擎 264。以此方式，不同形式的查询可以被应用于具有不同架构的系统以提供期望的安全级别。

[0091] 图 6 示出了可在其上实现本发明的合适的计算系统环境 600 的示例。计算系统环境 600 只是合适的计算环境的一个示例，而非意在暗示对本发明的使用或功能性范围有任

何限制。也不应该将计算环境600解释为对示例性操作环境600中示出的任一组件或其组合有任何依赖性或要求。

[0092] 本发明可用众多其他通用或专用计算系统环境或配置来操作。适合在本发明中使用的公知的计算系统、环境和/或配置的示例包括，但不限于，个人计算机、服务器计算机、手持或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机、大型计算机、包含上述系统或设备中的任一个的分布式计算环境等。

[0093] 该计算环境可以执行计算机可执行指令，如程序模块。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。本发明也可被实践在分布式计算环境中，分布式计算环境中任务是由通过通信网络链接的远程处理设备执行的。在分布式计算环境中，程序模块可以位于包括存储器存储设备的本地和远程计算机存储介质中。

[0094] 参考图6，用于实现本发明的示例性系统包括计算机610形式的通用计算设备。计算机610的组件可包括，但不限于，处理单元620、系统存储器630、以及将包括系统存储器在内的各种系统组件耦合到处理单元621的系统总线620。系统总线621可以是若干类型的总线结构中的任一种，包括使用各种总线体系结构中的任一种的存储器总线或存储器控制器、外围总线、以及局部总线。作为示例而非限制，这样的体系结构包括工业标准体系结构(ISA)总线、微通道体系结构(MCA)总线、增强型ISA(EISA)总线、视频电子技术标准协会(VESA)局部总线和外围部件互连(PCI)总线(也称为夹层(Mezzanine)总线)。

[0095] 计算机610通常包括各种计算机可读介质。计算机可读介质可以是能由计算机610访问的任何可用介质，而且包含易失性和非易失性介质、可移动和不可移动介质。作为示例而非限制，计算机可读介质可包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括，但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光盘存储、磁带盒、磁带、磁盘存储或其它磁性存储设备、或能用于存储所需信息且可以由计算机610访问的任何其它介质。通信介质通常以诸如载波或其他传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其他数据，并包括任意信息传送介质。术语“已调制数据信号”是指使得以在信号中编码信息的方式来设置或改变其一个或多个特性的信号。作为示例而非限制，通信介质包括诸如有线网络或直接线连接之类的有线介质，以及诸如声学、射频、红外及其他无线介质之类的无线介质。上述中任一组合也应包括在计算机可读介质的范围之内。

[0096] 系统存储器630包括易失性和/或非易失性存储器形式的计算机存储介质，如只读存储器(ROM)631和随机存取存储器(RAM)632。包含诸如在启动期间帮助在计算机610内的元件之间传输信息的基本例程的基本输入/输出系统633(BIOS)通常存储在ROM 631中。RAM 632通常包含处理单元620可立即访问和/或当前正在操作的数据和/或程序模块。作为示例而非限制，图6示出了操作系统634、应用程序635、其他程序模块636和程序数据637。

[0097] 计算机610也可以包括其他可移动/不可移动、易失性/非易失性计算机存储介质。仅作为示例，图6示出了从不可移动、非易失性磁介质中读取或向其写入的硬盘驱动器

641，从可移动、非易失性磁盘651中读取或向其写入的磁盘驱动器652，以及从诸如CD ROM或其他光学介质等可移动、非易失性光盘655中读取或向其写入的光盘驱动器656。可在示例性操作环境中使用的其它可移动/不可移动、易失性/非易失性计算机存储介质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字录像带、固态RAM、固态ROM等。硬盘驱动器641通常通过诸如接口640之类的不可移动存储器接口连接到系统总线621，并且磁盘驱动器651和光盘驱动器655通常通过诸如接口650之类的可移动存储器接口连接到系统总线621。

[0098] 以上讨论并在图6中示出的驱动器及其相关联的计算机存储介质为计算机610提供了对计算机可读指令、数据结构、程序模块和其他数据的存储。在图6中，例如，硬盘驱动器641被示为存储操作系统644、应用程序645、其他程序模块646和程序数据647。注意，这些组件可与操作系统634、应用程序635、其它程序模块636和程序数据637相同，也可与它们不同。在此操作系统644、应用程序645、其它程序模块646以及程序数据647被给予了不同的编号，以说明至少它们是不同的副本。用户可以通过输入设备，例如键盘662和定点设备661——通常是指鼠标、跟踪球或触摸垫——向计算机610输入命令和信息。其它输入设备（未示出）可包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等。这些以及其它输入设备通常通过耦合到系统总线的用户输入接口660连接到处理单元620，但也可通过诸如并行端口、游戏端口或通用串行总线(USB)之类的其它接口和总线结构来连接。监视器691或其他类型的显示设备也经由诸如视频接口690之类的接口连接至系统总线621。除了监视器以外，计算机还可包括诸如扬声器697和打印机696之类的其它外围输出设备，它们可通过输出外围接口695来连接。

[0099] 计算机610可使用到一个或多个远程计算机（诸如，远程计算机680）的逻辑连接而在联网环境中操作。远程计算机680可以是个人计算机、服务器、路由器、网络PC、对等设备或其他常见网络节点，并且通常包括许多或所有以上相对计算机610所描述的元件，但在图6中仅示出了存储器存储设备681。图6中所描绘的逻辑连接包括局域网(LAN)671和广域网(WAN)673，但还可包括其他网络。此类联网环境在办公室、企业范围的计算机网络、内联网和因特网中是常见的。

[0100] 当在LAN联网环境中使用时，计算机610通过网络接口或适配器671连接到LAN670。当在WAN联网环境中使用时，计算机610通常包括调制解调器672或用于通过诸如因特网等WAN 673建立通信的其它手段。调制解调器672可以是内置的或外置的，可经由用户输入接口660或其它适当的机制连接到系统总线621。在联网环境中，相关于计算机610所示的程序模块或其部分可被存储在远程存储器存储设备中。作为示例而非限制，图6示出了远程应用程序685驻留在存储器设备681上。应当理解，所示的网络连接是示例性的，并且可使用在计算机之间建立通信链路的其它手段。

[0101] 至此描述了本发明的至少一个实施例的若干方面，可以理解，本领域的技术人员可容易地想到各种更改、修改和改进。

[0102] 这样的更改、修改和改进旨在是本发明的一部分，且旨在处于本发明的精神和范围内。此外，尽管指示了本发明的有点，但应当领会，不是本发明的每个实施例均包括每一个所描述的有点。一些实施例可以不实现被描述为有优势的任何特征。从而，上述描述和附图仅用作示例。

[0103] 可以多种方式中的任一种来实现本发明的上述实施例。例如，可使用硬件、软件或其组合来实现各实施例。当使用软件实现时，该软件代码可在无论是在单个计算机中提供的还是在多个计算机之间分布的任何合适的处理器或处理器的集合上执行。此类处理器可以被实现为集成电路，其中一个或多个处理器在集成电路组件中。然而，可使用电路按照任何适合的方式来实现处理器。

[0104] 此外，应当理解，计算机可以用多种形式中的任一种来具体化，如机架式计算机、台式计算机、膝上型计算机、或平板计算机。此外，计算机可以具体化在通常不被认为是计算机但具有合适的处理能力的设备中，包括个人数字助理 (PDA)、智能电话、或任何其他适合的便携式或固定电子设备。

[0105] 同样，计算机可以具有一个或多个输入和输出设备。这些设备主要可被用来呈现用户界面。可被用来提供用户界面的输出设备的示例包括用于可视地呈现输出的打印机或显示屏和用于可听地呈现输出的扬声器或其他声音生成设备。可用于用户界面的输入设备的示例包括键盘和诸如鼠标、触摸板和数字化输入板等定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式来接收输入信息。

[0106] 这些计算机可以通过任何合适形式的一个或多个网络来互连，包括作为局域网或广域网，如企业网络或因特网。这些网络可以基于任何合适的技术并可以根据任何合适的协议来操作，并且可以包括无线网络、有线网络或光纤网络。

[0107] 而且，此处略述的各种方法或过程可被编码为可在采用各种操作系统或平台中任何一种的一个或多个处理器上执行的软件。此外，这样的软件可使用多种合适的程序设计语言和 / 或程序设计或脚本工具中的任何一种来编写，而且它们还可被编译为可执行机器语言代码或在框架或虚拟机上执行的中间代码。

[0108] 就此，本发明可被具体化为用一个或多个程序编码的一个计算机可读存储介质（或多个计算机可读介质）（例如，计算机存储器、一个或多个软盘、紧致盘 (CD)、光盘、数字视频盘 (DVD)、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置、或其他非瞬态的有形计算机存储介质），当这些程序在一个或多个计算机或其他处理器上执行时，它们执行实现本发明的上述各个实施例的方法。如从以上示例中显而易见的，计算机可读存储介质可包含以非瞬态形式提供计算机可执行指令的充足时间的信息。这一个或多个计算机可读存储介质可以是可移植的，使得其上存储的一个或多个程序可被加载到一个或多个不同的计算机或其他处理器上以便实现本发明上述的各个方面。如此处所使用的，术语“计算机可读存储介质”只涵盖可被认为是产品（即，制品）或机器的计算机可读介质。替换地或附加地，本发明可以被实施为计算机可读存储介质之外的计算机可读介质，诸如传播信号。

[0109] 本文中以一般的意义使用术语“程序”或“软件”来指可被用来对计算机或其他处理器编程以实现本发明上述的各个方面的任何类型的计算机代码或计算机可执行指令集。另外，应当理解，根据本实施例的一个方面，当被执行时实现本发明的方法的一个或多个计算机程序不必驻留在单个计算机或处理器上，而是可以按模块化的方式分布在多个不同的计算机或处理器之间以实现本发明的各方面。

[0110] 计算机可执行指令可以具有可由一个或多个计算机或其他设备执行的各种形式，诸如程序模块。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等。通常，程序模块的功能可以按需在各个实施例中进行组合或分

布。

[0111] 而且，数据结构能以任何合适的形式存储在计算机可读介质上。为了解说的简明，数据结构可以被示为具有于数据结构中的位置相关的字段。这些关系同样可以通过对各字段的存储分配传达各字段之间的关系的计算机可读介质中的位置来得到。然而，可以使用任何合适的机制来在数据结构的各字段中的信息之间建立关系，例如通过使用指针、标签、或在数据元素之间建立关系的其他机制。

[0112] 本发明的各个方面可单独、组合或以未在前述实施例中特别讨论的各种安排来使用，从而并不将其应用限于前述描述中所述或附图形中所示的组件的细节和安排。例如，可使用任何方式将一个实施例中描述的各方面与其他实施例中描述的各方面组合。

[0113] 同样，本发明可被具体化为方法，其示例已经提供。作为该方法的一部分所执行的动作可以按任何合适的方式来排序。因此，可以构建各个实施例，其中各动作以与所示的次序所不同的次序执行，不同的次序可包括同时执行某些动作，即使这些动作在各说明性实施例中被示为顺序动作。

[0114] 在权利要求书中使用诸如“第一”、“第二”、“第三”等序数词来修饰权利要求元素本身并不意味着一个权利要求元素较之另一个权利要求元素的优先级、先后次序或顺序、或者方法的各动作执行的时间顺序，而仅用作将具有某一名字的一个权利要求元素与（若不是使用序数词则）具有同一名字的另一元素区分开的标签以区分各权利要求元素。

[0115] 同样，此处所使用的短语和术语是出于描述的目的而不应被认为是限制。此处对“包括”、“包含”、或“具有”、“含有”、“涉及”及其变型的使用旨在涵盖其后所列的项目及其等效物以及其他项目。

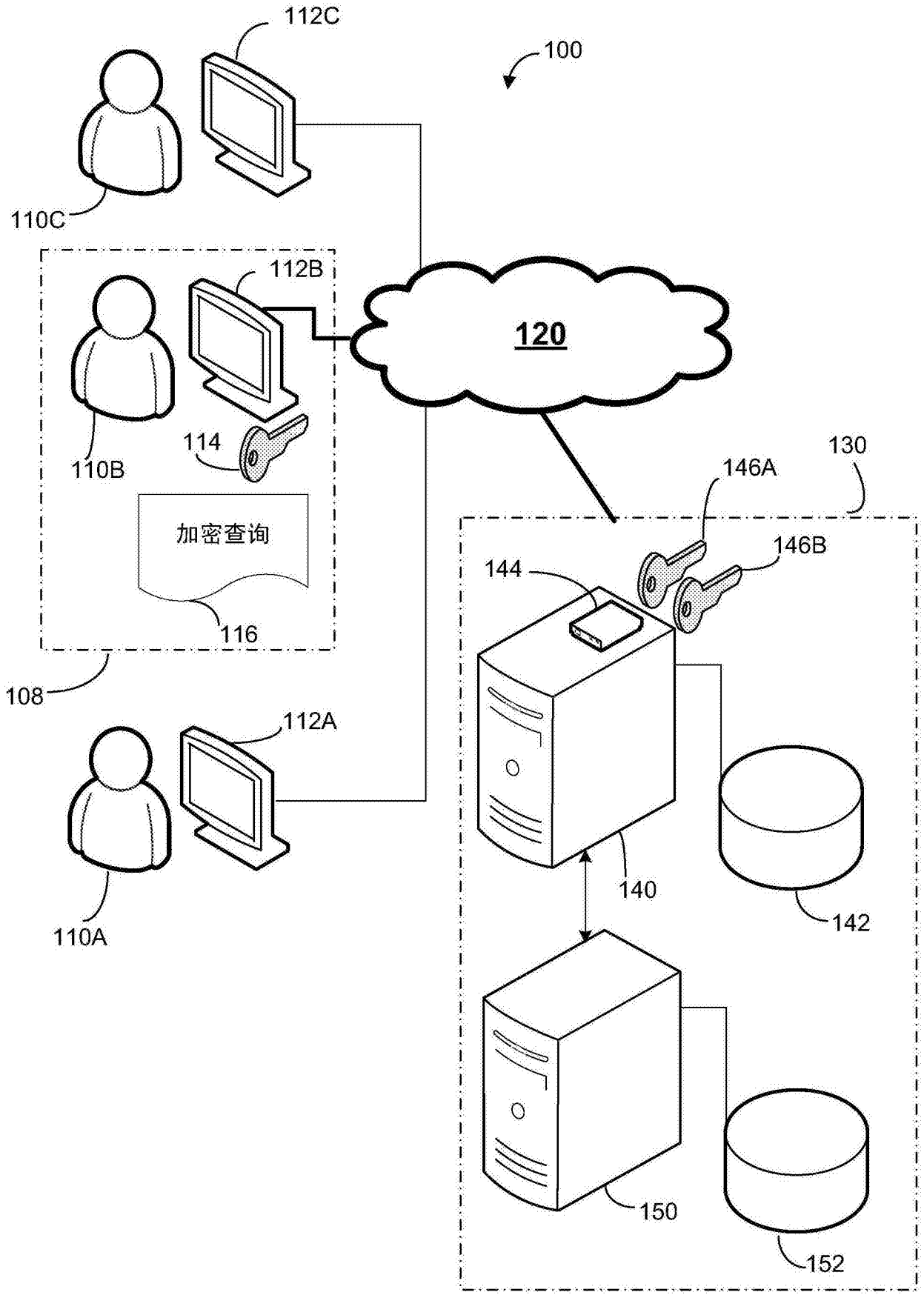

112C
100
110C
112B
120
114
130
146A
110B
加密查询
146B
144
116
108
112A
140
142
110A
150
152

图 1

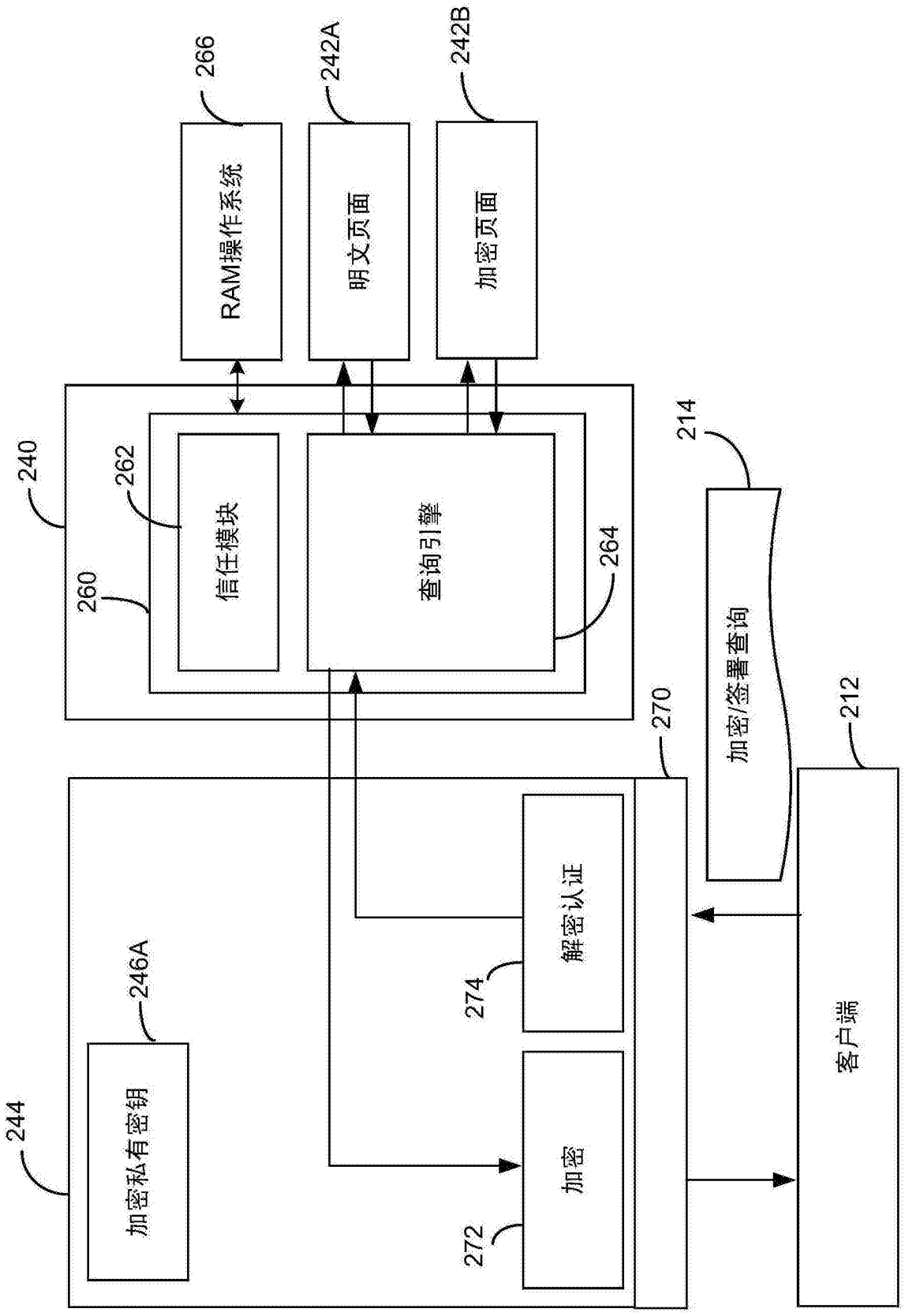

266
RAM操作系统
242A
明文页面
242B
加密页面
240
262
信任模块
260
查询引擎
264
214
加密/签署查询
270
212
客户端
解密认证
274
246A
加密私有密钥
244
加密
272

图 2

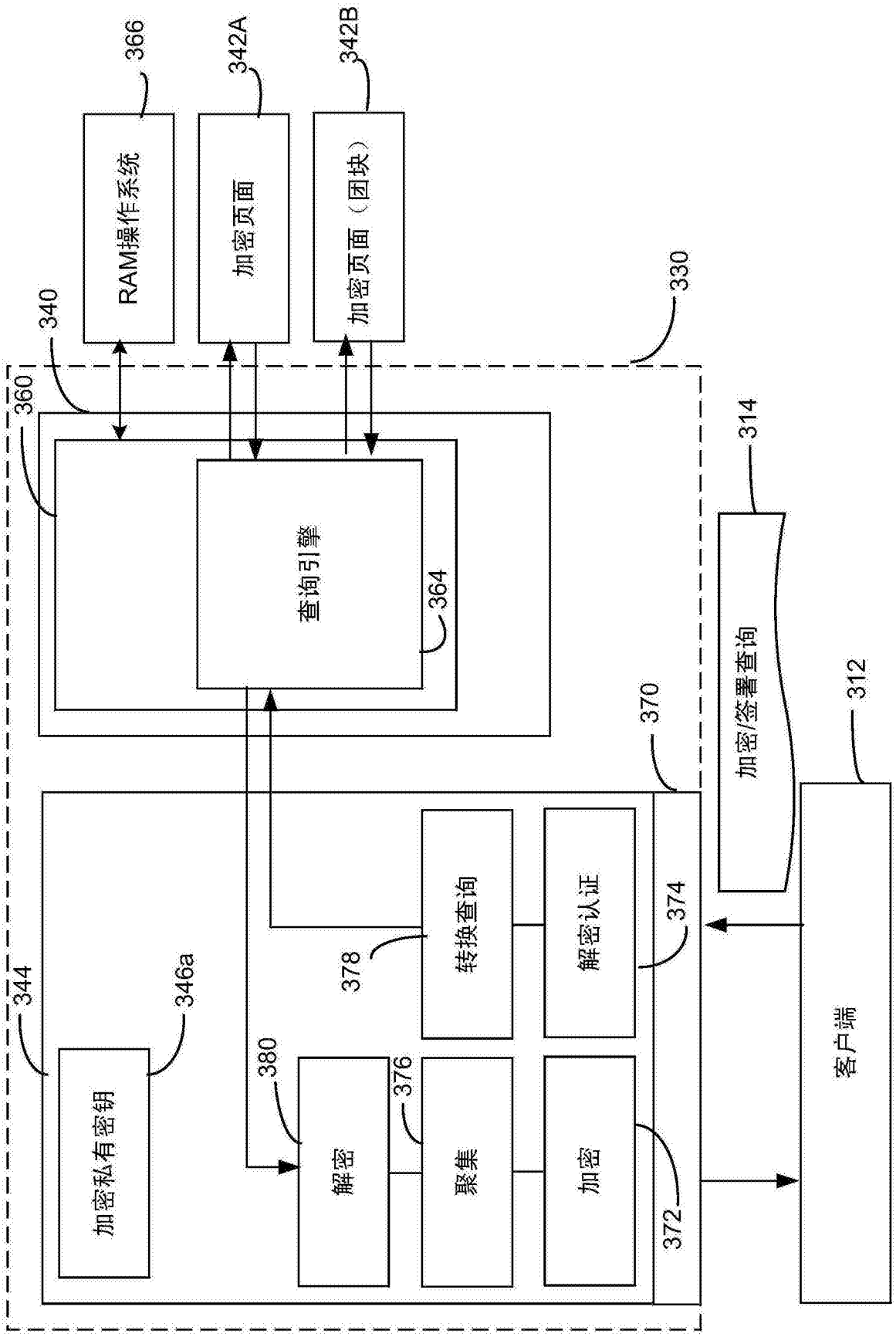

366
342A
342B
RAM操作系统
加密页面
加密页面（团块）
330
340
360
查询引擎
364
314
加密/签署查询
312
370
转换查询
解密认证
374
378
344
346a
加密私有密钥
380
376
解密
聚集
加密
372
客户端

图 3

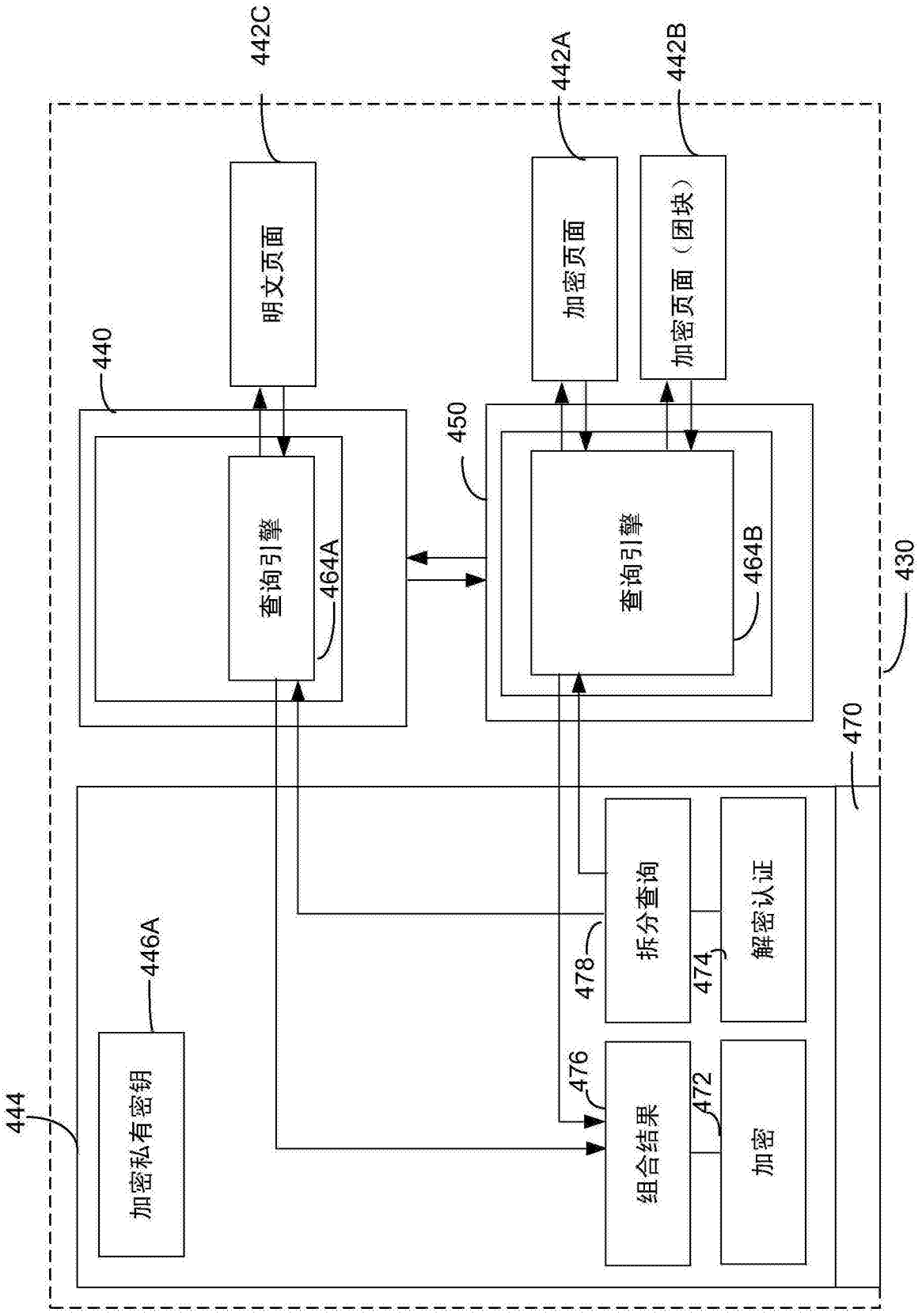

442C
442A
442B
明文页面
加密页面
加密页面（团块）
440
450
查询引擎
464A
查询引擎
464B
430
470
446A
加密私有密钥
444
478
拆分查询
474
解密认证
476
组合结果
472
加密

图 4

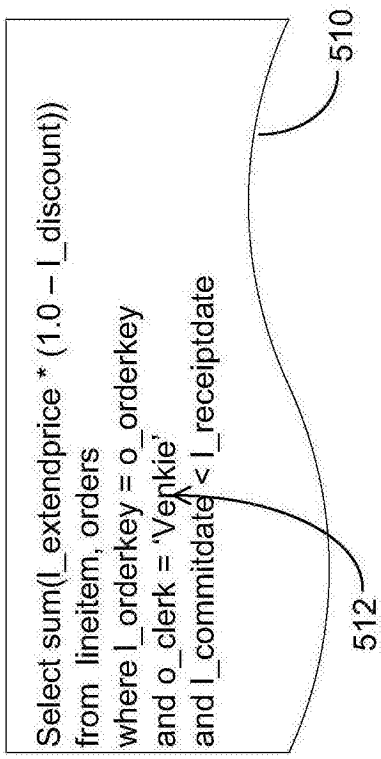

Select sum(l_extendprice * (1.0 – l_discount))
from lineitem, orders
where l_orderkey = o_orderkey
and o_clerk = 'Venkie'
and l_commitdate < l_receiptdate
510
512

图 5A

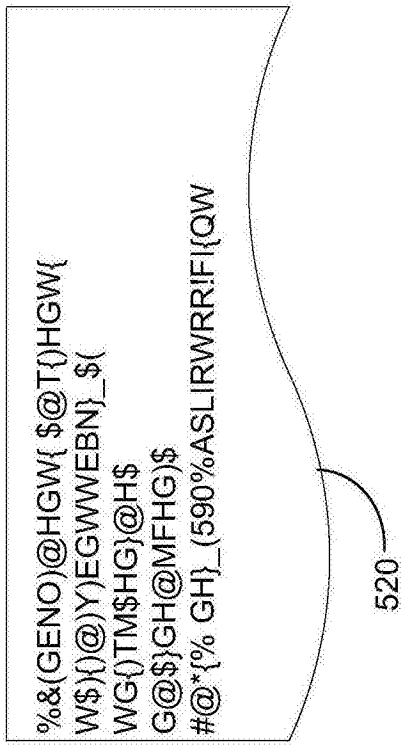

%&(GENO)@HGW{ $@T()HGW{
W$)()@)Y)EGWWEBN}_$(
WG()TM$HG}@H$
G@@$}GH@MFHG)$
#@*{% GH}_(590%ASLIRWRRIFI{QW
520

图 5B

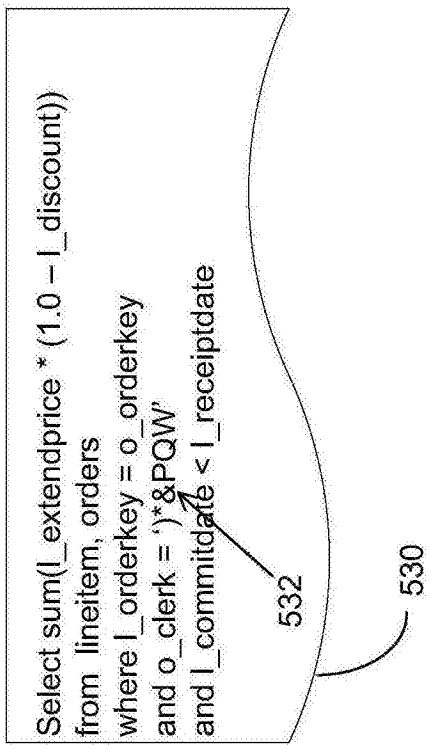

Select sum(l_extendprice * (1.0 – l_discount))
from lineitem, orders
where l_orderkey = o_orderkey
and o_clerk = ')*&PQW'
and l_commitdate < l_receiptdate
532
530

图 5C

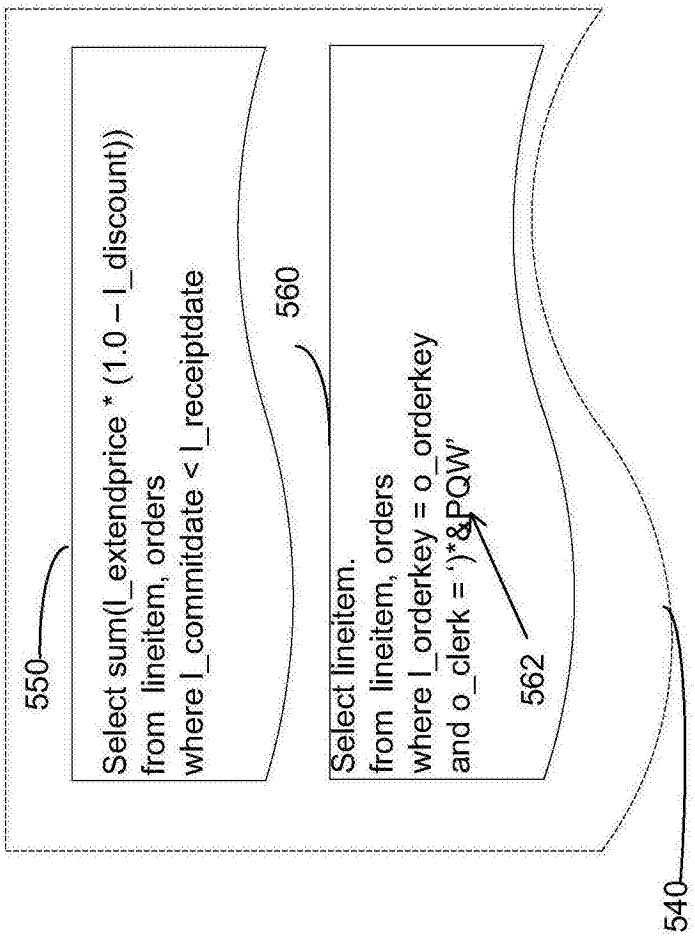

Select sum(l_extendprice * (1.0 – l_discount))
from lineitem, orders
where l_commitdate < l_receiptdate
Select lineitem.
from lineitem, orders
where l_orderkey = o_orderkey
and o_clerk = ')*&PQW'
550
560
562
540

图 5D

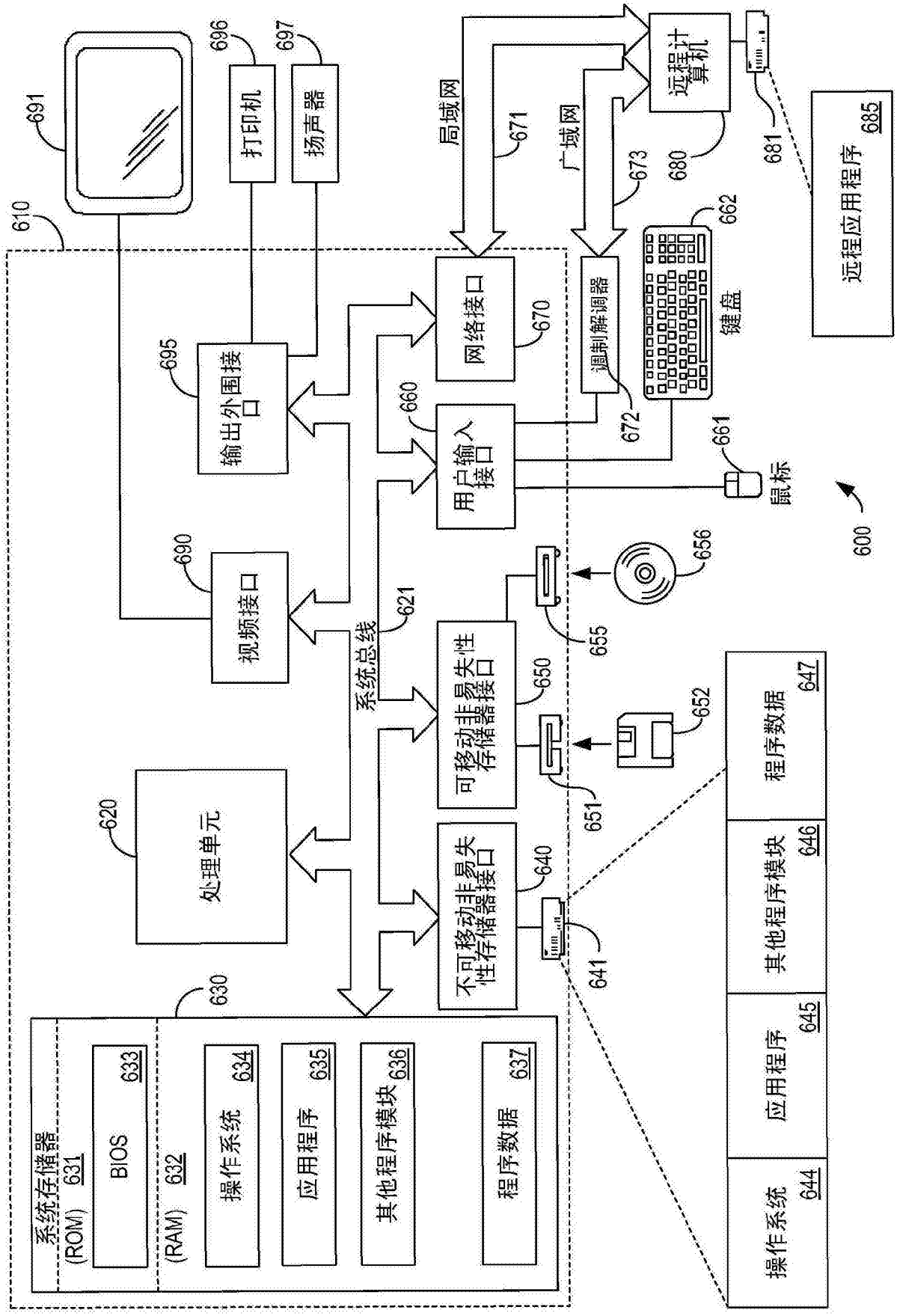

610
691
696
打印机
697
扬声器
局域网
671
广域网
673
远程计算机
680
681
远程应用程序
685
662
键盘
672
调制解调器
网络接口
670
695
输出外围接口
660
用户输入接口
661
鼠标
600
690
视频接口
621
系统总线
656
655
650
可移动非易失性存储器接口
652
651
620
处理单元
640
不可移动非易失性存储器接口
641
630
系统存储器
(ROM) 631
BIOS 633
(RAM) 632
操作系统 634
应用程序 635
其他程序模块 636
程序数据 637
操作系统 644
应用程序 645
其他程序模块 646
程序数据 647

图 6