[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/00

[12] 发明专利说明书

[21] ZL 专利号 00809589.2

[45] 授权公告日 2004 年 5 月 5 日

[11] 授权公告号 CN 1148926C

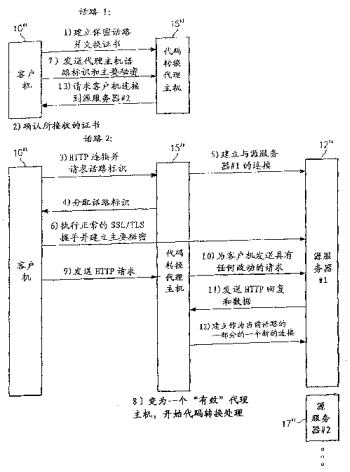
[22] 申请日 2000.6.28 [21] 申请号 00809589.2
[30] 优先权
[32] 1999.6.30 [33] US [31] 09/343,454
[86] 国际申请 PCT/GB2000/002469 2000.6.28
[87] 国际公布 WO01/003398 英 2001.1.11
[85] 进入国家阶段日期 2001.12.27
[71] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 托马斯·A·贝尔伍德
克里斯蒂安·利塔
马休·F·鲁特科斯基
审查员 贾丹明
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 付建军

权利要求书 6 页 说明书 15 页 附图 5 页

[54] 发明名称 使代理主机参与保密通信的方法和系统以及密码系统

[57] 摘要

使代理主机参与客户机与第一服务器之间的保密通信的方法。该方法开始时在客户机与代理主机之间建立第一保密话路。在确认该第一保密话路之后，该方法接着在该客户机和代理主机之间建立第二保密话路。在第二保密话路中，客户机要求代理主机作为通向第一服务器的通道。在此之后，客户机与第一服务器协商第一话路主要秘密。使用第一保密话路，由客户机把该第一话路主要秘密提供代理主机，使得代理主机参与该客户机与第一服务器之间的保密通信。在接收第一话路主要秘密之后，代理主机产生密码信息，使它为客户机提供给定的服务(例如，代码转换)，并且不需要该服务器的参与。如果在给定客户机向第一服务器发出请求过程中要求来自第二服务器的数据，则该代理主机向客户机发出一个请求，以利用相同的协议把该请求通过该代理主机返回到第二服务器。



ISSN1008-4274

1. 一种使代理主机（15）参与到客户机（10'）和第一源服务器（12a'）之间的保密通信中的方法，其中包括如下步骤:

（a） 在客户机与代理主机之间建立（20、22）第一保密话路;

（b） 在确认第一保密话路之后，在客户机与代理主机之间建立（24、26）第二保密话路，该第二保密话路要求该代理主机作为通向第一源服务器的管道;

（c） 使该客户机与第一源服务器协商（30）话路主要秘密;

（d） 使该客户机利用第一保密话路把该话路主要秘密传送（32）到该代理主机，使得该代理主机参与到该保密通信中;

（e） 响应对第一源服务器的客户机请求，建立该客户机与代理主机之间的第三保密话路，该第三保密话路要求该代理主机作为通向第二源服务器的管道;

（f） 使得该客户机与第二源服务器协商新的话路主要秘密；以及

（g） 使得该客户机利用在步骤（a）中产生的第一保密话路来把新的话路主要秘密传送到该代理主机。

2. 根据权利要求 1 所述的方法，其特征在于，进一步包括如下步骤:使得该代理主机（15）使用该话路主要秘密和新的话路主要秘密来产生给定的密码信息。

3. 根据权利要求 2 所述的方法，其特征在于，进一步包括如下步骤:使得代理主机（15）在步骤（d）中接收到该话路主要秘密之后进入有效工作状态。

4. 根据权利要求 3 所述的方法，其特征在于，该代理主机（15）在该有效工作状态中为该客户机（10'）执行给定的服务。

5. 根据权利要求 4 所述的方法，其特征在于，该给定服务是代码转

换。

6. 根据权利要求 1 所述的方法，其特征在于，第一和第二保密话路符合网络保密协议。

7. 根据权利要求 1 所述的方法，其特征在于，该服务器（12a'）是一种网络服务器，并且该客户机（10'）是一种分布式计算客户机。

8. 一种使代理主机（15）参与到客户机（10'）和服务器（12a'）之间的保密通信中的方法，该方法用于与 1 至"n"的一组服务器进行通信的客户机中，其中包括如下步骤:

（a）对于 1 至"n"的一组服务器中的每一个:

（1） 使得该客户机请求（20、22）到该代理主机的第一保密连接;

（2） 在认证来自该代理主机的证书的有效性之后，使客户机请求（24、26）到代理主机的第二保密连接，该第二保密连接要求该代理主机作为通向该服务器的管道;

（3） 使该客户机与服务器通过该管道协商（30）各个话路主要秘密;

（4） 在完成协商之后，使该客户机利用第一保密连接把该各个话路主要秘密传送（32）到该代理主机; 以及

（b）使得该代理主机使用各个话路主要秘密来产生给定的密码信息，该信息对于参与该保密通信是有用的。

9. 根据权利要求 8 所述的方法，其特征在于，进一步包括如下步骤: 使得代理主机（15）为该客户机执行给定的服务，该给定的服务是从一组服务中选择的，其中包括代码转换、缓存、加密、解密、监控、过滤和预取。

10. 一种使代理主机（15）参与保密通信的方法，该方法用于客户机

中并且包括如下步骤:

（a） 把来自客户机的请求发送到（20）代理主机，以建立第一保密话路;

（b） 把来自该客户机的请求发送到（24）该代理主机，以建立在该客户机和该代理主机之间的第二保密话路，该第二保密话路要求该代理主机作为通向源服务器的管道;

（c） 利用第一保密话路把来自客户机的话路主要秘密发送到(32)该代理主机，使该代理主机参与该保密通信;

（d） 响应在该客户机接收的来自该代理主机的请求，把来自该客户机的请求发送到该代理主机，以建立该客户机与该代理主机之间的第三保密话路，该第三保密话路要求该代理主机作为通向另一个源服务器的管道；以及

（e） 把新的话路主要秘密从该客户机发送到代理主机。

11. 根据权利要求 10 所述的方法，其特征在于，该新的话路主要秘密在第一保密话路上发送。

12. 一种使代理主机（15）参与到保密通信中的方法，该方法用于代理主机中并且包括如下步骤:

（a） 在代理主机接收（20）来自客户机的请求，以在该客户机和代理主机之间建立第一保密话路;

（b） 在该代理主机接收（24）来自该客户机的请求，以在该客户机和代理主机之间建立第二保密话路，该第二保密话路要求该代理主机作为通向源服务器的管道;

（c） 在该代理主机接收（32）从该客户机利用第一保密话路发送的话路主要秘密;

（d） 在把来自该代理主机的给定请求发送到该客户机之后，在该代理主机接收来自该客户机的请求，以建立该客户机与该代理主机之间的第二保密话路，该第二保密话路要求该代理主机作为通向另一个源服务器的管道；以及

（e） 在该代理主机接收从该客户机发送的新的话路主要秘密。

13. 根据权利要求 12 所述的方法，其特征在于，进一步包括如下步骤：使该代理主机（15）利用该话路主要秘密和新的话路主要秘密来产生给定的密码信息。

14. 一种使代理主机(15)参与到客户机(10')和第一源服务器(12a')之间的保密通信中的方法，该方法用于代理主机中并且包括如下步骤：

在该代理主机接收（20）来自客户机的请求，以建立该客户机与该代理主机之间的第一保密话路；

通过该代理主机，执行（20、22、24、26、30）该客户机与第一源服务器之间的保密握手程序，以产生第一话路密钥；

使该客户机把第一话路密钥发送到该代理主机，使得该代理主机可以在该话路过程中参与到客户机与第一源服务器之间的通信中；以及

随着该通话的继续，执行该客户机与第二源服务器之间的保密握手程序，以产生第二话路密钥；以及

使该客户机把第二话路密钥发送到该代理主机，从而该代理主机可以从第二源服务器获得数据，用于对该客户机向第一源服务器提出的请求来提供服务。

15. 根据权利要求 14 所述的方法，其特征在于，每个话路密钥被从客户机（10'）通过不同的保密连接发送到代理主机（15）。

16. 根据权利要求 14 所述的方法，其特征在于，每个话路密钥被从客户机（10'）通过相同的保密连接发送到该代理主机（15）。

17. 一种密码系统，其中包括：

客户机（10'）；

一组服务器（12a'、12b'）；

代理主机（15）；

用于使该客户机与每个服务器在一条保密连接上进行通信的网络协议服务;

用于控制该客户机请求到该代理主机的第一保密连接的装置;

用于在认证来自该代理主机的证书的有效性之后，控制该客户机请求到代理主机的第二保密连接的装置，该第二保密连接要求该代理主机作为通向一个给定服务器的管道;

用于控制该客户机与该给定服务器通过该管道进行协商，以获得一个话路主要秘密的装置;

在完成协商之后，控制该客户机利用第一保密连接把该话路主要秘密传送到该代理主机的装置;

用于控制该客户机利用该话路主要秘密来产生给定密码信息的装置;

用于控制该代理主机请求该客户机有选择地建立与另一个代理主机之间的独立保密连接的装置；以及

用于在该代理主机参与到该客户机与给定服务器之间的通信的过程中，把该代理主机切换为有效工作状态的装置。

18. 根据权利要求 17 所述的系统，其特征在于，该代理主机（15）包括用于为该客户机（10'）提供代码转换服务的装置。

19. 根据权利要求 18 所述的系统，其特征在于，该代理主机包括用于为该客户机（10'）提供加密/解密服务的装置。

20. 根据权利要求 17 所述的系统，其特征在于，该代理主机包括用于为该客户机（10'）提供缓存服务的装置。

21. 根据权利要求 17 所述的系统，其特征在于，该代理主机包括用于为该客户机（10'）提供监控服务的装置。

22.一种用于使代理主机（15）参与保密通信中的装置，其中包括:

用于把来自客户机的请求发送到代理主机，以建立第一保密话路的装置；

用于把来自该客户机的请求发送到该代理主机，以建立在该客户机和该代理主机之间的第二保密话路的装置，该第二保密话路要求该代理主机作为通向源服务器的管道；

用于利用第一保密话路把来自客户机的话路主要秘密发送到该代理主机，使该代理主机参与该保密通信的装置；

在用于在控制客户机的保密通信过程中响应在该客户机接收的来自该代理主机的请求，以获得新的话路主要秘密的装置；以及

用于把新的话路主要秘密从该客户机发送到代理主机的装置。

23.一种用于使代理主机参与保密通信中的装置，其中包括：

用于在代理主机接收来自客户机的请求，以在该客户机和代理主机之间建立第一保密话路的装置；

在该代理主机接收来自该客户机的请求，以在该客户机和代理主机之间建立第二保密话路的装置，该第二保密话路要求该代理主机作为通向源服务器的管道；

在该代理主机接收从该客户机利用第一保密话路发送的话路主要秘密的装置；

在保密通信过程中响应给定事件，用于把给定请求从该代理主机发送到该客户机的装置；以及

在该代理主机接收从该客户机发送的新的话路主要秘密的装置。

24. 根据权利要求 23 所述的装置，其特征在于，进一步包括用于利用话路主要秘密和新的话路秘密来产生给定的密码信息的装置。

使代理主机参与保密通信的方法和系统以及密码系统

技术领域

本发明一般涉及网络保密协议，特别涉及把客户机与一个或多个源服务器之间的保密话路(secure session)的保密性扩展到中介（例如，代码转换代理主机）的方法和系统以及一种密码系统。

背景技术

网络保密协议，例如网景的加密套接字层协议（SSL）以及互联网工程任务组（IETF）传输层保密协议（TLS）提供通信设备之间的保密性和数据完整性。这些协议例如是保证互联网上的电子商务交易的保密所通用的协议。

最近，计算机产业对通常被认为不同于传统计算机的其它设备添加了计算机处理和通信能力。这种设备相当广泛，并且例如包括个人数字处理（PDA）、商务管理器（business organizer）（例如，IBM®的 WorkPad®、以及 3Com®的 PalmPilot®）、小型电话（smartphone）、移动电话、其它手持设备等等。为了方便，这些设备作为一类产品有时被称为“分布式计算（pervasive computing）”客户机，因为它们是设计为无论其位置在何处都可以与计算机网络中的服务器相连接的设备并且用于计算。

但是，分布式计算客户机一般不支持 HTML 基于视窗的客户机的全套功能。结果，一般需要代码转换服务来把要显示在该分布式客户机上的信息从一种源标志语言（例如，HTML）转换为另一种（例如，HDML 或者手持设备标识语言）。但是，在保密网络连接上提供代码转换服务存在者问题。特别是，在保密和代码转换服务之间存在本质的冲突，因为例如 SSL 和 TLS 这样的传统保密协议正好是设计来用于防止第三者干预客户机与服务器之间的通信的。

在其它应用中,限制第三者干预保密话路也存在问题。例如，如果客户

为例如 SSL 和 TLS 这样的传统保密协议正好是设计来用于防止第三者干预客户机与服务器之间的通信的。

更加具体来说，当一个分布式计算客户机与一个或多个源服务器在保密链路上进行通信时，本发明能够使得代理主机提供代码转换服务。

本发明还能够使代理主机为客户机执行缓存或其它管理服务，该客户机利用网络保密协议与一个或多个服务器进行通信。

本发明能够使代理主机为客户机执行加密/解密，该客户机使用网络服务器协议与一个或多个源服务器进行通信。

在一个优选实施例中，代理主机参与客户机与第一服务器之间的保密通信。该方法开始时首先在客户机与代理主机之间建立第一保密话路。在确认该第一保密话路之后，该方法接着在该客户机和代理主机之间建立第二保密话路。在第二保密话路中，客户机要求代理主机作为通向第一服务器的通道。在此之后，客户机与第一服务器协商第一话路主要秘密。使用第一保密话路，由客户机把该第一话路主要秘密提供代理主机，使得代理主机参与该客户机与第一服务器之间的保密通信。在接收第一话路主要秘密之后，代理主机产生密码信息，使它为客户机提供给定的服务（例如，代码转换、监控、加密/解密、缓存等等），并且不需要该服务器的参与。在这种通信过程中，在客户机与代理主机之间保持第一保密话路。

根据本发明的一个特征，如果代理主机要求来自第二服务器的数据，以处理给定客户机的请求，则重复上述协议。特别地，该代理主机向客户机发出请求，以再次通过该代理主机建立与第二服务器之间的另外一条连接。如上文所述，该协议使得该客户机与第二服务器之间建立第二话路主要秘密，按照上述方式把该秘密与该代理主机共享。然后，该代理主机继续通过利用该第二秘密进行它的服务操作（例如代码转换），以从第二服务器获得保密数据。

因此，一旦在客户机与给定的源服务器之间建立基本的隧道协议（tunneling protocol），则按照客户机的要求重复该协议，以使得代理主机能够从多达“n”个其它源服务器获得保密数据，同时把给定客户机

的请求传送到给定的源服务器。

本发明提供一种使代理主机参与到客户机和第一源服务器之间的保密通信中的方法，其中包括如下步骤：在客户机与代理主机之间建立第一保密话路；在确认第一保密话路之后，在客户机与代理主机之间建立第二保密话路，该第二保密话路要求该代理主机作为通向第一源服务器的管道；使该客户机与第一源服务器协商话路主要秘密；使该客户机利用第一保密话路把该话路主要秘密传送到该代理主机，使得该代理主机参与到该保密通信中；响应对第一源服务器的客户机请求，建立该客户机与代理主机之间的第三保密话路，该第三保密话路要求该代理主机作为通向第二源服务器的管道；得该客户机与第二源服务器协商新的话路主要秘密；以及使得该客户机利用第一保密话路来把新的话路主要秘密传送到该代理主机。

本发明还提供一种使代理主机参与到客户机和服务器之间的保密通信中的方法，该方法用于与 1 至“n”的一组服务器进行通信的客户机中，其中包括如下步骤：对于 1 至“n”的一组服务器中的每一个：（1）使得该客户机请求到该代理主机的第一保密连接；（2）在认证来自该代理主机的证书的有效性之后，使客户机请求到代理主机的第二保密连接，该第二保密连接要求该代理主机作为通向该服务器的管道；（3）使该客户机与服务器通过该管道协商各个话路主要秘密；（4）在完成协商之后，使该客户机利用第一保密连接把该各个话路主要秘密传送到该代理主机；以及（b）使得该代理主机使用各个话路主要秘密来产生给定的密码信息，该信息对于参与该保密通信是有用的。

本发明还提供一种使代理主机参与保密通信的方法，该方法用于客户机中并且包括如下步骤：把来自客户机的请求发送到代理主机，以建立第一保密话路；把来自该客户机的请求发送到该代理主机，以建立在该客户机和该代理主机之间的第二保密话路，该第二保密话路要求该代理主机作为通向源服务器的管道；利用第一保密话路把来自客户机的话路主要秘密发送到该代理主机，使该代理主机参与该保密通信；响应在该客户机接收的来自该代理主机的请求，把来自该客户机的请求发送到该

代理主机，以建立该客户机与该代理主机之间的第三保密话路，该第三保密话路要求该代理主机作为通向另一个源服务器的管道；以及把新的话路主要秘密从该客户机发送到代理主机。

本发明还提供一种使代理主机参与到保密通信中的方法，该方法用于代理主机中并且包括如下步骤：在代理主机接收来自客户机的请求，以在该客户机和代理主机之间建立第一保密话路；在该代理主机接收来自该客户机的请求，以在该客户机和代理主机之间建立第二保密话路，该第二保密话路要求该代理主机作为通向源服务器的管道；在该代理主机接收从该客户机利用第一保密话路发送的话路主要秘密；在把来自该代理主机的给定请求发送到该客户机之后，在该代理主机接收来自该客户机的请求，以建立该客户机与该代理主机之间的第二保密话路，该第二保密话路要求该代理主机作为通向另一个源服务器的管道；以及在该代理主机接收从该客户机发送的新的话路主要秘密。

本发明还提供一种使代理主机参与到客户机和第一源服务器之间的保密通信中的方法，该方法用于代理主机中并且包括如下步骤：在该代理主机接收来自客户机的请求，以建立该客户机与该代理主机之间的第一保密话路；通过该代理主机，执行该客户机与第一源服务器之间的保密握手程序，以产生第一话路密钥；使该客户机把第一话路密钥发送到该代理主机，使得该代理主机可以在该话路过程中参与到客户机与第一源服务器之间的通信中；以及随着该通话的继续，执行该客户机与第二源服务器之间的保密握手程序，以产生第二话路密钥；以及使该客户机把第一话路密钥发送到该代理主机，从而该代理主机可以从第二源服务器获得数据，用于对该客户机向第一源服务器提出的请求来提供服务。

本发明还提供一种密码系统，其中包括：客户机；一组服务器；代理主机；用于使该客户机与每个服务器在一条保密连接上进行通信的网络协议服务；一种计算机程序，（i）用于控制该客户机请求到该代理主机的第一保密连接；(ii)在认证来自该代理主机的证书的有效性之后，控制该客户机请求到代理主机的第二保密连接，该第二保密连接要求该代理主机作为通向一个给定服务器的管道；（iii）控制该客户机与该给定服务

器通过该管道进行协商，以获得一个话路主要秘密；以及（iv）在完成协商之后，控制该客户机利用第一保密连接把该话路主要秘密传送到该代理主机；以及一种计算机程序，（i）用于控制该客户机利用该话路主要秘密来产生给定密码信息；（ii）用于控制该代理主机请求该客户机有选择地建立与另一个代理主机之间的独立保密连接；以及（iii）用于在该代理主机参与到该客户机与给定服务器之间的通信的过程中，把该代理主机切换为有效工作状态。

本发明还提供一种在用于密码系统的计算机可读介质中的计算机程序产品，该密码系统包括客户机、一组服务器以及代理主机，其中包括：第一例程，（i）用于控制该客户机请求到该代理主机的第一保密连接；(ii)在认证来自该代理主机的证书的有效性之后，控制该客户机请求到代理主机的第二保密连接，该第二保密连接要求该代理主机作为通向一个给定服务器的管道；（iii）控制该客户机与该给定服务器通过该管道进行协商，以获得一个话路主要秘密；以及（iv）在完成协商之后，控制该客户机利用第一保密连接把该话路主要秘密传送到该代理主机；以及第二例程，（i）用于控制该客户机利用该话路主要秘密来产生给定密码信息；（ii）用于控制该代理主机请求该客户机有选择地建立与另一个代理主机之间的独立保密连接；以及（iii）用于在该代理主机参与到该客户机与给定服务器之间的通信的过程中，把该代理主机切换为有效工作状态。

本发明还提供一种计算机程序产品，其具有在用于客户机中的可用介质上的计算机可读程序代码，用于使代理主机参与保密通信中，其中包括：用于把来自客户机的请求发送到代理主机，以建立第一保密话路的方法；用于把来自该客户机的请求发送到该代理主机，以建立在该客户机和该代理主机之间的第二保密话路的方法，该第二保密话路要求该代理主机作为通向源服务器的管道；用于利用第一保密话路把来自客户机的话路主要秘密发送到该代理主机，使该代理主机参与该保密通信的方法；在用于在控制客户机的保密通信过程中响应在该客户机接收的来自该代理主机的请求，以获得新的话路主要秘密的方法；以及用于把新的话路主要秘密从该客户机发送到代理主机的方法。

本发明还提供一种计算机程序产品，其具有在用于代理主机中的可用介质上的计算机可读程序代码，用于使代理主机参与保密通信中，其中包括：用于在代理主机接收来自客户机的请求，以在该客户机和代理主机之间建立第一保密话路的方法；在该代理主机接收来自该客户机的请求，以在该客户机和代理主机之间建立第二保密话路的方法，该第二保密话路要求该代理主机作为通向源服务器的管道；在该代理主机接收从该客户机利用第一保密话路发送的话路主要秘密的方法；在保密通信过程中响应给定事件，用于把给定给定请求从改代理主机发送到该客户机的方法；以及在该代理主机接收从该客户机发送的新的话路主要秘密的方法。

附图简述

现在将参照附图通过举例描述本发明，其中：

图 1 为使用网络保密协议的已有客户机-服务器网络环境的示意图；

图 2 为一种客户机-服务器网络环境的简化示意图，其中第三方中介或代理主机参与到保密话路中；

图 3 为基本隧道方法的详细流程图；

图 4 为本发明的简化方框图，其中在客户机最初把保密信息委派给代理主机之后，该代理主机要求该客户机通过开隧道经过该代理主机到达“n”个其它源服务器，以建立一个或多个其它保密连接；以及

图 5 为一种采用本发明的分布式计算客户机-服务器构架的方框图。

具体实施方式

图 1 示出一种现有技术的常规客户机-服务器网络构架。在该图中，客户机 10 通过网络 14 与服务器 12 进行通信，该网络可能是互联网、内部网、广域网、局域网等等。客户机 10 和服务器 12 使用一种网络保密协议进行通信，例如网景的加密套接字层协议（SSL）以及 IETF 传输层保密协议（TLS）。一般来说，客户机是发起建立到服务器的 TLS 或 SSL 的连接的任何应用实体。服务器是接受连接以通过发送返回响应而对请

求提供服务的任何应用实体或程序。任何给定的程序可以称为客户机和服务器。服务器和客户机之间的主要操作差别在于该服务器通常被认证，而客户机仅仅是可选地进行认证。具有给定资源或者创造给定资源的服务器在本文中有时被称为源服务器。

客户机和服务器参与一个保密话路中。SSL 或 TLS 话路是由握手协议创建的在客户机与服务器之间的连接。话路定义一组密码保密参数，该参数可以在多个连接之间共享。它们被用于避免在每次连接对新的保密参数进行协商。在 SSL 或 TLS 中，话路标识符是一个由服务器所产生的数值，其识别定的话路。为了建立一个 SSL 或 TLS 话路，客户机和服务器执行握手操作，该操作是建立该实体之间的事务处理的参数的初始协商。一旦创建一个话路，则在一条连接上进行客户机与服务器之间的通信，该连接是提供适当类型的服务的（在 OSI 分层模型定义中的）传

输层。对于 SSL 和 TLS，这种连接是对等关系的。该连接是暂时性的，并且每个连接与一个话路相关联。一般来说，在该连接上的通信是利用公钥加密技术而保证保密的，该技术是一种采用双密钥密码的加密技术。用公钥加密的信息仅仅可以用相关的私钥来解密。相反，用私钥签署的消息可以用公钥来验证。

一旦建立该话路，则该客户机具有由源服务器所发出的用于向源服务器认证该客户机的证书。该客户机还要求源服务器提供一个证书，使得它可以认证该源服务器有效。认证是一个实体确定另一个实体的身份的能力。一般来说，作为 X.509 协议的一部分（a/k/a ISO 认证构架），证书由一个收信人的证书授权机构来颁发，并且使当事人的身份（或者一些其它属性）与其公钥紧密结合。

上述功能是本领域所公知的。该功能例如在符合 IETF TLS 1.0 版和 SSL 2.0/3.0 版的协议中实现。这些协议非常类似，它们包括两个层：记录协议和握手协议。如下文所述，本发明利用扩展这些类型的保密协议的方法的优点，来把话路的保密性延伸到第三方中介或代理主机。最好，本发明与客户机和代理主机之间的握手协议一同应用，如下文所述该协议是在保密话路之上的层面。该延伸不改变在记录协议层的保密连接的基本特性。尽管该技术在 TLS 和 SSL 的上下文中描述，但是这不是对本发明的限制。

现在参照图 2，该基本方法使得利用 SSL 或 TLS 作为保密协议来与一个或多个源服务器 12’ a-n 进行通信的客户机 10’ 允许一个代理主机 15 参与该话路，而不改变该话路的保密特性。如上文所述，本方法独立于由客户机 10’ 和给定源服务器 12’ 所使用来进行相互认证的加密强度或步骤本发明具有与 TLS/SSL 相同的优点在于，它扩展该协议，但仍然允许较高层协议处于其上方。这种高层协议例如包括应用协议（例如，HTTP, TELNET, FTP 和 SMTP），该协议通常是紧接着在传输层（例如 TCP/IP）之上的层面。

图 3 为示出在本发明中有用的一种保密代理协议的操作。根据该协议，客户机 10’ 在每次需要建立于给定源服务器的连接时设置两个（2）完全

不同的话路。第一个保密话路设置在客户机 10’ 与代理主机 15 之间，并且该话路被用作为在客户机与代理主机之间传送秘密信息的管道或通道。第一保密话路由该流程图的前两列所表示。另外，客户机 10 还设置与代理主机之间的第二保密话路，由该流程图的后三列所表示，但是，在该话路中，代理主机 15 被用于隧道通向该源服务器 12’ 。隧道是一种中介程序，其作为两个连接之间的盲中介。一旦激活，隧道不被认为是给定通信的一方（例如，HTTP 请求或响应），尽管该隧道可能已经由该通信所启动。

在所示实施例中，假设该客户机希望访问一个源服务器（有时称为第一服务器），以检索给定内容，但是希望使用该代理主机来正确地显示这些内容。对该请求的服务可能还需要从一个或多个源服务器检索给定的对象。如上文所述，根据 SSL/TLS 协议，该客户机具有由一个源服务器所颁布用于向该源服务器认证该客户机的证书，并且该客户机还要求源服务器提供一个证书，从而它可以认证该源服务器为有效。如下文所述，在客户机向代理主机写入一个话路主要秘密之前，该客户机还要求代理主机提供由该客户机所认证的证书。

该例程以步骤 20 为开始，该客户机请求建立与代理主机之间的保密话路。这是上文所述的第一保密话路。如流程图中所示，该客户机必须要求来自该代理主机的证书，因为它要代表其保密属性。这是主要话路，通过该话路客户机将把任何源服务器的协商秘密与一个内部话路标识符一同发送到该代理主机。一般来说，该标识符与 SSL/TLS 话路标识符不同。它将在下文的步骤中更加具体描述。

在步骤 22，客户机认证由该代理主机接收的证收的有效性，结果，这满足它具有与该代理主机之间的保密话路的条件。然后，该例程进行到步骤 24，该客户机开启到该代理主机的第二连接。这是上述的第二保密话路。如上文所述，该客户机要求隧道通向给定的源服务器（例如，对一个请求使用 HTTP 连接方法）。作为通过代理主机的隧道请求的一部分，该客户机把一个报头添加到该 HTTP 请求，通知该代理主机要产生一个内部话路标识符。该报头意味着该客户机要在将来把主要秘密转发

到该代理主机。

在步骤 26，该代理主机产生一个唯一的内部话路标识符，并且把该信息返回到客户机。内部话路标识符的数值被附加到该保密 HTTP 答复上。这是该客户机要在把话路主要秘密转发到代理主机时将使用的数值。在步骤 28，该代理主机建立与源服务器之间的连接，并且允许数据在客户机与源服务器之间流动。在这一点，该代理主机作为一个隧道。如下文所述，直到该客户机转发该话路主要秘密时为止，该代理主机才变为一个“有效代理主机”。在步骤 30，该客户机与源服务器执行握手操作，以协商一个话路主要秘密。

然后，继续到步骤 32。在这一点，客户机把内部话路标识符与话路主要秘密一同发送到代理主机。如图所示，该信息是在主要话路上发送的。在步骤 34，该代理主机接收内部话路标识符和该话路主要秘密。它使用该信息来产生必要的密码信息，用于对源服务器的答复进行解密，以修改所提供的内容，和/或在把数据发送到客户机之前进行加密。然后，该代理主机切换到“有效代理主机”，用于与源服务器的当前连接。

在步骤 36，该客户机发送用于获得在源服务器上的资源的保密 HTTP 请求。可选地，在步骤 38，该代理主机可以对该请求解密，并且按照需要改变该请求，然后对新的请求加密并把其发送到其服务器。在步骤 40，该源服务器满足该请求，并且把答复数据发送回该代理主机。请注意，该源服务器甚至没有意识到代理主机活动的参与。在步骤 42，该代理主机接收该内容，对该数据进行解密和修改，以满足客户机的代码转换需要。可选地，在步骤 44，代理主机可以建立与源服务器的另一条连接（如果源服务器支持话路恢复的话）用于获得其它数据和/或改进性能。如果建立多个连接，使用密码链接（CBC）来调节该密码。如果，该代理主机没有建立另外的连接作为该话路的一部分，则它必须通过发送关于主要话路与话路标识符的通知而把该密码标准改变的情况通知给客户机。该处理在步骤 46 中示出，并且需要允许该客户机在将来的时间恢复与源服务器之间的话路。

根据本发明，在处理到初始源服务器的给定客户机请求过程中，该代

理主机可能要求到其它源服务器的其它保密话路。因此，例如，如果该代理主机要求到其它源服务器的其它保密话路，例如用于对该当前请求进行代码转换，它把一个通知发送到该客户机，要求该客户机建立与每个其它所要求的源服务器之间的新话路。这一般在步骤 48 中示出。最后，该代理主机对最终的代码转换后的内容进行加密，并且把它发送到客户机。这是步骤 50。

图 4 更加详细地示出该代理主机如何启动到其它源服务器的一个或多个其它保密话路。在该例子中，客户机 10" 按照上文所述的方式，与代码转换代码代理主机 15" 以及第一源服务器 12" 协作。如图中所示。话路 1 表示该客户机与该代理主机之间建立的初始话路，并且话路 2 表示该客户机与第一源服务器之间建立的保密话路。在图中所示的步骤（1）-（12）对应于在图 3 的流程图中所述的步骤。如果在所示的代码转换操作过程中，该代理主机 15" 确定它要求来自第二源服务器 17" 的保密数据，则该代理主机要求客户机 10" 建立与服务器 17" 之间的第二链接，特别地，通过再次隧道经过该代理主机而建立。这使得该客户机建立与第二服务器 17" 之间的一个主要秘密。该主要秘密有时被称为第二主要秘密，以使它区别于该客户机隧道经过代理主机到达第一源服务器而产生的第一话路主要秘密。特别地，在图 4 中的步骤（13）示出向客户机 10" 发出请求的代理主机 15"。然后，按照上文所述的方式对第二源服务器 17" 重复步骤（3）-（7）。

该代理主机 15" 具有按照需要使主要秘密保持隔离的能力，以便于一方面能够保证与客户机之间的保密通信，另一方面保证与各个源服务器之间的保密通信。因此，在原始客户机请求的情况下，该客户机和代理主机使用于每个源服务器话路的主要秘密保持隔离。这使得代理主机为客户访问并使用多个源服务器的数据。如果需要的话，该客户机可以把该话路主要秘密在相同的保密话路（例如，如图 1 中所示的话路 1）上，或者通过使用不同的保密话路传送到该代理主机。

如上文所示，给定的源服务器和代理主机都共享一个重要话路秘密。特别地，一旦客户机与给定的源服务器对一个重要话路秘密达成协议，

该秘密被通过以前在客户机与代理主机之间产生的一个保密话路提供到该代理主机。换句话说，该客户机在建立（客户机与代理主机之间的）主要（即，第一）话路之后，它释放该主要话路密钥（到该代理主机）。但是，源服务器不需要得知（并且一般也不会知道）该代理主机正在做一些工作或者参与到该保密连接中。

如上文所述，支持该保密代理所需的改变是很小的，并且仅仅影响该客户机和代理主机，而不会对需要处理给定客户机请求的给定源服务器造成影响。并且，该方法不需要该客户机泄露与其私钥相关的信息，或者泄露向该源服务器认证该客户机所用的方法。另外，由于该客户机能够建立到一个源服务器的其它连接，因此它可以改变密码标准或结束该话路，因此限制了该代理主机为该客户机建立到源服务器的其它连接的能力。

总结所需的改变，该客户机需要能够对与一个或多个源服务器分别协商的一个或多个话路主要秘密进行保密，并且把它们安全地传送到代理主机。该代理主机需要能够从客户机的主要秘密产生必须的加密信息，使其开始参与到该客户机的话路中。上述方法不需要对在话路秘密协商中所用的握手协议作任何改变。对整个网络业务量的额外负担为最小，因为在客户机与代理主机之间仅仅有一个额外的话路，而该客户机要求来自该代理主机的服务。不需要对源服务器作出改变。

客户机与代理主机之间的主要话路可以被认为是异步的，因为对每个到来的记录都有一个话路标识符。从客户机到代理主机的写入可能独立于代理主机对客户机的写入，因为在此不需要确认。当然，在此假设下层的传输层采用了可靠的传输方法。代理主机要求客户机建立新的连接（到其它源服务器），最好使用零*话路标识符，因为当客户机要求隧道通信时，可以由该代理主机随后指定一个标识符。为了提高性能，该代理主机不必把密码标准改变的情况通知给客户机，基于这种理解，该客户机将被强制执行完全认证握手操作，因为它将不与给定的源服务器相同步。这意味着在初始话路建立过程中对源服务器具有较大的有效负荷，但是如果代理主机建立新的连接或者向给定的源服务器或者一些其它源

服务器发送其它请求，则减少了无意义的通信。

现在有许多关于代理主机的应用。下面是几个代表性的例子。

代理主机的一种这样应用是减小对客户机执行加密/解密所要求的计算能力。例如，如果客户机处于防火墙背后，使用该代理主机，则该客户机可以仅仅一次执行认证步骤，然后无加密地在它与代理主机之间实际发送和接收数据，因此把加密有效负荷转移到代理主机。另外，在该代理主机可以与源服务器交换任何实际数据记录之前，它通过允许（或者要求）该客户机传递该话路秘密，而提供对防火墙配置审查的能力。在这种情况下，该代理主机不要求客户机传送任何关于它本身或源服务器的秘密/特权信息。在另一个例子中，该代理主机通过允许缓存代理主机参与该话路中而不改变客户机与源服务器之间的话路的保密特性，来提高客户机的性能。另外，该代理主机可以用于为该客户机预取内容（通过在以后重新启动话路），而不需要该代理主机明确知道该客户机的私钥。在这种情况下，该代理主机例如可以在非繁忙时间过程中定期地更新该用户的预定内容。这些例子仅仅是说明性的而不是对本发明的范围的限制。

因此，如上文所述，本发明的另一个应用是使得第三方能够参与涉及分布式计算客户机设备的保密话路中。代表性的设备包括分布式客户机，即，基于 x86-, PowerPc®或者 RISC（精简指令集计算机）的客户机，其包括一种实时的操作系统，例如，WindRiver VXWorks™、QSSL QNXNeutrino™ 或者 Microsoft Windows CE，并且其可以包括网络浏览器。该应用没有在下文中更加详细描述。

现在参见图 5，一种代表性的分布式计算设备包括客户机堆栈 140，其中包括多个部件，例如，客户机应用程序构架 143、虚拟机 144、语音引擎 146 以及工业上应用的实时操作系统（RTOS）148。该客户机应用程序构架 142 一般包括浏览器 150、用户界面 152、分布式计算客户应用程序类库 154、标准 Java 类库 156 以及通信堆栈 158。分布式计算客户机通过连接服务 162 连接到服务器平台 160。

在其下层，该连接服务 62 包括提供压缩和加密功能的网关 164。该网

(修改)

关采用网络保密协议，该协议已经被根据本发明的方法而扩展。连接服务 162 的上层是代理主机 166，其提供一种或多种不同的功能，例如：代码转换、过滤、优先排列以及链接到设备管理。

该服务器平台 160，即给定的源服务器，可以是几种不同的类型。该平台 160 可以是网络/应用程序服务器 170（同步请求响应型服务器）或者数据同步服务器 172（异步队列通信型服务器）。在此说明每种服务器的基本功能。另外，该平台 160 可以是一种增值服务器 174，其提供附加的服务，例如 LDAP 目录/档案管理、警告和通知、网络管理、设备使用寿命周期管理、用户和设备登记或者编制帐单。

保密代理协议提供多种比现有技术更优越的性能。如上文所述，协议扩展不改变在记录协议的保密连接的基本特性。另外，对代理主机的连接是秘密，并且对称的密码技术（例如，DES、RC4 等等）可以用于数据加密。用于该对称加密的密钥最好是对每次连接唯一产生的，并且基于通过另一种协议所协商的秘密（例如 TLS 或者 SSL 握手协议）。另外，到代理主机的连接是可靠的。消息传输一般包括使用键控的 MAC 的消息完整性检查。最好，保密散列函数（例如，SHA、MD5 等等）被用于 MAC 计算。

握手协议提供具有几个基本特征的保密性。对等身份可以使用不对称密码技术（例如，RSA、DSS 等等）来认证，即使用公钥进行认证。该认证是可选的，但是一般需要至少一个对等机。另外，共享秘密的协商是保密的。协商的秘密不被窃听，并且对任何认证的连接，该秘密甚至不能被置身于该连接中的攻击者所获得。另外，与代理主机的协商是可靠的。没有攻击者能够改变协商的通信而不被通信方所检测。

如上文所述，保密协议使得代理主机参与到客户机与一组源服务器之间的保密话路中，而不改变该话路的属性。该方法还独立于加密强度或者所用的认证技术。

本发明可以在处理器中用可执行软件实现，例如，作为驻留在计算机的随机存取存储器的代码模块中的一组指令（程序代码）。直到由计算机所要求，该组指令才可以存储在另一个计算机存储器中，例如存储在

硬盘驱动器中，或者存储在可移动存储器中，或者通过互联网或其它计算机网络下载。

另外，尽管所述的各种方法在由软件选择激活或重新配置的普通计算机中实现，但是本领域内的专业人员，可以认识到这种方法可以在硬件、固件或者在被构造用于执行所需方法步骤的更加专用的装置中执行。

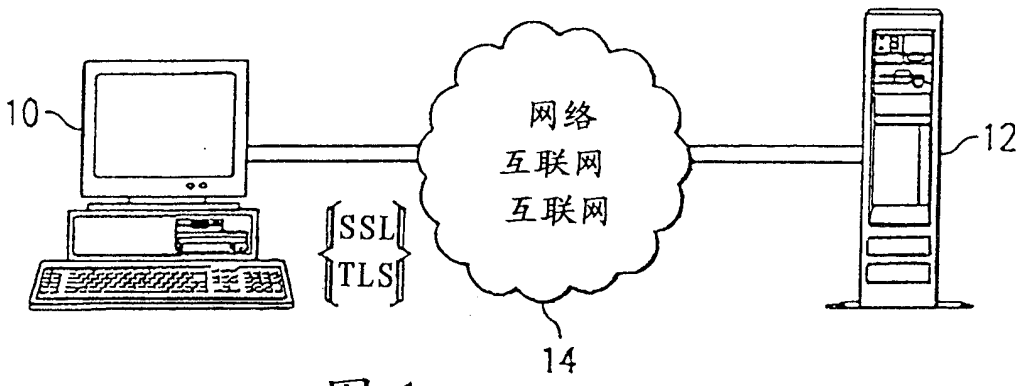

10
网络
互联网
互联网
12
SSL
TLS
14

图 1

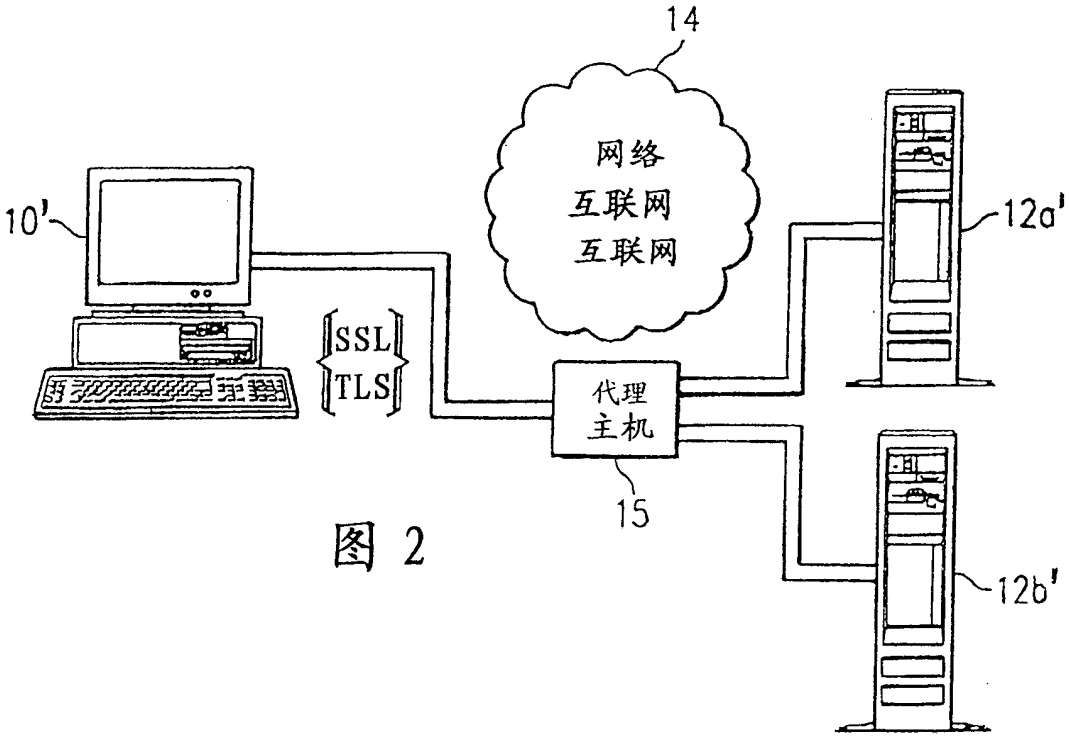

14
网络
互联网
互联网
10'
12a'
SSL
TLS
代理
主机
15
12b'

图 2

客户机（1）	代理主机（1）	客户机（2）	代理主机（2）	源服务器
客户机问候				
	服务器问候			
20	证书*			
	证书请求*			
	服务器密钥交换*			
证书*				
客户机密钥交换				
证书认证*				
改变密码标准				
结束				
	交换密码标准	24		
22	结束		26	
		HTTP “连接”		
			创建话路标识	
		客户机问候		
			28	服务器问候
				证书*
				证书请求*
				服务器密钥交换*
		证书*		
		客户机密钥交换		
		证书认证		
32		改变密码标准	30	
		结束		
发送“主要秘密”和代理主机话路标识				改变密码标准

到图 3B

图 3A

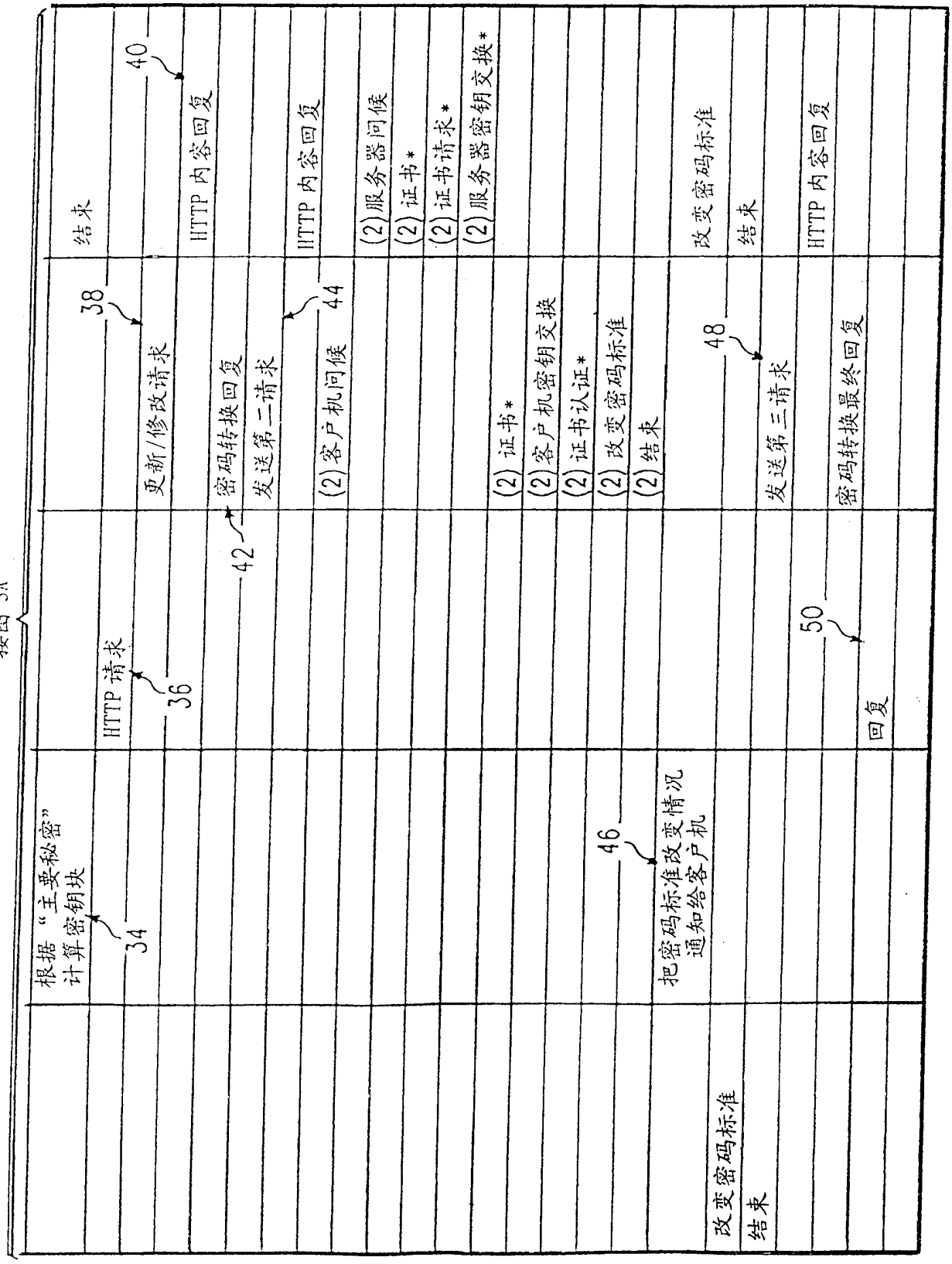

接图 3A
根据“主要秘密”计算密钥块
34
HTTP 请求
36
更新/修改请求
38
结束
40
HTTP 内容回复
密码转换回复
42
发送第二请求
(2)客户机问候
44
HTTP 内容回复
(2)服务器问候
(2)证书*
(2)证书请求*
(2)服务器密钥交换*
(2)证书*
(2)客户机密钥交换
(2)证书认证*
(2)改变密码标准
46
(2)结束
把密码标准改变情况通知给客户机
改变密码标准
48
结束
发送第三请求
50
HTTP 内容回复
密码转换最终回复
回复

图 3B

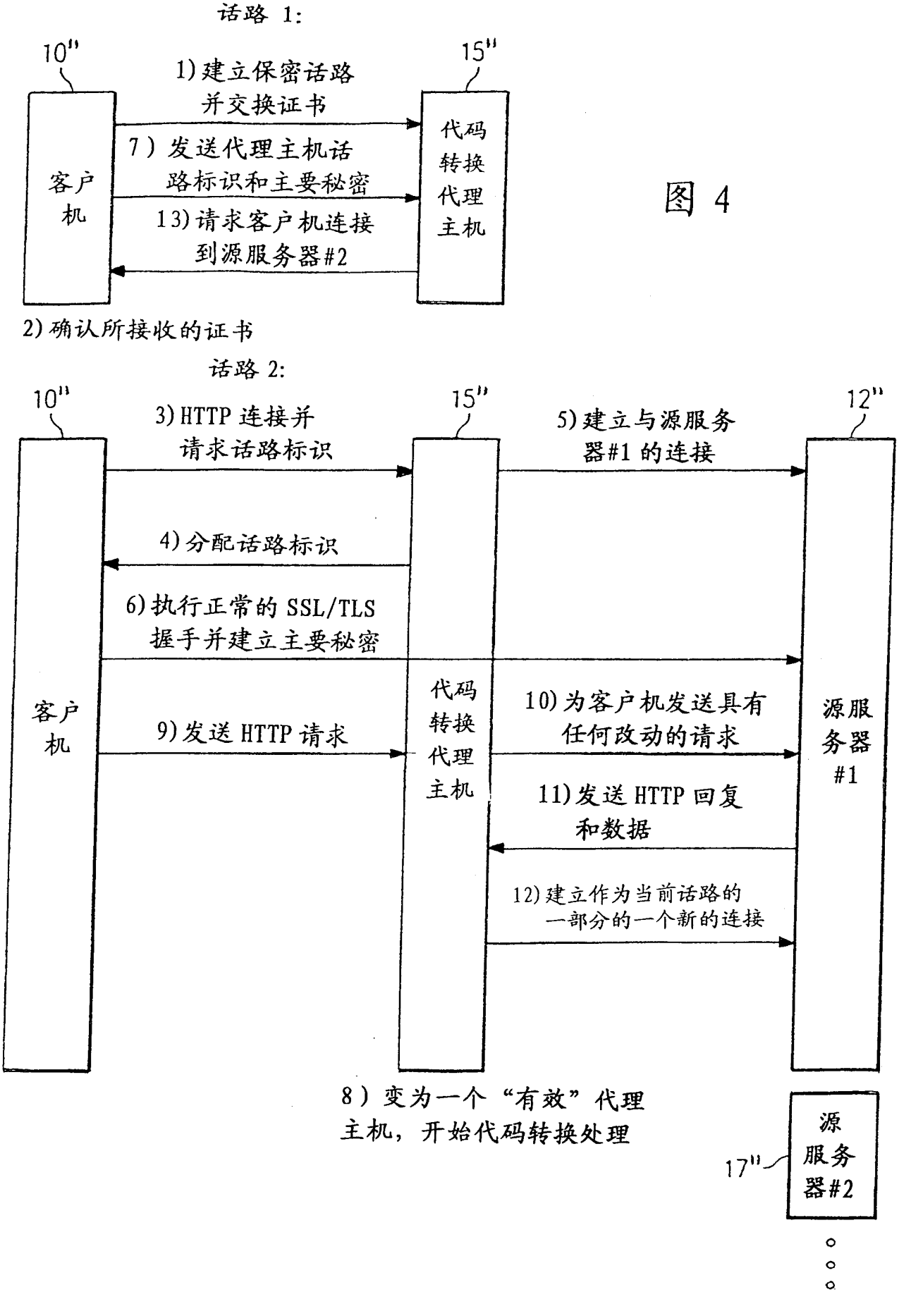

话路 1:
10''
15''
1) 建立保密话路
并交换证书
7) 发送代理主机话
路标识和主要秘密
13) 请求客户机连接
到源服务器#2
客户机
代码转换代理主机
2) 确认所接收的证书
话路 2:
10''
15''
12''
3) HTTP 连接并
请求话路标识
5) 建立与源服务
器#1 的连接
4) 分配话路标识
6) 执行正常的 SSL/TLS
握手并建立主要秘密
客户机
9) 发送 HTTP 请求
代码转换代理主机
10) 为客户机发送具有
任何改动的请求
源服务器#1
11) 发送 HTTP 回复
和数据
12) 建立作为当前话路的
一部分的一个新的连接
8) 变为一个“有效”代理
主机，开始代码转换处理
17''
源服务器#2

图 4

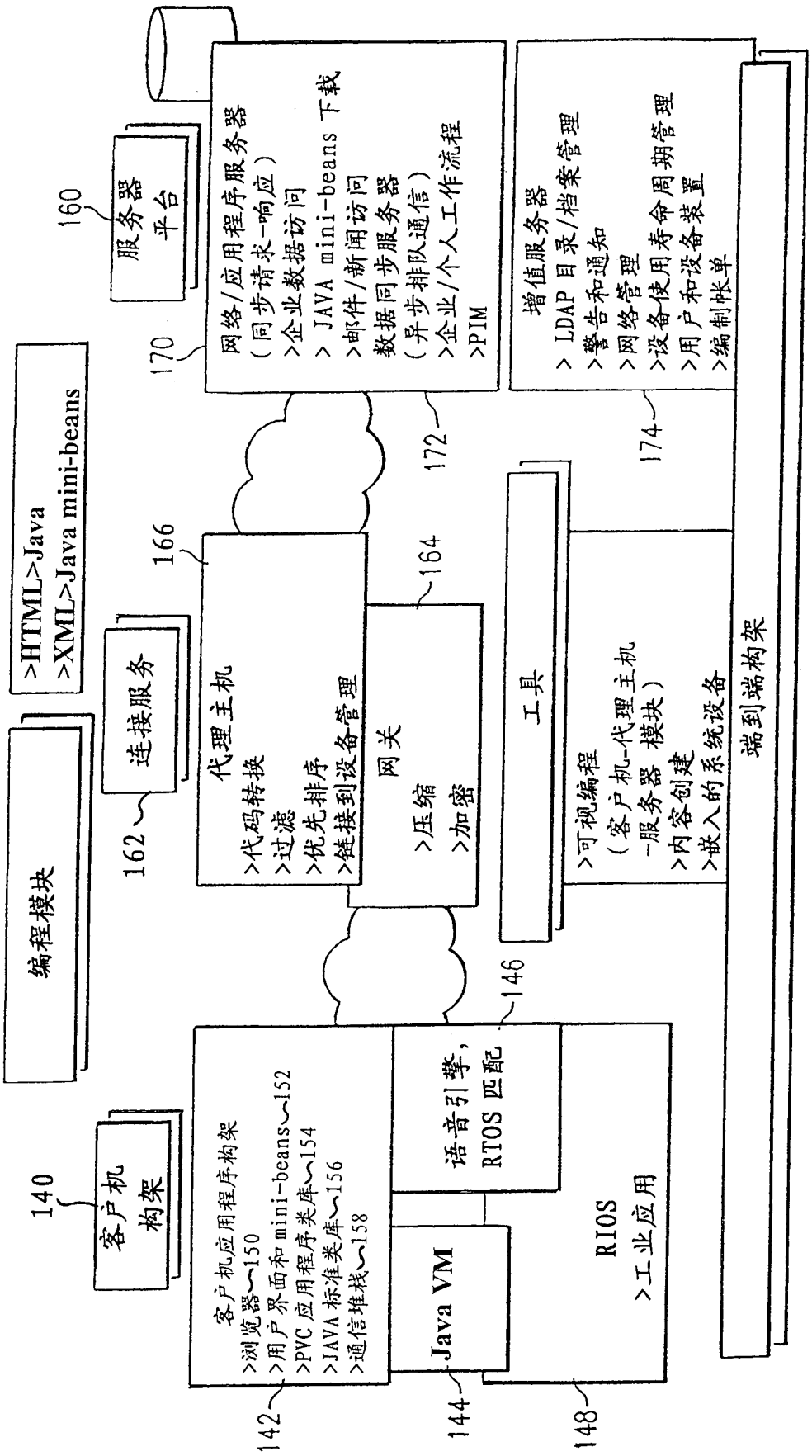

140
客户机
构架
编程模块
>HTML>Java
>XML>Java mini-beans
160
服务器
平台
170
网络/应用程序服务器
（同步请求-响应）
>企业数据访问
> JAVA mini-beans 下载
>邮件/新闻访问
数据同步服务器
（异步排队通信）
>企业/个人工作流程
>PIM
172
增值服务器
> LDAP 目录/档案管理
>警告和通知
>网络管理
>设备使用寿命周期管理
>用户和设备装置
>编制帐单
174
162
连接服务
166
代理主机
>代码转换
>过滤
>优先排序
>链接到设备管理
164
网关
>压缩
>加密
工具
>可视编程
（客户机-代理主机
-服务器 模块）
>内容创建
>嵌入的系统设备
端到端构架
146
客户机应用程序构架
>浏览器150
>用户界面和 mini-beans152
>PVC 应用程序类库154
>JAVA 标准类库156
>通信堆栈158
142
Java VM
144
语音引擎，
RTOS 匹配
RIOS
>工业应用
148

图 5