(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101156346 B
(45)授权公告日 2012.04.18

(21)申请号 200680011542.2

(22)申请日 2006.02.10

(30)优先权数据
60/652,063 2005.02.11 US

(85)PCT申请进入国家阶段日
2007.10.09

(86)PCT申请的申请数据
PCT/US2006/004901 2006.02.10

(87)PCT申请的公布数据
WO2006/086721 EN 2006.08.17

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 迈克尔·帕登
格雷戈里·戈登·罗斯
詹姆斯·森普尔
菲利普·迈克尔·霍克斯

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 刘国伟

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/00(2006.01)

(56)对比文件
JP 特开 2004-208073 A,2004.07.22,
JP 特开 2004-207965 A,2004.07.22,

审查员 高霞

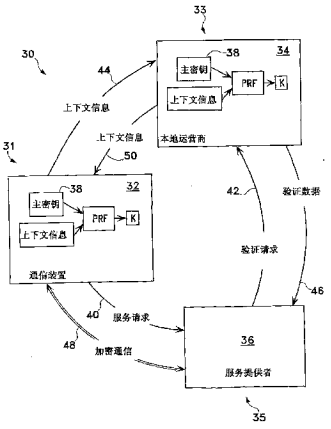
权利要求书 2 页 说明书 6 页 附图 6 页

(54)发明名称

受上下文限制的共享密钥

(57)摘要

在其中两个通信实体想要进行秘密或机密通信对话的通信系统中，需要首先建立信任关系。信任关系是基于对共享密钥的确定，而共享密钥又是根据上下文信息产生的。所述上下文信息可自通信对话周围的环境中导出。例如，上下文信息可包括拓扑信息、基于时间的信息和事务信息。共享密钥可以是自身产生的或自第三方接收的。在任一情形中，可将共享密钥用作在通信实体之间所使用的任一加密协议的关键资料。



CN 101156346 B

1. 一种用于建立与通信实体的信任关系的方法，其包括：

发送请求以从通信实体接收服务作为通信对话的一部分；

获得主密钥；

基于上下文信息和所述主密钥产生共享密钥，其中所述上下文信息从对应于所述通信对话的至少一个环境导出；及

基于所述共享密钥建立与所述通信实体的安全通信。

2. 如权利要求 1 所述的方法，其中所述上下文信息进一步包括拓扑信息。

3. 如权利要求 1 所述的方法，其中所述上下文信息进一步包括基于时间的信息。

4. 如权利要求 1 所述的方法，其中所述上下文信息进一步包括事务信息。

5. 如权利要求 1 所述的方法，其进一步包括自另一通信实体接收所述上下文信息。

6. 如权利要求 1 所述的方法，其进一步包括使用所述共享密钥作为关键资料来以加密方式与所述通信实体通信。

7. 一种用于调解至少两个通信实体的信任关系的方法，其包括：

从第一通信实体接收已经请求接收来自所述第一通信实体的服务作为通信对话的一部分的第二通信实体的验证请求；

获得主密钥；

基于上下文信息和所述主密钥产生共享密钥，其中所述上下文信息从对应于所述通信对话的至少一个环境导出；及

基于所述共享密钥将验证信息提供至所述第一通信实体或者所述第二通信实体中的至少一者。

8. 如权利要求 7 所述的方法，其中所述上下文信息进一步包括拓扑信息。

9. 如权利要求 7 所述的方法，其中所述上下文信息进一步包括基于时间的信息。

10. 如权利要求 7 所述的方法，其中所述上下文信息进一步包括事务信息。

11. 如权利要求 7 所述的方法，其进一步包括所述第一通信实体或者所述第二通信实体的一者接收所述上下文信息。

12. 如权利要求 7 所述的方法，其进一步包括将所述验证信息中的所述共享密钥提供至所述第一通信实体。

13. 一种用于与通信实体建立信任关系的设备，其包括：

用于发送请求从一通信实体接收服务作为通信对话的一部份的装置；

用于获得主密钥的装置；

用于基于上下文信息和所述主密钥产生共享密钥的装置，其中所述上下文信息从对应于所述通信对话的至少一个环境导出；及

用于基于所述共享密钥建立与所述通信实体的安全通信的装置。

14. 如权利要求 13 所述的设备，其中所述上下文信息进一步包括拓扑信息。

15. 如权利要求 13 所述的设备，其中所述上下文信息进一步包括基于时间的信息。

16. 如权利要求 13 所述的设备，其中所述上下文信息进一步包括事务信息。

17. 如权利要求 13 所述的设备，其进一步包括用于从另一通信实体接收所述上下文信息的装置。

18. 如权利要求 13 所述的设备，其进一步包括用于使用所述共享密钥作为关键资料而

以加密方式与所述通信实体通信的装置。

19. 一种用于调解与至少两个通信实体的信任关系的设备，其包括：

用于从第一通信实体接收已经请求接收来自所述第一通信实体的服务作为通信对话的一部分的第二通信实体的验证请求的装置；

用于获得主密钥的装置；

用于基于上下文信息和所述主密钥产生共享密钥的装置，其中所述上下文信息从对应于所述通信对话的至少一个环境导出；及

用于基于所述共享密钥将验证信息提供至所述第一通信实体或者所述第二通信实体中的至少一者的装置。

20. 如权利要求 19 所述的设备，其中所述上下文信息进一步包括拓扑信息。

21. 如权利要求 19 所述的设备，其中所述上下文信息进一步包括基于时间的信息。

22. 如权利要求 19 所述的方法，其中所述上下文信息进一步包括事务信息。

23. 如权利要求 19 所述的设备，其进一步包括用于从所述第一通信实体或者所述第二通信实体中的一者接收所述上下文信息的装置。

24. 如权利要求 19 所述的设备，其进一步包括用于将所述验证信息中的所述共享密钥提供至所述第一通信实体的装置。

受上下文限制的共享密钥

[0001] 根据 35 U.S.C. §119 主张优先权

[0002] 本专利申请案主张优先于 2005 年 2 月 11 日提出申请且名称为“受上下文限制的密钥 (Context Limited Secret Key)”的第 60/652,063 号美国临时申请案，所述美国临时申请案受让于本发明的受让人，且以引用方式明确地并入本文中。

技术领域

[0003] 本发明大体而言涉及通信，且更具体而言，涉及使用根据受上下文限制的信息所产生的共享密钥进行安全和秘密通信。

背景技术

[0004] 共享密钥的使用对于想要安全或秘密的通信而言很常见。在典型的共享密钥方案中，是共享仅为通信实体已知的共用密钥，其中各通信实体依赖所述密钥来建立信任关系。不具有共享密钥的一方被排除在信任关系之外。

[0005] 共享密钥可以是永久的或临时的。临时的共享密钥可用于在有限时期内保护通信。举例而言，临时的共享密钥可仅适用于一次性事务。

[0006] 为提供额外的安全级别，通常自永久密钥导出临时密钥。在这种安排中，临时密钥被用作建立信任关系的基础。例如，想要与对应方建立信任关系的一方可使用临时密钥，所述临时密钥作为与对应方进行加密通信的关键资料而与对应方共享。

[0007] 对于有时称作主密钥的永久密钥而言，其极少被无限制地共享。例如，在移动通信设定中，仅在用户单元和用户的本地运营商之间共享主密钥。当用户单元经由安全通信自第三方请求服务时，所述用户单元根据主密钥产生临时密钥。同时，用户单元也发送请求至本地运营商，本地运营商又根据共享的主密钥产生相同的临时密钥。同样，所述临时密钥形成用户与第三方之间的信任关系的基础。例如，除了别的以外，用户单元和本地运营商二者还可根据所述临时密钥而产生随后可供服务提供者使用的加密密钥。其后，可交换用户单元与服务提供者之间的加密通信。

[0008] 从主密钥导出临时密钥的基本原理是降低暴露主密钥的可能性。可基于用户单元和本地运营商之间的某些预先安排的演算法而从主密钥导出临时密钥。

[0009] 上述安全模型基于下述假设：任一可能已访问任何所导出密钥的第三方将愿意保护所导出密钥的机密性。例如，如果第三方将所导出密钥暴露给再一方，则自第三方购买服务的信任度将被严重损害。因此，作为持久性商务实体，第三方将受到不利影响，更不必说暴露密钥的法律后果。

[0010] 然而，可能存在某些对于将共享密钥保密既没有经济动机也没有伦理考虑的参与方。例如，如果所导出密钥被传送至自称为用户的欺诈方，则欺诈方可能使用所导出密钥假扮合法用户，并能够访问其本来不能访问的服务。更复杂的是，从所述非法访问中可能进一步暴露其他敏感信息。如果欺诈方将其自身设定为服务提供者，则会导致同样或更严重的后果。

[0011] 因此，需要提供一种更安全的通信方案以避免暴露和误用所导出密钥。

发明内容

[0012] 在其中两个通信实体想要进行秘密或机密通信对话的通信系统中，需要首先建立信任关系。信任关系是基于对共享密钥的确定，而共享密钥是根据主密钥和所选的上下文信息而产生。上下文信息可根据所述通信对话周围的环境导出。共享密钥可由每一通信实体自身产生。或者，在其中所述实体并无足够信息以直接导出共享密钥的情形中，可自第三方导出共享密钥。所述共享密钥可用作加密协议的关键资料，用于验证和建立各通信实体之间的安全通信。

[0013] 在一实例性实施例中，作为一个通信实体的用户单元从作为另一通信实体的服务提供者处寻求服务。用户单元基于预存储的主密钥和预定的上下文信息而独立地产生共享密钥，上下文信息可包括（但不限于）拓扑信息、基于时间的信息和事务信息。不具有主密钥的服务提供者自再一方获得共享密钥。随后，服务提供者和用户单元使用其对共享密钥的共有知识建立信任关系。在这一实例中，所述另一实体是用户单元的本地运营商。在将共享密钥发送至服务提供者之前，本地运营商以与用户单元大致相同的方式产生共享密钥。将共享密钥从本地运营商发送至服务提供者也可以经由预先商定的保护机制来保护。

[0014] 因此，通过以上述方式操作，所产生的共享密钥不太可能被非法复制和误用。

[0015] 结合附图阅读下文详细说明，所属技术领域的技术人员将易于了解这些和其他特征及优点，其中相同的参考符号表示相同的部件。

附图说明

[0016] 图 1 是显示本发明的一般实施例的简化示意图；

[0017] 图 2A 是根据一实施例的流程图，其显示通信实体在为进行通信对话而首先想要建立信任关系时所涉及的步骤；

[0018] 图 2B 是根据图 2A 所示实施例的流程图，其显示中间实体促进建立所述信任关系所涉及的步骤；

[0019] 图 3A 是根据另一实施例的流程图，其显示通信实体在为进行通信对话而首先想要建立信任关系时所涉及的步骤；

[0020] 图 3B 是根据图 3A 所示实施例的流程图，其显示中间实体促进建立所述信任关系所涉及的步骤；及

[0021] 图 4 是显示用于实施本发明实施例的硬件实施方案的一部分的示意图。

具体实施方式

[0022] 提供下述说明旨在使所属技术领域的技术人员均能够制作及利用本发明。出于解释的目的，在下文说明中列举若干细节。应了解，所属技术领域的技术人员将认识到，不使用这些具体细节也可以实施本发明。在其他实例中，为避免因不必要的细节而淡化本发明的说明，未详细阐述熟知的结构和过程。因此，本发明并不打算受限于所示实施例，而是欲赋予其与本文所揭示原理及特征相一致的最宽广范畴。

[0023] 图 1 显示本发明的一般实施例的简化示意图。通信系统总体上由参考数字 30 表

示，且可以是载送语音、数据、多媒体或其组合的系统。此外，系统 30 可按各种标准和协议操作，其实例包括 cdma2000（码分多工存取 2000）、GSM（全球移动通信系统）、WCDMA（宽频码分多址存取）和 IP（因特网协议）。

[0024] 出于清晰和简练说明的目的，图 1 中仅显示 3 个实体，也就是第一通信实体 31、第二通信实体 33 和第三通信实体 35。在这一实例性实施例中，第一实体 31 是通信装置 32。第二实体 33 是本地运营商 34。第三实施例 35 是服务提供者 36。

[0025] 在这一实例中，假设通信装置 32 是本地运营商 34 的用户。通信装置 32 可以是有线装置，例如，装置 32 可以是连线至与本地运营商 34 处于相同网络的操作站。另一选择为，通信装置 32 可以是无线装置。例如，装置 32 可以是移动电话、移动计算机或个人数字助理 (PDA)。因此，通信装置 32 可以与本地运营商 34 位于相同的网络中。另外，通信装置 32 也可以定位于本地运营商 34 所处的网络之外。例如，通信装置 32 可以自本地运营商 34 所处的网络漫游至其他网络，且可与其他网络中的其他实体通信。

[0026] 现在返回参看图 1。在这一实例中，假设通信装置 32 向服务提供者 36 请求服务。当通信装置 32 位于本地运营商 34 的网络中时，所请求的服务可以是向本地运营商 34 正常请求的服务。作为另一实例，所请求的服务也可以是仅由服务提供者 36 而非本地运营商 34 提供的服务。服务提供者 36 可以在本地运营商 34 的网络内部或外部。

[0027] 出于安全和秘密的原因，通信装置 32 可能首先想要确保服务提供者 36 经授权以提供这种服务。同样地，服务提供者 36 本身也可能（例如）出于收费的目的而需要了解通信装置 32 是合法的。换句话说，在任何通信之前，需要首先在通信装置 32 和服务提供者 36 之间建立信任关系。

[0028] 根据这一实施例，通信装置 32 和本地运营商 34 共享由图 1 中的参考数字 38 象征性地标识的主密钥。

[0029] 为开始所述过程，通信装置 32 首先将服务请求发送至服务提供者 36（以通信路径 40 表示）。其后，遵循建立信任关系的过程。

[0030] 对于通信装置 32 而言，其首先通过伪随机函数 (PRF) 产生共享密钥 K。除了别的以外，PRF 的输入还可包括主密钥 38 和上下文信息。

[0031] PRF 的实例可以是基于散列的消息验证代码 (HMAC)、安全散列演算法 1(SHA-1) 或其组合。HMAC 和 SHA-1 二者均可以在由因特网工程任务组 (IETF) 发布的征求评论 (RFC) 中找到。具体而言，HMAC 列举于 1997 年 2 月的 RFC 2104 中，其名称为“HMAC :用于消息验证的密钥散列 (HMAC :Keyed-Hashing for MessageAuthentication)”。SHA-1 演算法界定于 2001 年 9 月的 RFC 3174 中，其名称为“美国安全散列演算法 1(U.S. Secure Hash Algorithm 1)”。

[0032] 根据本发明的这一实施例，可自通信对话周围的环境中导出上下文信息。

[0033] 上下文信息可以是基于拓扑的。例如，在根据 IP 操作时，拓扑信息可包括图 1 所示各实体 31、33 和 35 的源地址和目的地址。另外，前述地址可另外包括为获得额外安全等级而指定地址块的网络掩码。对于根据传输控制协议 (TCP) 和用户数据报协议 (UDP) 的通信而言，也可以包括源端口和目的端口。

[0034] 上下文信息也可以和时间相关。换句话说，通信对话的环境周围的某些时间参数可以用于上下文信息。例如，上下文信息可以包括特定通信对话（例如，通信装置 32 发送

至服务提供者 36 的服务请求 40 的对话）的开始时间、结束时间、持续时间。

[0035] 上下文信息也可以是针对具体事务的。在各种通信系统中，通常以一标识符唯一地标识每一通信对话，一般将所述标识符称作现时或事务标识符。也可以使用及包含这种标识信息作为上下文信息。

[0036] 如先前提及，为产生共享密钥 K，对 PRF 的输入可包括主密钥和上下文信息。其以算术方式可表达如下：

[0037] K = PRF（主密钥，上下文信息） (A)

[0038] 其中主密钥是（例如）前述密钥 38，且上下文信息可进一步表达如下：

[0039] 上下文信息 = ∪（服务器地址，服务器端口，

[0040] 开始时间，结束时间，随机现时） (B)

[0041] 其中 ∪ 将一组参数标示为包含于方程式 (B) 的括号内。在这一特定实例中，服务器地址是服务提供者 36 的网络地址，服务器端口是服务提供者 36 的端口编号，开始时间是通信装置 32 将服务请求 40 发送至服务提供者 36 的时间的起点，结束时间是前述服务请求结束时的终点时间。

[0042] 就服务提供者 36 而言，在从通信装置 32 接收到服务请求时，如图 1 所示通信路径 42 所标识，服务提供者 36 通知本地运营商 34 进行验证。同时，如通信路径 44 所标识，通信装置 32 出于自身主动、或根据来自本地运营商 34 的请求而将上下文信息发送至本地运营商 34。借助上下文信息和预存储的主密钥 38，本地运营商 34 又根据方程式 (A) 和 (B)、以与先前所述由通信装置 32 产生共享密钥 K 的相同方式产生共享密钥 K。

[0043] 共享密钥 K 为服务提供者 36 和通信装置 32 之间的后续安全通信提供支持基础。

[0044] 例如，对于安全和秘密通信而言，可稍后在服务提供者 36 和通信装置 32 之间使用各种加密协议。每一加密协议可要求一加密密钥 Ke 以对安全通信数据加密。所述加密密钥 Ke 可根据共享密钥 K 产生。

[0045] 作为另一实例，如果可行，可使用共享密钥 K 产生在服务提供者 36 和通信装置 32 之间交换的询问数据。询问数据可包括询问消息和所期望回应。所期望回应可仅根据所述询问消息及使用关于共享密钥 K 的所知信息而产生。例如，参看图 1，如果服务提供者 36 已自本地运营商 34 接收到共享密钥 K，则服务提供者 36 可通过将询问消息发送至通信装置 32 来询问通信装置 32 的可靠性。通信装置 32 具有共享密钥 K。通信装置 32 可随后基于共享密钥 K 产生所期望消息，并将所期望消息发送至服务提供者 36 进行验证。随后，服务提供者 36 可基于先前自本地运营商 34 接收的共享密钥 K，通过比较从通信装置 32 接收的所期望消息和其自身产生的期望消息来确定通信装置 32 的可靠性。

[0046] 现在继续参看图 1。如通信路径 46 所标识，回应于验证请求 32 且根据随后要使用的加密协议，本地运营商 33 将验证数据（其在这一实例中包括共享密钥 K）发送至服务提供者 36。经由通信路径 46 传输验证数据可由预先安排的安全机制来保护。

[0047] 一旦通信装置 32 和服务提供者 36 拥有共享密钥 K，则其可使用密钥 K 作为建立加密安全通信的关键资料。通信装置 32 和服务提供者 36 之间的加密通信的通信路径由图 1 所示的参考数字 48 标示。

[0048] 上述过程概述于图 2A 及图 2B 所示的流程中。图 2A 显示由通信装置 32 执行的过程步骤。图 2B 显示由本地运营商 34 执行的对应过程步骤。

[0049] 通过以上述方式进行操作，如果共享密钥 K 被不正确地泄露至未授权方，则由于必须复制最初为之产生共享密钥 K 的确切上下文信息才能成功，因而会大大降低未授权方未经授权地使用密钥 K 冒充合法密钥持有者的可能性。

[0050] 另一选择为，除了使通信装置 32 将上下文信息发送至本地运营商 38 之外，也可相反地进行。也就是说，在接收到来自服务提供者 36 的验证请求时，本地运营商 38 可将上下文信息发送至通信装置 32。举例而言，方程式 (B) 中的预定参数开始时间和结束时间可分别设定于图 1 所示验证请求 42 的开始和结束时间处。随后，通信装置 32 可使用所接收的上下文信息产生共享密钥 K。再次，共享密钥 K 可再次用作适用于任一要用于通信装置 32 和服务提供者 36 之间的加密通信的加密协议的关键资料。所述过程与上述过程大致类似，且概述于图 3A 及 3B 所示流程图中。图 3A 显示由通信装置 32 执行的过程步骤。图 3B 显示由本地运营商 34 执行的对应过程步骤。

[0051] 图 4 示意性地显示根据本发明的实例性实施例由参考数字 60 表示的设备（例如，图 1 所示通信实体 31 和 33）的硬件实施方案的一部分。设备 60 可以各种形式建立和合并，例如固定式计算机、网络硬件的一部分、膝上型计算机、PDA 或蜂窝式电话（文中仅列举少量）。

[0052] 设备 60 包括将数个电路链接在一起的中央数据总线 62。所述电路包括 CPU（中央处理单元）或控制器 64、接收电路 66、发射电路 68 和存储器电路 70。

[0053] 如果设备 60 是无线装置的一部分，则接收电路 66 和发射电路 68 可连接至 RF（射频）电路，但未显示于图式中。接收电路 66 在将所接收信号发送出至数据总线 62 之前对其进行处理和缓冲。另一方面，发射电路 68 在将来自数据总线 62 的数据发送出装置 60 之前对其进行处理和缓冲。CPU/ 控制器 64 执行数据总线 62 的数据管理功能，并进一步执行一般数据处理功能，包括执行存储器单元 70 的指令内容。

[0054] 或者，发射电路 68 和接收电路 66 可以是 CPU/ 控制器 64 的一部分，而非如图 4 中所示单独放置。

[0055] 存储器单元 70 包括一组总体上由参考数字 72 表示的指令。在这一实施例中，除了别的以外，相依于设备 60 所起的作用，所述指令还包括图 2A、2B、3A 和 3B 所示流程图所显示及阐述的过程步骤，所述步骤笼统地由参考数字 74 指定为图 4 所示“共享密钥产生及处理功能”。函数 74 中可包含前述 PRF。

[0056] 存储器单元 70 中还包含用于实施任何所选加密协议的加密通信功能 76。此外，除了别的以外，同一存储器单元 70 中还存储有主密钥 38。例如，在设备 60 的加电期间，可将函数 74、76 和主密钥 38 从一不同的存储器单元（未显示）传递至存储器单元 70。

[0057] 在这一实施例中，存储器单元 70 是 RAM（随机访问存储器）电路。实例性指令部分 72 是软件例程或模块。如上文提及，存储器单元 70 可连接至另一易失性或非易失性类型的存储器电路（未显示）。或者，存储器单元 70 可由其他电路类型制成，例如 EEPROM（电可擦除可编程只读存储器）、EPROM（电可编程只读存储器）、ROM（只读存储器）、ASIC（应用专用集成电路）、磁盘、光盘和所属技术领域中熟知的其他电路。

[0058] 进一步应了解，上文中图 2A、2B、3A 和 3B 所阐述及显示的过程也可以编码为承载于所属技术领域中熟知的任何计算机可读媒体上的计算机可读指令。在本说明书及随附权利要求书中，术语“计算机可读媒体”是指任何参与将指令提供至任一处理器（例如，图 4 所

示及所述 CPU/ 控制器 64) 以供用于执行的媒体。这种媒体可以是任一存储器类型，且可以采取先前阐述（例如，在图 4 所示存储器单元 70 的说明中所述）的易失性或非易失性存储媒体的形式。这种媒体也可以是传输型的，且可包括同轴电缆、铜导线、光纤和携载能够携载机器或计算机可读信号的声波或电磁波的无线接口。

[0059] 最后，如所述实施例中阐述，第一、第二和第三通信实体 31、33 和 35 分别被阐述为通信装置 32、本地运营商 34 和服务提供者 36。本发明中可存在不同安排。例如，第一实体 31 除装置外还可呈现不同形式，例如路由器、网络或运营商的一部分。同样地，第二和第三实体 33 和 35 也可以呈现与先前所提及不同的形式。在所述实例性实施例中，共享密钥被阐述为根据主密钥以及上下文信息而产生。可想象共享密钥也可以使用不同于上述方程式 (A) 中所列的其他信息而产生。例如，诸如来自全球定位系统 (GPS) 的坐标或通信实体的电子标识等非上下文信息当然可充当方程式 (A) 的额外输入。对于可包括不同于所述的其他上下文信息的方程式 (B) 而言，同样如此。另一方面，并非必需包含在实例性实施例中所阐述的所有上下文信息才能产生共享密钥。可仅使用部分或所选信息。例如，可并非如上文所述使用各种拓扑、时间相关和事务信息来产生所述共享密钥，而是可仅将所选的拓扑信息输入至 PRF 以得出共享密钥。此外，在实例性实施例中，通信装置 32 和本地运营商 34 被阐述为收集所述上下文信息的实体。使服务提供者 36 执行上下文信息收集职能并将所收集信息直接或间接地发送至其他方也是确实可行的。此外，结合所述实施例阐述的任何逻辑块、电路和算法步骤均可实施于硬件、软件、固件或其组合中。所属技术领域中的技术人员将了解，可在不背离本发明的精神及范畴的情况下对其中在形式和细节上作出这些和其他改变。

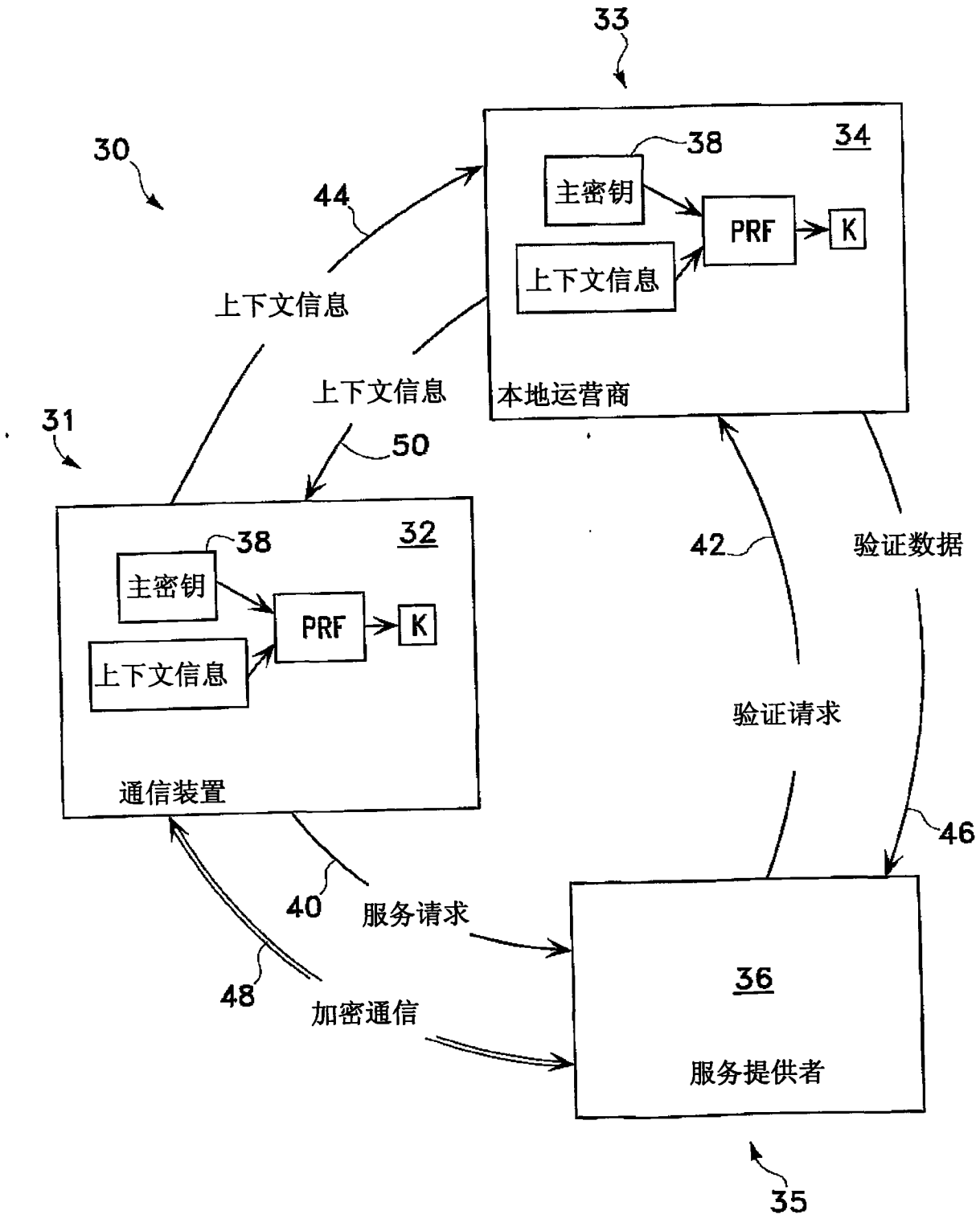

33
30
34
38
主密钥
PRF
K
上下文信息
44
上下文信息
本地运营商
上下文信息
31
50
32
38
主密钥
PRF
K
上下文信息
通信装置
42
验证数据
验证请求
46
40
服务请求
48
加密通信
36
服务提供者
35

图 1

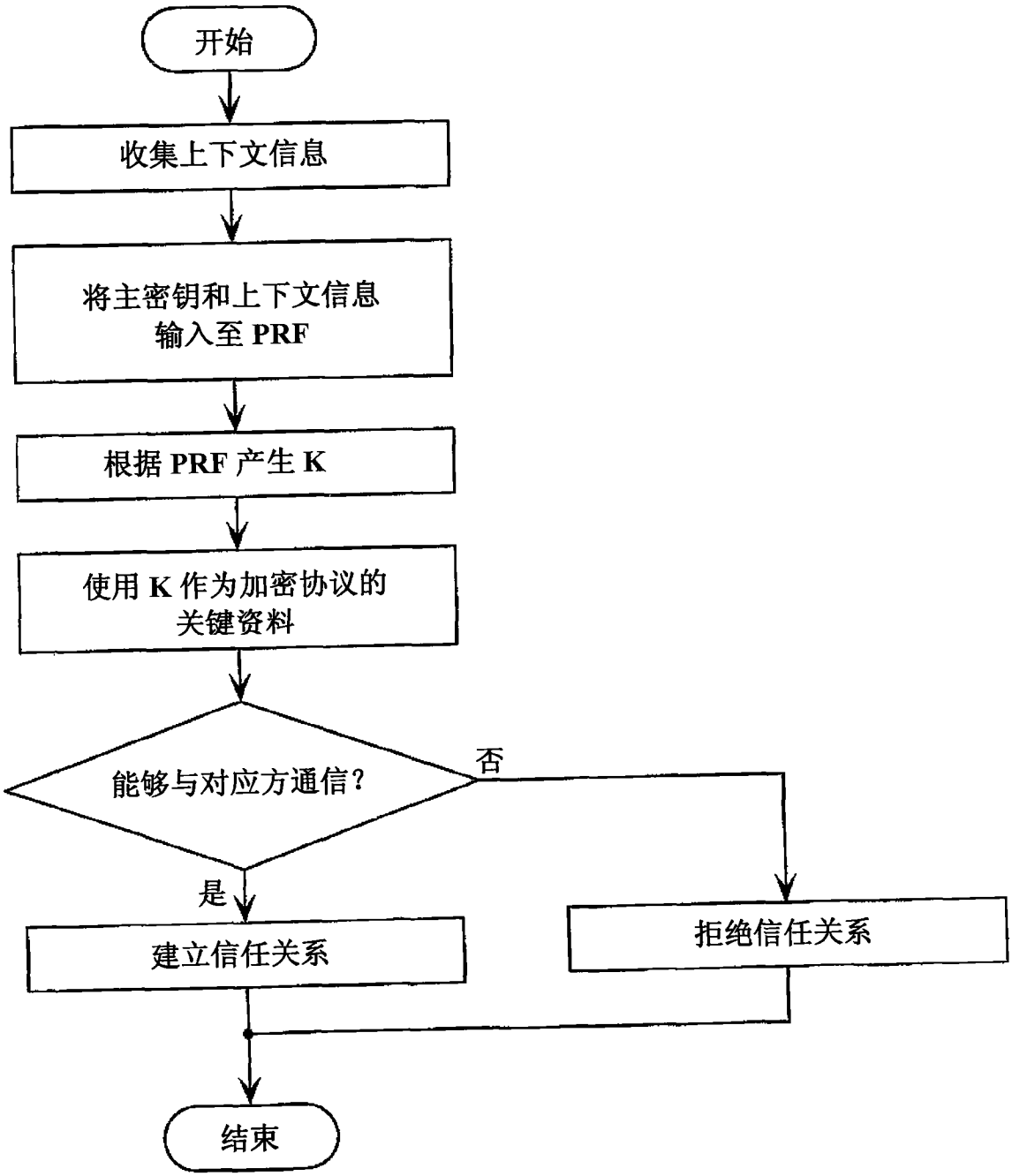

开始
收集上下文信息
将主密钥和上下文信息
输入至 PRF
根据 PRF 产生 K
使用 K 作为加密协议的
关键资料
能够与对应方通信？
否
是
建立信任关系
拒绝信任关系
结束

图 2A

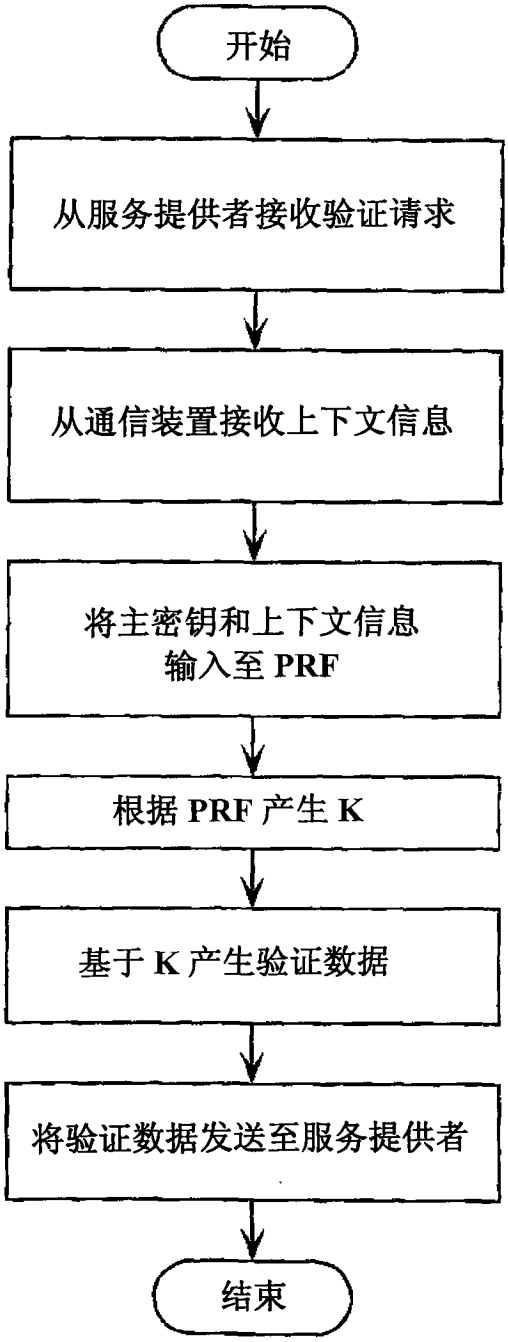

开始
从服务提供者接收验证请求
从通信装置接收上下文信息
将主密钥和上下文信息
输入至 PRF
根据 PRF 产生 K
基于 K 产生验证数据
将验证数据发送至服务提供者
结束

图 2B

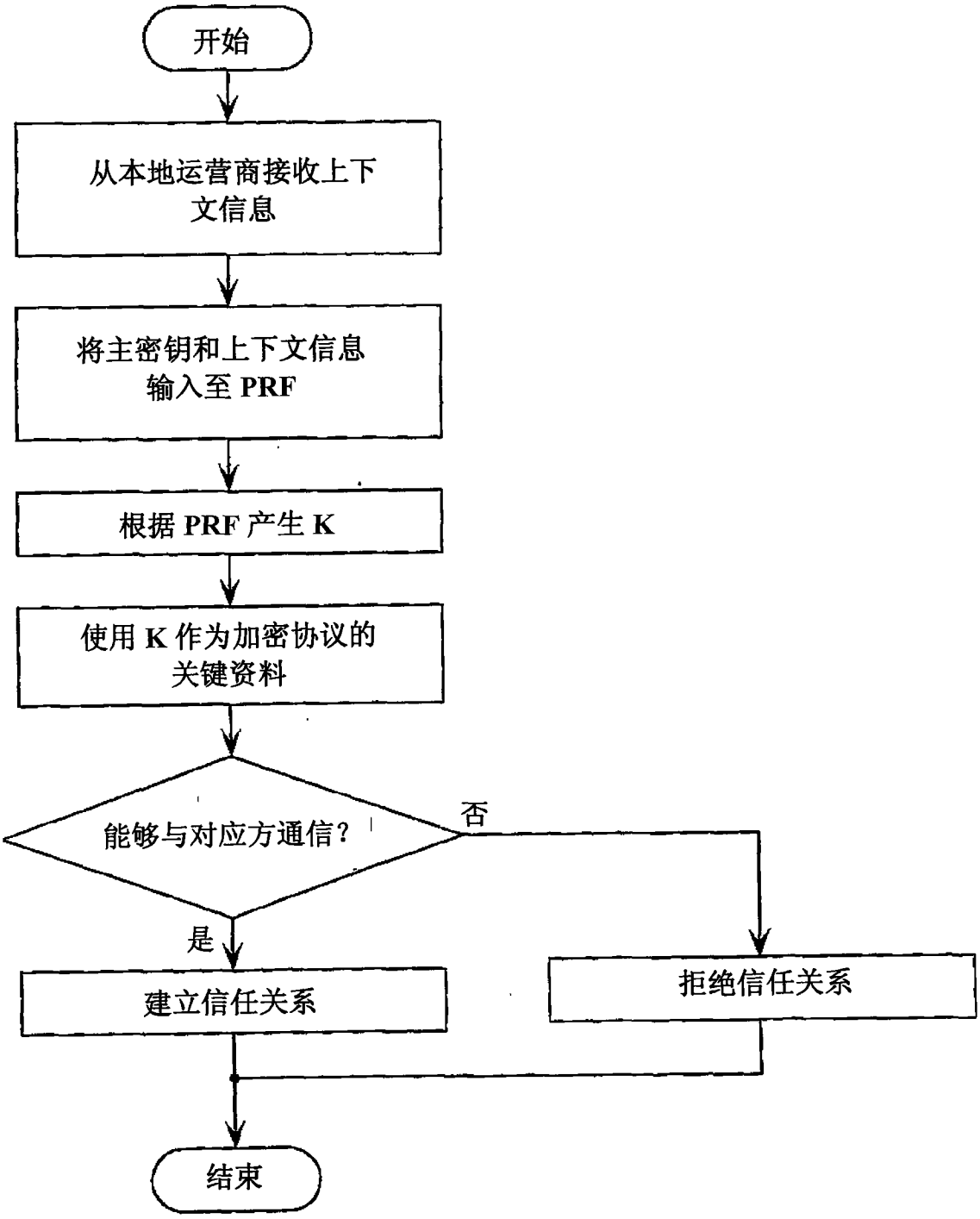

开始
从本地运营商接收上下文信息
将主密钥和上下文信息输入至 PRF
根据 PRF 产生 K
使用 K 作为加密协议的关键资料
能够与对应方通信？
否
是
建立信任关系
拒绝信任关系
结束

图 3A

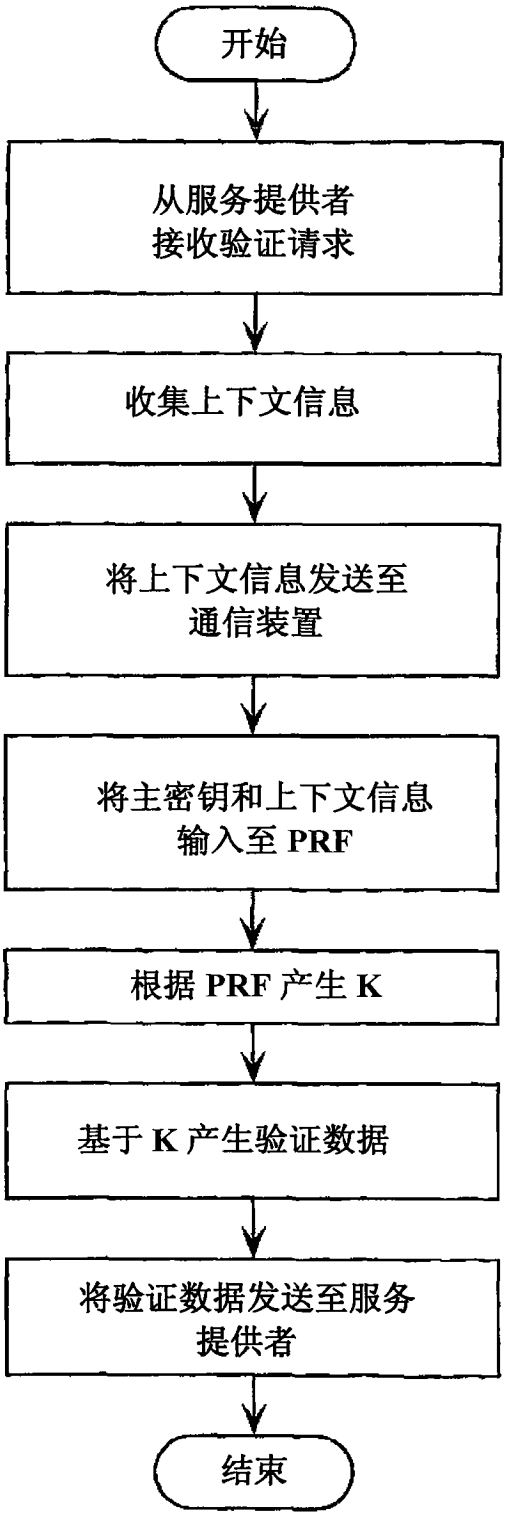

开始
从服务提供者
接收验证请求
收集上下文信息
将上下文信息发送至
通信装置
将主密钥和上下文信息
输入至 PRF
根据 PRF 产生 K
基于 K 产生验证数据
将验证数据发送至服务
提供者
结束

图 3B

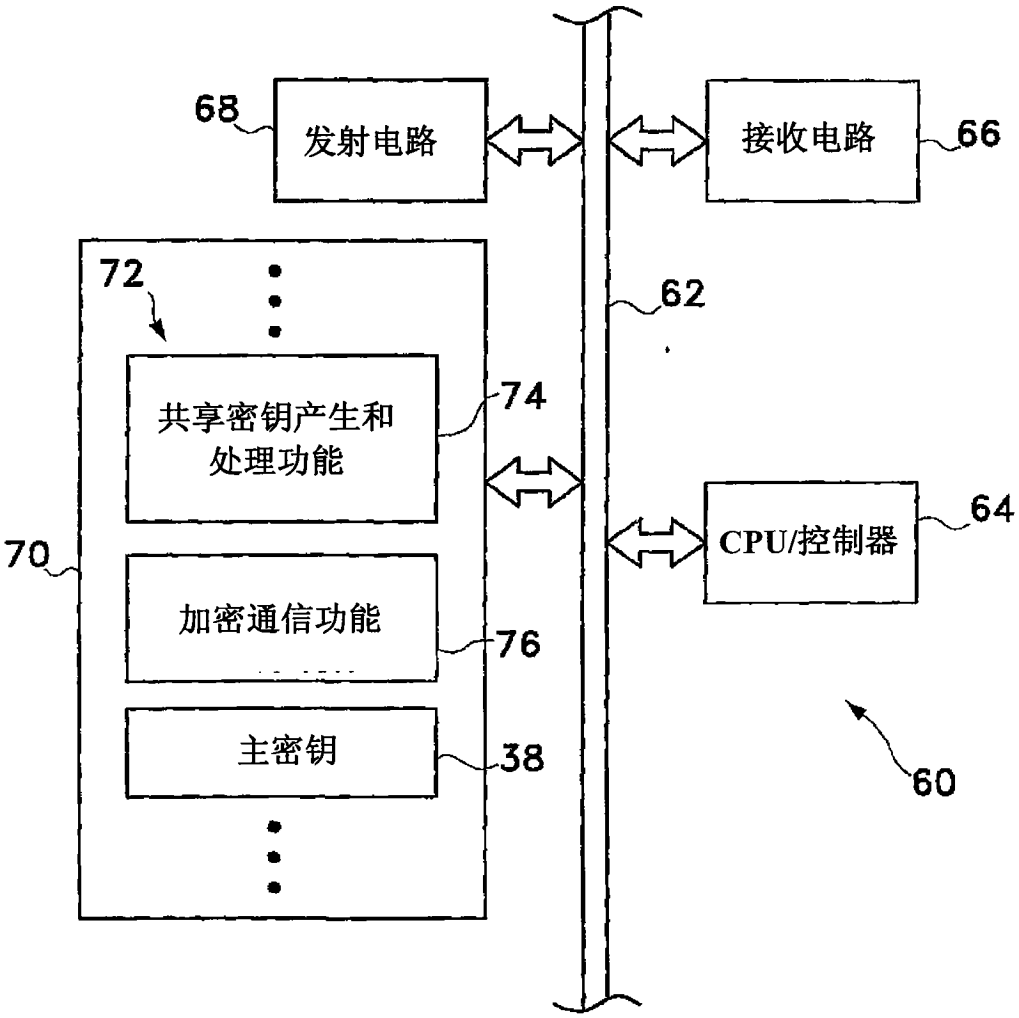

68
发射电路
接收电路
66
72
62
共享密钥产生和
处理功能
74
70
CPU/控制器
64
加密通信功能
76
主密钥
38
60

图 4