[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710188317.2

[43] 公开日 2009 年 5 月 20 日

[11] 公开号 CN 101436930A

[22] 申请日 2007.11.16
[21] 申请号 200710188317.2
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 李春强

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 宋志强 麻海明

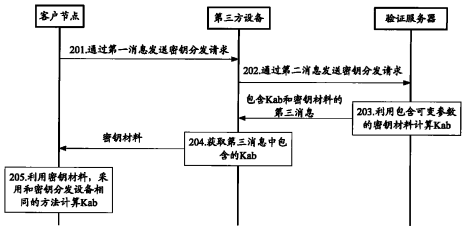
权利要求书 8 页 说明书 23 页 附图 5 页

[54] 发明名称

一种密钥分发的方法、系统和设备

[57] 摘要

本发明实施例提供了密钥分发的方法、系统和设备，通过在计算客户节点和第三方设备之间的共享密钥 Kab 过程中，在密钥材料中引入可变参数来计算 Kab，而不是仅采用固定不变的参数，使得一旦 Kab 泄漏，也能够通过更新该可变参数简单、及时地对 Kab 进行更新，从而提高了消息传输的安全性。 并且，在具体的实现中，采用了对消息进行安全性保护，以及安全性验证的方法，能够有效地防止伪造消息或重放攻击等对消息安全造成的威胁，从而更进一步提高了消息传输的安全性。



1、一种密钥分发的方法，其特征在于，该方法包括:

客户节点向第三方设备发送第一密钥分发请求；所述第三方设备接收到所述第一密钥分发请求后，向验证服务器发送第二密钥分发请求;

所述验证服务器接收到所述第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向所述第三方设备发送包含 Kab 和密钥材料的密钥分发应答;

所述第三方设备接收到所述密钥分发应答后，获取所述 Kab，并将所述密钥材料转发给客户节点；所述客户节点接收到所述密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab。

2、根据权利要求 1 所述的方法，其特征在于，所述第一密钥分发请求和第二密钥分发请求包含所述客户节点标识 IDa 和第三方设备标识 IDb；所述第二密钥分发请求消息还包含所述第一密钥分发请求。

3、根据权利要求 2 所述的方法，其特征在于，所述第一密钥分发请求是利用所述客户节点和验证服务器之间的共享秘密 Kas 进行安全保护的请求消息；和/或，所述第二密钥分发请求是利用所述第三方设备和验证服务器之间的共享秘密 Kbs 进行安全保护的请求消息;

在所述计算 Kab 之前还包括：所述验证服务器利用所述 Kas 对所述第一密钥分发请求进行安全性验证，和/或利用所述 Kbs 对所述第二密钥分发请求进行安全性验证，如果验证成功，则继续执行所述计算 Kab 的步骤。

4、根据权利要求 1 所述的方法，其特征在于，所述密钥分发应答包含两部分，其中第一部分包含所述 Kab、IDa 和 IDb，第二部分包含所述密钥材料;

该方法还包括：所述验证服务器利用第三方设备和验证服务器之间的共享秘密 Kbs 对所述密钥分发应答中的第一部分进行安全保护；所述第三方设备在获取所述 Kab 之前，利用所述 Kbs 对所述第一部分进行安全性验证；和/或，

所述验证服务器利用客户节点和验证服务器之间的共享秘密 Kas 对所述密

钥分发应答中的第二部分进行安全保护；所述客户节点节在计算 Kab 之前，利用所述 Kas 对所述第二部分进行安全性验证。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述进行安全保护包括：生成完整性验证码 MIC；所述进行安全性验证包括：对所述 MIC 进行消息完整性验证；

或者，所述进行安全保护包括：进行加密；所述进行安全性验证包括：进行解密。

6、根据权利要求 2 所述的方法，其特征在于，所述第一密钥分发请求和第二密钥分发请求还包含所述客户节点生成的临时值 Na；

所述验证服务器在计算 Kab 之前还包括：将所述第二密钥分发请求中包含的 Na 与自身存储的 Na 进行比较，如果满足验证条件，则利用所述第二密钥分发请求中包含的 Na 替换自身存储的 Na，继续执行所述 Kab 的步骤，否则，丢弃所述第二密钥分发请求。

7、根据权利要求 1 所述的方法，其特征在于，所述第一密钥分发请求和第二密钥分发请求中包含所述客户节点生成的临时值 Na；和/或，所述第二密钥分发请求中包含所述第三方设备生成的临时值 Nb；和/或，所述验证服务器生成临时值 Ns；

所述可变参数包括所述 Na、Nb 和 Ns 中的一种或任意组合。

8、根据权利要求 6 或 7 所述的方法，其特征在于，所述临时值为随机数或时间戳。

9、根据权利要求 1 所述的方法，其特征在于，该方法还包括：第三方设备获取 Kab 后，利用所述 Kab 生成所述密钥材料的完整性校验码，并将该完整性校验码和密钥材料一起转发给客户节点；

所述客户节点计算出 Kab 后，利用计算出的 Kab 对所述密钥材料的完整性校验码进行校验，如果验证失败，则向所述第三方设备回复失败消息。

10、一种密钥分发的系统，其特征在于，该系统包括：客户节点、第三方设备和验证服务器；

所述客户节点，用于向第三方设备发送第一密钥分发请求，接收到所述第三方设备转发的密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab;

所述第三方设备，用于接收到所述客户节点发送的第一密钥分发请求后，向验证服务器发送第二密钥分发请求，接收到所述验证服务器发送的密钥分发应答后，获取该密钥分发应答中包含的 Kab，将该密钥分发应答中包含的密钥材料转发给所述客户节点;

所述验证服务器，用于接收到所述第三方设备发送的第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向所述第三方设备发送包含所述 Kab 和密钥材料的密钥分发应答。

11、根据权利要求 10 所述的系统，其特征在于，所述客户节点，还用于利用自身和验证服务器之间的共享秘密 Kas 对所述第一密钥分发请求进行安全保护;

所述第三方设备，还用于利用自身和验证服务器之间的共享秘密 Kbs 对所述第二密钥分发请求进行安全保护;

所述验证服务器，还用于利用所述 Kbs 对所述第二密钥分发请求进行安全性验证，利用所述 Kas 对所述第二密钥分发请求中包含的第一密钥分发请求进行安全性验证。

12、根据权利要求 10 所述的系统，其特征在于，所述验证服务器，还用于利用自身和客户节点之间的共享秘密 Kas 对所述密钥分发应答中包含密钥材料的部分进行安全保护，利用自身和第三方设备之间的共享秘密 Kbs 对所述密钥分发应答中包含 Kab 的部分进行安全保护;

所述第三方设备，还用于利用所述 Kbs 对接收到的所述密钥分发应答中包含 Kba 的部分进行安全性验证;

所述客户节点，还用于利用所述 Kas 对接收到的密钥材料进行安全性验证。

13、一种验证服务器，其特征在于，该验证服务器包括：接收单元、计算单元和发送单元;

所述接收单元，用于接收密钥分发请求；

所述计算单元，用于在所述接收单元接收到密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab；

所述发送单元，用于发送包含所述 Kab 和密钥材料的密钥分发请求。

14、根据权利要求 13 所述的验证服务器，其特征在于，所述验证服务器还包括：安全性验证单元，用于对所述接收单元接收到的密钥分发请求进行安全性验证，如果验证通过，则触发所述计算单元执行所述计算 Kab 的操作。

15、根据权利要求 13 所述的验证服务器，其特征在于，所述密钥生成单元还包括：安全保护单元，用于利用客户节点和验证服务器之间的共享秘密 Kas 对所述密钥分发应答中包含密钥材料的部分进行安全保护，利用第三方设备和验证服务器之间的共享秘密 Kbs 对所述密钥分发应答中包含 Kab 的部分进行安全保护。

16、根据权利要求 13 所述的验证服务器，其特征在于，所述计算单元包括：可变参数获取单元和密钥计算单元；

所述可变参数获取单元，用于获取包括客户节点生成的临时值 Na、第三方设备生成的临时值 Nb 和自身所在验证服务器生成的临时值 Ns 中的一个或任意组合的可变参数；

所述密钥计算单元，用于利用包含所述可变参数的密钥材料计算所述 Kab。

17、一种客户节点，其特征在于，该客户节点包括：发送单元、密钥材料接收单元和计算单元；

所述发送单元，用于向第三方设备发送密钥分发请求；

所述密钥材料接收单元，用于接收第三方设备转发的密钥材料；

所述计算单元，用于利用所述密钥材料接收单元接收到的密钥材料，采用和验证服务器相同的方法计算客户节点和第三方设备之间的共享密钥 Kab。

18、根据权利要求 17 所述的客户节点，其特征在于，该客户节点还包括：临时值生成单元，用于生成临时值，并将该临时值携带在所述发送单元发送的密钥分发请求中。

19、根据权利要求 17 所述的客户节点，其特征在于，该客户节点还包括：安全性验证单元，用于利用自身所在客户节点与验证服务器之间的共享秘密 Kas 对所述密钥材料接收单元接收到的密钥材料进行安全性验证，验证通过，则触发所述计算单元执行所述计算 Kab 的操作。

20、根据权利要求 17 所述的客户节点，其特征在于，该客户节点还包括：Kab 确认单元，用于利用所述计算单元计算出的 Kab 验证所述密钥材料的完整性验证码，如果验证通过，则确认所述 Kab 安全；

所述发送单元，还用于在所述 Kab 确认单元验证失败后，向第三方设备发送失败消息。

21、一种密钥分发的方法，其特征在于，该方法包括：

客户节点向第三方设备发送包含密码学参数、根据所述密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息，并对所述第一消息进行安全保护；第三方设备接收到该第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，并对该第二消息进行安全保护；

验证服务器对接收到的第二消息和第二消息中包含的第一消息进行安全性验证，验证通过后，向第三方设备发送包含 PKa 和 PKb 的响应消息，并对该响应消息的内容进行安全性保护；

第三方设备对接收到的响应消息进行安全性验证，验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab；将包含 PKa 或 PKb 的响应消息发送给客户节点；客户节点对接收到的包含 PKa 或 PKb 的响应消息进行安全性验证，验证通过后，按照预设的第二方式，利用 PKa 或 PKb 以及自身私钥 x 计算 Kab；

其中，利用所述第一方式和第二方式计算出的所述 Kab 相同。

22、根据权利要求 21 所述的方法，其特征在于，所述对第一消息进行安全保护和安全性校验是利用客户节点与验证服务器之间的共享秘密 Kas 进行的；

所述对第二消息进行安全保护和安全性校验是利用第三方设备与验证服务

器之间的共享秘密 Kbs 进行的;

所述对响应消息进行安全保护和安全性校验是将所述响应消息分成两部分，分别利用所述 Kas 和 Kbs 进行的。

23、根据权利要求 22 所述的方法，其特征在于，所述安全保护为生成完整性验证码 MIC，所述安全性校验为对所述 MIC 进行完整性验证;

或者，所述安全保护为进行加密，所述安全性校验为进行解密。

24、根据权利要求 21 所述的方法，其特征在于，所述第一消息和第二消息中还包含所述客户节点生成的临时值 Na;

所述验证服务器在发送响应消息之前还包括: 将所述第二消息中包含的 Na 与自身存储的 Na 进行比较，如果满足验证条件，则利用所述第二消息中包含的 Na 替换自身存储的 Na，继续执行所述发送响应消息的步骤，否则，丢弃所述第二消息。

25、根据权利要求 21 所述的方法，其特征在于，所述密码学参数为基于离散对数的 Diffie-Hellman 密钥交换密码学参数，或者，椭圆曲线密码系统参数。

26、根据权利要求 24 所述的方法，其特征在于，所述临时值为随机数或时间戳。

27、一种密钥分发的系统，其特征在于，该系统包括: 客户节点、第三方设备和验证服务器;

所述客户节点，用于向所述第三方设备发送包含密码学参数、根据所述密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息，并对所述第一消息进行安全保护; 对所述第三方设备发送的包含 PKa 或 PKb 的响应消息进行安全性验证，验证通过后，按照预设的第二方式，利用 PKa 或 PKb 以及自身私钥 x 计算 Kab;

所述第三方设备，用于接收到所述第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，并对该第二消息进行安全保护; 对所述验证服务器发送的响应消息进行安全性验证，验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私

钥 y 计算客户节点和第三方设备的共享密钥 Kab，将包含 PKa 或 PKb 的响应消息发送给客户节点；

所述验证服务器，用于对接收到的第二消息和第二消息中包含的第一消息进行安全性验证，验证通过后，向所述第三方设备发送包含 PKa 和 PKb 的响应消息，并对该响应消息的内容进行安全性保护。

28、一种验证服务器，其特征在于，该验证服务器包括：接收单元、安全性验证单元、发送单元和安全保护单元；

所述接收单元，用于接收第三方设备发送的包含客户节点公钥 PKa 和第三方设备公钥 PKb 的第二消息；

所述安全性验证单元，用于对所述接收单元接收到的第二消息和第二消息中包含的第一消息进行安全性验证；

所述发送单元，用于在所述安全性验证单元验证通过后，向第三方设备发送包含客户节点公钥 PKa 和第三方设备公钥 PKb 的响应消息；

所述安全保护单元，用于对所述发送单元发送的响应消息进行安全保护。

29、根据权利要求 28 所述的验证服务器，其特征在于，该验证服务器还包括：比较单元和 Na 存储单元；

所述比较单元，用于将所述接收单元接收到的第二消息中包含的临时值 Na 与所述 Na 存储单元存储的 Na 值进行比较，如果满足验证条件，则触发所述发送单元执行所述发送响应消息的操作，如果不满足验证条件，则禁止所述发送单元执行所述发送响应消息的操作；

所述 Na 存储单元，用于在所述比较单元的比较结果为满足验证条件时，存储所述第二消息中包含的 Na。

30、一种第三方设备，其特征在于，该第三方设备包括：接收单元、发送单元、安全保护单元、安全性验证单元和计算单元；

所述接收单元，用于接收客户节点发送的第一消息，接收验证服务器发送的响应消息；

所述发送单元，用于在所述接收单元接收到第一消息后，向验证服务器发

送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，在所述安全性验证单元验证通过后，将包含客户节点公钥 PKa 和 PKb 的响应消息发送给客户节点；

所述安全保护单元，用于对所述发送单元发送的第二消息进行安全保护；

所述安全性验证单元，对所述接收单元接收的响应消息进行安全性验证；

所述计算单元，用于在所述安全性验证单元验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab。

31、根据权利要求 30 所述的第三方设备，其特征在于，该第三方设备还包括：公钥生成单元，用于利用所述第一消息中包含的密码学参数、以及自身私钥 y 生成第三方设备公钥 PKb。

32、一种客户节点，其特征在于，该客户节点包括：发送单元、安全保护单元、接收单元、安全性验证单元、和计算单元；

所述发送单元，用于向第三方设备发送包含密码学参数、以及根据该密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息；

所述安全保护单元，用于对所述发送单元发送的第一消息进行安全保护；

所述接收单元，用于接收第三方设备发送的包含 PKa 或 PKb 的响应消息；

所述安全性验证单元，用于对所述接收单元接收到的响应消息进行安全性验证；

所述计算单元，用于在所述安全性验证单元验证通过后，按照预设的第二方式，利用所述 PKa 或 PKb 以及自身私钥 x 计算客户节点和第三方设备的共享密钥 Kab。

33、根据权利要求 32 所述的客户节点，其特征在于，该客户节点还包括：密码学参数生成单元和公钥生成单元；

所述密码学参数生成单元，用于生成密码学参数；

所述公钥生成单元，用于根据所述密码学参数生成单元生成的密码学参数计算和自身私钥 x 生成客户节点公钥 PKa。

一种密钥分发的方法、系统和设备

技术领域

本发明涉及网络安全技术，特别涉及一种密钥分发的方法、系统和设备。

背景技术

随着网络安全技术的不断发展，对网络的安全保护技术要求也越来越高，密码学是网络与信息安全的核心技术，现代密码学的安全是建立在密钥的保护而不是算法保密的基础上的，因此密钥的保护管理成了信息保密的关键。密钥的管理包含密钥的生成、存储、分发等，而密钥的分发是密钥管理的一个关键问题。在基于对称密码系统中，为了解决密钥的分发问题，通常存在密钥分发服务器，系统中待通信的双方都与密钥分发服务器存在共享秘密，通过一定的消息交换建立一个用于保护双方通信的共享密钥。

在实际应用的过程中，通常会遇到如下情况：客户节点与验证服务器之间存在一个或多个共享秘密 Kas，第三方设备与验证服务器之间存在一个或多个共享秘密 Kbs，然而在客户节点和第三方设备之间需要进行消息交互时，为了对该客户节点和第三方设备之间消息的交互进行安全保护，则需要在客户节点和第三方设备之间存在共享密钥 Kab。这就需要验证服务器生成客户节点和第三方设备之间的共享密钥 Kab，并将该 Kab 分发给客户节点和第三方设备，使得客户节点和第三方设备能够获取该 Kab。例如图 1 所示的网络架构中，作为验证服务器的家乡 EAP 服务器，需要生成 EAP 客户节点和本地认证服务器之间的共享密钥。

现有技术中，密钥分发的过程主要为：客户节点向第三方设备发送客户节点标识 IDa 和第三方设备标识 IDb 的密钥分发请求；第三方设备接收到该密钥分发请求后，向验证服务器发送包含客户节点标识 IDa 和第三方设备标

识 IDb 的密钥分发请求；验证服务器收到第三方设备发送的密钥分发请求后，利用客户节点和验证服务器之间的共享密钥 Kas、与 Kab 用途相关的字符串 Label、客户节点标识 IDa、第三方设备标识 IDb 以及密钥长度等密钥生成材料生成共享密钥 Kab，并将该生成的 Kab、IDa、IDb、Kab 生存期等利用 Kbs 进行加密后形成的部分和将生成的 Kab、IDa、IDb、Kab 生存期等利用 Kas 生成 MIC 的部分发送给第三方设备；第三方设备利用 Kbs 对加密的部分进行解密，从而获取 Kab，并将利用 Kas 进行完整性保护的部分转发给客户节点；客户节点利用 Kas 对第三方设备转发来的部分信息进行完整性验证，验证通过后获取到 Kab。

然而，在现有技术的方法中，由于验证服务器生成的共享密钥 Kab 所使用的密钥材料均是固定不变的参数，当在 Kab 的生存期内，一旦该 Kab 泄漏，则无法对该 Kab 进行变更，这必然降低了密钥分发的安全性。

发明内容

本发明实施例提供了一种密钥分发的方法、系统和设备，以便于提高密钥分发的安全性。

一种密钥分发的方法，该方法包括:

客户节点向第三方设备发送第一密钥分发请求；所述第三方设备接收到所述第一密钥分发请求后，向验证服务器发送第二密钥分发请求；

所述验证服务器接收到所述第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向所述第三方设备发送包含 Kab 和密钥材料的密钥分发应答；

所述第三方设备接收到所述密钥分发应答后，获取所述 Kab，并将所述密钥材料转发给客户节点；所述客户节点接收到所述密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab。

一种密钥分发的系统，该系统包括：客户节点、第三方设备和验证服务器；

所述客户节点，用于向第三方设备发送第一密钥分发请求，接收到所述第

三方设备转发的密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab;

所述第三方设备，用于接收到所述客户节点发送的第一密钥分发请求后，向验证服务器发送第二密钥分发请求，接收到所述验证服务器发送的密钥分发应答后，获取该密钥分发应答中包含的 Kab，将该密钥分发应答中包含的密钥材料转发给所述客户节点;

所述验证服务器，用于接收到所述第三方设备发送的第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向所述第三方设备发送包含所述 Kab 和密钥材料的密钥分发应答。

一种验证服务器，该验证服务器包括：接收单元、计算单元和发送单元;

所述接收单元，用于接收密钥分发请求;

所述计算单元，用于在所述接收单元接收到密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab;

所述发送单元，用于发送包含所述 Kab 和密钥材料的密钥分发请求。

一种客户节点，该客户节点包括：发送单元、密钥材料接收单元和计算单元;

所述发送单元，用于向第三方设备发送密钥分发请求;

所述密钥材料接收单元，用于接收第三方设备转发的密钥材料;

所述计算单元，用于利用所述密钥材料接收单元接收到的密钥材料，采用和验证服务器相同的方法计算客户节点和第三方设备之间的共享密钥 Kab。

一种密钥分发的方法，该方法包括:

客户节点向第三方设备发送包含密码学参数、根据所述密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息，并对所述第一消息进行安全保护;第三方设备接收到该第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，并对该第二消息进行安全保护;

验证服务器对接收到的第二消息和第二消息中包含的第一消息进行安全性

验证，验证通过后，向第三方设备发送包含 PKa 和 PKb 的响应消息，并对该响应消息的内容进行安全性保护；

第三方设备对接收到的响应消息进行安全性验证，验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab；将包含 PKa 或 PKb 的响应消息发送给客户节点；客户节点对接收到的包含 PKa 或 PKb 的响应消息进行安全性验证，验证通过后，按照预设的第二方式，利用 PKa 或 PKb 以及自身私钥 x 计算 Kab；

其中，利用所述第一方式和第二方式计算出的所述 Kab 相同。

一种密钥分发的系统，该系统包括：客户节点、第三方设备和验证服务器；

所述客户节点，用于向所述第三方设备发送包含密码学参数、根据所述密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息，并对所述第一消息进行安全保护；对所述第三方设备发送的包含 PKa 或 PKb 的响应消息进行安全性验证，验证通过后，按照预设的第二方式，利用 PKa 或 PKb 以及自身私钥 x 计算 Kab；

所述第三方设备，用于接收到所述第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，并对该第二消息进行安全保护；对所述验证服务器发送的响应消息进行安全性验证，验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab，将包含 PKa 或 PKb 的响应消息发送给客户节点；

所述验证服务器，用于对接收到的第二消息和第二消息中包含的第一消息进行安全性验证，验证通过后，向所述第三方设备发送包含 PKa 和 PKb 的响应消息，并对该响应消息的内容进行安全性保护。

一种验证服务器，该验证服务器包括：接收单元、安全性验证单元、发送单元和安全保护单元；

所述接收单元，用于接收第三方设备发送的包含客户节点公钥 PKa 和第三方设备公钥 PKb 的第二消息；

所述安全性验证单元，用于对所述接收单元接收到的第二消息和第二消息中包含的第一消息进行安全性验证；

所述发送单元，用于在所述安全性验证单元验证通过后，向第三方设备发送包含客户节点公钥 PKa 和第三方设备公钥 PKb 的响应消息；

所述安全保护单元，用于对所述发送单元发送的响应消息进行安全保护。

一种第三方设备，该第三方设备包括：接收单元、发送单元、安全保护单元、安全性验证单元和计算单元；

所述接收单元，用于接收客户节点发送的第一消息，接收验证服务器发送的响应消息；

所述发送单元，用于在所述接收单元接收到第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，在所述安全性验证单元验证通过后，将包含客户节点公钥 PKa 和 PKb 的响应消息发送给客户节点；

所述安全保护单元，用于对所述发送单元发送的第二消息进行安全保护；

所述安全性验证单元，对所述接收单元接收的响应消息进行安全性验证；

所述计算单元，用于在所述安全性验证单元验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab。

一种客户节点，该客户节点包括：发送单元、安全保护单元、接收单元、安全性验证单元、和计算单元；

所述发送单元，用于向第三方设备发送包含密码学参数、以及根据该密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息；

所述安全保护单元，用于对所述发送单元发送的第一消息进行安全保护；

所述接收单元，用于接收第三方设备发送的包含 PKa 或 PKb 的响应消息；

所述安全性验证单元，用于对所述接收单元接收到的响应消息进行安全性验证；

所述计算单元，用于在所述安全性验证单元验证通过后，按照预设的第二

方式，利用所述 PKa 或 PKb 以及自身私钥 x 计算客户节点和第三方设备的共享密钥 Kab。

由以上技术方案可以看出，在本发明实施例提供的第一种方法、系统和设备中，客户节点向第三方设备发送第一密钥分发请求；第三方设备接收到所述第一密钥分发请求后，向验证服务器发送第二密钥分发请求；验证服务器接收到第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向第三方设备发送包含 Kab 和密钥材料的密钥分发应答；第三方设备接收到该密钥分发应答后，获取该 Kab，并将生成 Kab 的密钥材料转发给客户节点；客户节点接收到该密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab。通过这种方式，验证服务器将可变参数引入密钥材料来计算 Kab，而不是全部采用固定不变的参数，使得一旦 Kab 泄漏，也能够利用该可变参数及时对 Kab 进行更新，从而提高了消息传输的安全性；并且，验证服务器将密钥材料提供给客户节点，使得客户节点能够通过相同的密钥计算方法，采用该密钥材料计算 Kab，这更进一步提高了消息传输的安全性。

在本发明实施例提供的第二种方法、系统和设备中，客户节点和第三方设备根据相同的密码学参数和自身的私钥生成各自的公钥，并将该公钥发送给验证服务器进行安全性验证，验证通过后，客户节点和第三方设备按照预先设定的方式，利用验证服务器回复的响应中包含的客户节点的公钥或第三方节点的公钥，以及自身的私钥生成相同的共享密钥 Kab。该方法通过在计算 Kab 的过程中引入可变的私钥，而不是全部采用固定不变的参数，使得一旦 Kab 泄漏，能够利用该可变的私钥及时对 Kab 进行更新，从而提高了消息传输的安全性。

附图说明

图 1 为现有技术中的一种网络结构图；

图 2 为本发明实施例提供的第一种主要方法流程图；

图 3 为本发明实施例提供的第一种具体方法流程图；

图 4 为本发明实施例提供的第一种系统结构图；

图 5 为本发明实施例提供的验证服务器结构图；

图 6 为本发明实施例提供的第一种客户节点结构图；

图 7 为本发明实施例提供的第二种主要方法流程图；

图 8 为本发明实施例提供的第二种系统结构图；

图 9 为本发明实施例提供的验证服务器的结构图；

图 10 为本发明实施例提供的第三方设备结构图；

图 11 为本发明实施例提供的第二种客户节点结构图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

图 2 为本发明实施例提供的第一种主要方法流程图，该方法中，客户节点与验证服务器之间的共享秘密，记为 Kas，第三方设备与验证服务器之间的共享秘密，记为 Kbs，验证服务器需要为客户节点和第三方设备分发客户节点和第三方设备之间的共享密钥 Kab。其中，Kas 可以是一个或多个共享口令、共享密钥、也可以是由共享密钥派生出的其它共享秘密。如图 2 所示，该方法可以包括以下步骤：

步骤 201：客户节点通过第一消息向第三方设备发送密钥分发请求。

该第一消息可以包含客户节点标识 IDa 和第三方设备标识 IDb，还可以包含客户节点生成的临时值 Na 等信息。

并且该消息可以受客户节点与密钥分发服务器间的共享秘密的安全保护。客户节点可以利用自身与验证服务器之间的共享秘密 Kas 生成该第一消息的完整性验证码，记为 MIC 1，也可以采用该 Kas 对该第一消息进行加密。其中临时值 Na 可以是随机数、序列号或时间戳等信息。

步骤 202：第三方设备接收到客户节点发送的密钥分发请求后，通过第

二消息向验证服务器发送密钥分发请求。

该第二消息可以包含用户标识 IDa 和第三方设备标识 IDb，以及第一消息，还可以包含第三方设备生成的临时值 Nb。其中临时值 Nb 可以是随机数、或时间戳。

本步骤中，第三方设备还可以利用自身与验证服务器之间的共享密钥 Kbs 生成该第二消息的完整性验证码，记为 MIC 2，同样也可以对该第二消息进行加密。

步骤 203：验证服务器利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，并通过包含 Kab 和密钥材料的第三消息向第三方设备发送密钥分发应答。

验证服务器收到第三方设备发送的第二消息，利用自身与第三方设备之间的共享密钥 Kbs 对 MIC 2 进行消息完整性验证，利用自身与客户节点之间的共享密钥 Kas 对 MIC 1 进行消息完整性验证，如果验证都通过，生成 Kab；如果其中任意一个验证不通过，则向第三方设备回复验证失败消息。如果客户节点和第三方设备分别对第一消息和第二消息进行加密，则验证服务器首先对该第一消息和第二消息进行解密，还可以对户节点和第三方设备的身份标识进行验证，如果解密成功且身份验证通过，则生成包含 Kab 和密钥材料的密钥分发应答消息发送给第三方设备。。

本步骤中，验证服务器在生成 Kab 时，可以将客户节点生成的 Na、第三方设备生成的 Nb 或验证服务器自身生成的临时值 Ns 中的一个或任意组合作为密钥材料中的可变参数，生成 Kab。即 Kab 可以采用如下方法进行计算：Kab = KDF（Kas，Label | IDa | IDb | Na），或者，

Kab = KDF（Kas，Label | IDa | IDb | Nb），或者，

Kab = KDF（Kas，Label | IDa | IDb | Ns），或者，

Kab = KDF（Kas，Label | IDa | IDb | Na | Nb），或者，

Kab = KDF（Kas，Label | IDa | IDb | Na | Ns），或者，

Kab = KDF（Kas，Label | IDa | IDb | Nb | Ns），或者，

Kab = KDF（Kas，Label | IDa | IDb | Na | Nb | Ns）。其中，KDF 为生成密钥的函数，Label 为一个预先设定的与 Kab 用途相关的字符串，| 为连接符。

另外，还可以将 Kab 生存期 K_Lifetime、Kab 长度 K_Length 等也作为密钥材料生成 Kab，例如：Kab = KDF（Kas，Label | IDa | IDb | K_Lifetime | K_Length | Na）等。

在发送给第三方设备的第三消息中，生成 Kab 的密钥材料可以包含在第三消息的第一部分信息中，该第一部分信息中还可以包含 Na 值，该第一部分信息可以使用验证服务器与客户节点之间的共享密钥 Kas 生成 MIC 3，或者可以使用 Kas 进行加密。Kab 可以包含在第三消息的第二部分信息中，如果在步骤 202 中，第三方设备生成的临时值 Nb，则该第二部分信息中还可以包含 Nb 或 Nb 经过一定运算生成的值，比如 Nb+1。可以使用验证服务器与第三方设备之间的共享密钥 Kbs 生成整个消息的完整性验证码，记为 MIC 4；或者，可以使用 Kbs 对整个第三消息进行加密。

步骤 204：第三方设备接收到验证服务器发送的第三消息后，获取其中包含的 Kab，并将生成 Kab 的密钥材料转发给客户节点。

本步骤中，该包含密钥材料的部分记为 Key_Auth_Msg，该 Key_Auth_Msg 可以是验证服务器利用 Kas 进行安全保护的消息。

本步骤中，第三方设备可以首先对该第三消息中采用 Kbs 进行加密的部分进行解密，或者，首先对该第三消息中的 MIC 4 进行完整性验证，验证通过后，获取 Kab，并将包含密钥材料的 Key_Auth_Msg 转发给客户节点。转发给客户节点的消息还可以携带第三方设备使用 Kab 生成的消息验证码 MIC5，可以是以 Key_Auth_Msg 为输入生成的完整性验证码，也可以是对 Key_Auth_Msg 中的一部分生成完整性验证码，比如 Na、IDa、IDb、MIC3 中的一个或其任意组合，将该完整性验证码记为 MIC 5。

步骤 205：客户节点接收到第三方设备转发的生成 Kab 的密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算自身和第三方设备之间

的共享密钥 Kab。

本步骤中，在该步骤中，可以预先在客户节点中设置与验证服务器相同的密钥计算方法。

客户节点接收到该密钥材料后，如果验证服务器对该部分进行了完整性保护，则客户节点首先利用密钥分发服务器与客户节点间的共享秘密 Kas 对该密钥材料的 MIC 3 进行完整性验证，如果验证通过，则利用该密钥材料计算 Kab；如果验证服务器对该部分进行了加密，则客户节点首先利用密钥分发服务器与客户节点间的共享秘密 Kas 对该密钥材料进行解密，然后利用该密钥材料计算 Kab。

上述临时值 Na、Nb 和 Ns 可以是一个随机数，序列号、或一个时间戳。

另外，在上述方法中，验证服务器还可以每次保存客户节点或第三方设备发送的临时值 Na 或 Nb，接收到第三方设备发送的第二消息后，提取消息中的 IDa，如果首次接收到该客户节点的消息，则 MIC 1，如果验证通过，则存储该 Na，如果不是首次接收到该客户节点的消息，则可以将其中包含的 Na 与自身存储的上一次该用户设备发送的 Na 值进行比较，如果满足验证条件，则执行计算 Kab 的步骤。这样可以进一步地增强消息发送过程中的安全性。其中，如果临时值是每次递增的序列号，则验证服务器判断如果接收到的 Na 值比自身存储的 Na 值大，则满足验证条件，可以继续计算 Kab，否则，拒绝计算 Kab。另外，第三方设备同样也可以保存客户节点发送的 Na 值，在接收到第一消息或第三消息时，同样可以根据接收到的 Na 值和自身存储的 Na 值进行上述安全验证。另外，客户节点也可以保存自身生成的 Na 值，在接收到第四消息时，可以首先将密钥材料中包含的 Na 值与自身存储的 Na 值进行比较，如果相同，则验证成功。

下面具几个具体的实施例对上述方法进行描述。图 3 为本发明实施例提供的第一个具体方法流程图，该方法中，进行通信的三方分别为 EAP 客户节点、本地认证服务器和家乡 EAP 服务器，分别对应客户节点、第三方设备和验证服务器。EAP 客户节点与家乡 EAP 服务器已通过认证，并生成了

共享秘密，即扩展主会话密钥 (EMSK，Extended Master Session Key)以及通过 EMSK 派生出的保护消息完整性的共享密钥 KI_as；当 EAP 客户节点离开家乡域时，为了减小切换认证时延，需要家乡 EAP 服务器为 EAP 客户节点和本地认证服务器分发一个共享密钥 Kab，使得 EAP 客户节点在访问地进行重认证时，可以使用该共享密钥 Kab 向本地认证服务器进行认证。如图 3 所示，该方法具体包括以下步骤：

步骤 301：EAP 客户节点通过第一消息向本地认证服务器发送密钥分发请求。该第一消息包含 EAP 客户节点标识 IDa、本地认证服务器标识 IDb、以及 EAP 客户节点生成的临时值 Na，并通过 EAP 客户节点和家乡 EAP 服务器之间的共享秘密 KI_as 生成该第一消息的完整性验证码，记为 MIC 1。

步骤 302：本地认证服务器接收到该第一消息后，存储 Na 值，通过第二消息向家乡 EAP 服务器发送密钥分发请求。该第二消息中包含 EAP 客户节点标识 IDa、本地认证服务器标识 IDb、本地认证服务器生成的临时值 Nb、以及第一消息，并通过本地认证服务器与家乡 EAP 服务器之间的共享秘密 Kbs 生成该第二消息的完整性验证码；或者利用 Kbs 生成 Nb、IDa、IDb、以及 MIC 1 生成完整性验证码，记为 MIC 2。

步骤 303：家乡 EAP 服务器接收到该第二消息后，对该第二消息中的 MIC 1 和 MIC 2 进行完整性验证，如果验证成功，则将 Label、IDa、IDb 以及可变参数 Na、Nb 作为密钥材料，并使用 EMSK 生成 EAP 客户节点和本地认证服务器之间的共享密钥 Kab。即：Kab = KDF（EMSK，Label | IDa | IDb | Na | Nb）。并向本地认证服务器发送第三消息，该第三消息中包含两部分，其中一部分包含 Kab 以及 IDa、IDb 和 Na、Nb，并通过 Kbs 对该包含 Kab 的部分进行加密，另一部分包含 Kas、Label、IDa、IDb、Na，并通过客户节点与家乡服务器之间的共享秘密 KI_as 生成该包含密钥材料的部分的完整性验证码，记为 MIC 3。

或者该第三消息包含使用 Kbs 加密的 kab，还包含 Na、Nb、IDa、IDb 及给客户节点的包含密钥材料的密钥验证授权消息 Key_Auth_Msg，该第三

消息作为服务器对第一消息的响应包含了生成 Kab 的密钥材料、生存期，及使用 KI_as 生成的完整性验证码等信息，并使用 Kbs 对整个消息生成完整性验证码。

或者该第三消息包含 kab,及给客户节点的包含密钥材料的密钥验证授权信息 Key_Auth_Msg，Key_Auth_Msg 作为服务器对第一消息的响应包含了生成 Kab 的密钥材料及生存期，使用 KI_as 生成的完整性验证码等信息，并使用 Kbs 对整个消息加密。

步骤 304：本地认证服务器接收到该第三消息后，利用 Kbs 进行解密，判断该第三消息中包含的 Na、Nb 是否与自身存储的 Na、Nb 相同，如果不相同，则验证失败，向密钥分发服务器及客户节点发送失败消息；如果相同，则验证成功，将包含密钥材料的部分通过第四消息转发给 EAP 客户节点，另外，本地认证服务器还可以利用 Kab 生成该第四消息的完整性验证码，记为 MIC4，或使用 Kab 进行加密的 Na、IDa、IDb 等信息。

更优地，该第三消息中，也可以包含经过特殊处理后的 Na，例如，Na + 1；本地认证服务器对该经过特殊处理后的 Na 进行逆处理，即 Na + 1 - 1，将逆处理后的结果与自身存储的 Na 进行比较，如果相同，则验证成功。这样可以进一步保证消息的安全性。

步骤 305：EAP 客户节点接收到第四消息后，利用 KI_as 对包含密钥材料的部分的 MIC 3 进行完整性验证，且将密钥材料中包含的 Na 值与自身存储的 Na 值进行比较，如果都验证成功，利用该密钥材料，采用和家乡 EAP 服务器相同的方法计算 EAP 客户节点和第三方设备之间的共享密钥 Kab，并使用 Kab 验证 MIC4。

同样地，在包含 Kab 的部分中，也可以包含经过特殊处理后的 Na，例如，Na + 1；该 EAP 客户节点也可以将经过特殊处理后的 Na 进行逆处理，将逆处理后的结果与自身存储的 Na 进行比较，如果相同，则验证成功。

图 4 为本发明实施例提供的第一种系统结构图，如图 4 所示，该系统包括：客户节点 401、第三方设备 402 和验证服务器 403；

客户节点 401，用于通过第一消息向第三方设备发送密钥分发请求，接收到第三方设备 402 转发的密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab。

第三方设备 402，用于接收到客户节点 401 发送的第一消息后，通过第二消息向验证服务器 403 发送密钥分发请求，接收到验证服务器 403 发送的密钥分发应答后，获取该密钥分发应答中包含的 Kab，将该密钥分发应答中包含的密钥材料转发给客户节点 401。

验证服务器 403，用于接收到第三方设备 402 发送的第二消息后，利用包含可变参数的密钥材料计算客户节点 401 和第三方设备 402 之间的共享密钥 Kab，向第三方设备 402 发送包含 Kab 和密钥材料的密钥分发应答。

另外，客户节点 401，还可以用于利用自身和验证服务器之间的共享秘密 Kas 对第一消息进行安全保护。

第三方设备 402，还可以用于利用自身和验证服务器 403 之间的共享秘密 Kbs 对第二消息进行安全保护。

验证服务器 403，还可以用于利用 Kbs 对第二消息进行安全性验证，利用 Kas 对第二消息中包含的第一消息进行安全性验证。

验证服务器 403，还可以用于利用自身和客户节点 401 之间的共享秘密 Kas 对密钥分发应答中包含密钥材料的部分进行安全保护，利用自身和第三方设备 402 之间的共享秘密 Kbs 对密钥分发应答中包含 Kab 的部分进行安全保护。

第三方设备 402，还可以用于利用 Kbs 对接收到的密钥分发应答中包含 Kba 的部分进行安全性验证。

客户节点 401，还可以用于利用 Kas 对接收到的密钥材料进行安全性验证。

另外，第三方设备 402，还用于利用获取的 Kab 对所述包含密钥材料的部分生成完整性校验码，记为 MIC 5;

客户节点 401，还用于在计算出 Kab 后，利用该 Kab 对该 MIC 5 进行完整性校验，如果校验失败，则向第三方设备 402 发送失败消息，如果校验通过，则确认该计算出的 Kab 安全。

图 5 为本发明实施例提供的第一种验证服务器的结构图，如图 5 所示，该验证服务器包括：接收单元 501、计算单元 502 和发送单元 503。

接收单元 501，用于接收密钥分发请求。

计算单元 502，用于在接收单元 501 接收到密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab。

发送单元 503，用于发送包含 Kab 和密钥材料的密钥分发请求。

验证服务器还可以包括：安全性验证单元 504，用于对接收单元 501 接收到的密钥分发请求进行安全性验证，如果验证通过，则触发计算单元 502 执行计算 Kab 的操作。

密钥生成单元还可以包括：比较单元 505 和 Na 存储单元 506。

比较单元 505，用于将接收单元 501 接收到的密钥分发请求中包含的 Na 值与 Na 存储单元 506 存储的 Na 值进行比较，如果满足验证条件，则触发计算单元 502 执行计算 Kab 的操作。

Na 存储单元 506，用于在比较单元 505 比较的结果为满足验证条件时，存储密钥分发请求中包含的 Na 值。

更优地，密钥生成单元还可以包括：安全保护单元 507，用于利用客户节点和验证服务器之间的共享秘密 Kas 对密钥分发应答中包含密钥材料的部分进行安全保护，利用第三方设备和验证服务器之间的共享秘密 Kbs 对密钥分发应答中包含 Kab 的部分进行安全保护。

其中，计算单元 502 可以包括：可变参数获取单元 5021 和密钥计算单元 5022。

可变参数获取单元 5021，用于获取包括客户节点生成的临时值 Na、第三方设备生成的临时值 Nb 和自身所在验证服务器生成的临时值 Ns 中的一个或任意组合的可变参数。

密钥计算单元 5022，用于利用包含可变参数的密钥材料计算 Kab。

图 6 为本发明实施例提供的第一种客户节点的结构图，如图 6 所示，该客户节点可以包括：发送单元 601、密钥材料接收单元 602 和计算单元 603。

发送单元601，用于向第三方设备发送密钥分发请求。

密钥材料接收单元602，用于接收第三方设备转发的密钥材料。

计算单元603，用于利用密钥材料接收单元602接收到的密钥材料，采用和验证服务器相同的方法计算客户节点和第三方设备之间的共享密钥Kab。

另外，该客户节点还可以包括：临时值生成单元604，用于生成临时值，并将该临时值携带在发送单元601发送的密钥分发请求中。

更优地，该客户节点还可以包括：安全性验证单元605，用于利用自身所在客户节点与验证服务器之间的共享秘密Kas对密钥材料接收单元602接收到的密钥材料进行安全性验证，验证通过，则触发计算单元603执行计算Kab的操作。

另外，该客户节点还可以包括：Kab确认单元606，用于利用计算单元603计算出的Kab验证密钥材料的完整性验证码，记为MIC 5，如果验证通过，则确认该Kab安全。

发送单元601，还用于在所述Kab确认单元606验证失败后，向第三方设备发送失败消息。

图7为本发明实施例提供的第二种主要方法流程图，如图7所示，该方法主要包括以下步骤：

步骤701：客户节点向第三方设备发送包含密码学参数（p，g）、根据该密码学参数和自身私钥x生成的客户节点公钥PKa的第一消息，并利用客户节点和验证服务器之间的共享秘密Kas对该第一消息进行安全保护。

本步骤中，第一消息中包括客户标识IDa、第三方设备标识IDb；并且，在以下步骤中传输的消息中均包含IDa和IDb。在以下的描述中不再赘述。

本步骤中，客户节点可以基于离散对数的Diffie-Hellman密钥交换密码学参数（p，g），其中，p是素数，g是有限域F_p的生成元，且g<p。客户节点可以根据该密码学参数（p，g）和自身的私钥x生成自身的公钥PKa，即$PKa = g^x \bmod p$。

本步骤中，该第一消息中还可以包括客户节点生成的临时值 Na。

对第一消息的安全保护可以是利用客户节点和验证服务器之间的共享秘密 Kas 生成该第一消息的 MIC 1，还可以是利用该 Kas 对该第一消息进行加密。

步骤 702：第三方设备接收到该第一消息后，向验证服务器发送包含第一消息、以及自身利用密码学参数和自身私钥生成的第三方设备公钥 PKb 的第二消息，并利用第三方设备和验证服务器之间的共享秘密 Kbs 对该第二消息进行安全保护。

本步骤中，第三方设备从所述第一消息中获取密码学参数，并利用该密码学参数（p，g）和自身的私钥 y 生成自身的公钥 PKb，即 $PKb = g^y \bmod p$。

另外，第三设备在接收到该第一消息后，还可以保存该第一消息中包含的 Na 值。在第二消息中也可以包含第三方设备生成的临时值 Nb。

本步骤中，对该第二消息进行安全保护可以是利用第三方设备和验证服务器之间的共享秘密 Kbs 生成该第二消息的完整性验证码 MIC 2，或者，对该第二消息中不包含第一消息的部分生成 MIC 2，还可以是利用该 Kbs 对该第二消息进行加密，或者，对该第二消息中不包含第一消息的部分进行加密。

步骤 703：验证服务器接收到第二消息后，对接收到的第二消息和其中包含的第一消息进行安全性验证，如果验证通过，则向第三方设备发送包含 PKa 和 PKb 的响应消息，并通过客户节点和验证服务器之间的共享秘密 Kas 对包含 PKa 的部分进行安全保护，通过第三方设备和验证服务器之间的共享秘密 Kbs 对包含 PKb 的部分进行安全保护。

进行安全保护的方式同样可以是利用 Kas 对包含 PKa 的部分生成 MIC 3，或者进行加密；利用 Kbs 对包含 PKb 的部分生成 MIC 4，或者进行加密。该包含 PKa 的部分还可以包含：Na、Nb、IDa、IDb 等，包含 PKb 的部分还可以包含 Na、Nb、IDa、IDb 等。

另外，验证服务器在回复响应消息之前还可以根据第二消息中包含的

Na值与自身存储的Na值进行比较，如果满足验证条件，则存储该接收到的Na值，并继续执行回复响应消息的步骤。

另外，响应消息中包含PKa的部分还可以包含Na，或经过特殊处理后的Na。

步骤704：第三方设备接收到该响应消息后，使用Kbs对包含PKb的部分进行安全性验证，如果验证通过，则按照预设的方式，利用该PKb和自身私钥y计算客户节点和第三方设备的共享密钥Kab；将包含PKa的部分转发给客户节点。

本步骤中，第三方设备对包含PKb的部分进行安全性验证可以是：利用Kbs对包含PKb的部分的MIC 4进行完整性验证或者进行解密。

其中，按照预设的方式计算Kab可以是：

$$Kab = PKb^{y} \bmod p = g^{xy} \bmod p 。 \qquad (1)$$

另外，第三方设备在计算Kab之前还可以根据包含PKb部分中包含的Na值与自身存储的Na值进行比较，如果满足验证条件，则验证成功，继续执行计算Kab的步骤；或者，将包含PKb部分中包含的对Na进行特殊处理的值进行逆处理，并将逆处理后的值与自身存储的Na值进行比较，如果满足验证条件，则验证成功，继续执行计算Kab的步骤。

步骤705：客户节点对接收到的包含PKa的部分进行安全性验证，如果验证通过，则利用该PKa和自身的私钥x计算Kab。

本步骤中，同样客户节点对包含PKb的部分进行安全性验证可以是利用Kas对包含PKa的部分的MIC 3进行完整性验证或者进行解密。

其中，按照预设的方式计算Kab可以是：

$$Kab = PKa^{x} \bmod p = g^{xy} \bmod p 。 \qquad (2)$$

由（1）式和（2）式可以看出，采用这种方式，第三方设备和客户节点分别计算出的Kab值相同。

另外，客户节点在计算Kab之前还可以根据包含PKa部分中包含的Na

值与自身存储的 Na 值进行比较，如果满足验证条件，则验证成功，继续执行计算 Kab 的步骤；或者，将包含 PKa 部分中包含的对 Na 进行特殊处理的值进行逆处理，并将逆处理后的值与自身存储的 Na 值进行比较，如果满足验证条件，则验证成功，继续执行计算 Kab 的步骤。

另外，在上述流程中，步骤 703 回复的响应消息中包含 PKa 的部分和包含 PKb 的部分还可以同时包含 Na、Nb 和验证服务器生成的临时值 Ns 中的一种或任意组合。在步骤 704 和步骤 705 中，可以将式（1）和式（2）计算出的值作为密钥材料 Master Key，即在步骤 704 中计算出的 Master Key 为：$Master\ Key = PKb^{y} \bmod p = g^{xy} \bmod p$，在步骤 705 中计算出的 Master Key 为：$Master\ Key = PKa^{x} \bmod p = g^{xy} \bmod p$。并在步骤 704 和步骤 705 中，继续将 Na、Nb 和 Ns 中的一种或任意组合、以及计算出的 Master Key 作为密钥材料生成 Kab。该 Kab 的计算公式可以为：

Kab = KDF（Master Key，Label | IDa | IDb | Na），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Nb），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Ns），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Na | Nb），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Na | Ns），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Nb | Ns），或者，

Kab = KDF（Master Key，Label | IDa | IDb | Na | Nb | Ns）。其中，KDF 为生成密钥的函数，Label 为一个预先设定的与 Kab 用途相关的字符串，| 为分隔符。

另外，还可以将密钥生存期 K_Lifetime、密钥长度 K_Length 等也作为密钥材料生成 Kab，例如：Kab = KDF（Master Key，Label | IDa | IDb | K_Lifetime | K_Length | Na）等。

另外，除了上述基于离散对数的 Diffie-Hellman 密钥交换密码学参数（p，g）外还可以采用其它的密码学参数，例如，还可以采用椭圆曲线密码系统

参数（p，d，f，G，n），其中，p为正整数，d和f是有限域F_p上的正整数，G是椭圆曲线$E(F_p)$上的基点，n是素数，是基点G的阶，其中，椭圆曲线的方程为$y^2= x^3+dx+f$。

采用该椭圆曲线密码系统参数时，在步骤701中生成的公钥PKa可以为：PKa = x×G，其中，x小于n。并且，客户节点将生成的公钥PKa和密码学参数（p，d，f，G，n）包含在第一消息中发送给第三方设备。在步骤702中第三方设备生成的公钥PKb可以为：PKb = y×G，同样，y小于n。步骤704中，计算Kab的方法是第三方设备利用PKa和自身私钥y计算，即：Master Key = y×PKa = y×x×G，可以将该Master Key作为Kab；也可以进一步利用该Master Key作为密钥材料生成Kab。步骤705中，计算Kab的方法是客户节点利用PKb和自身私钥x计算，即：Master Key = x×PKb = x×y×G，可以将该Master Key作为Kab；也可以进一步利用该Master Key作为密钥材料生成Kab。可以看出，无论采用什么方式的密码学参数，必需保证在步骤704和步骤705第三方设备和客户节点结合自身私钥计算的Master Key相同。

图8为本发明实施例提供的第二种系统结构图，如图8所示，该系统包括：客户节点801、第三方设备802和验证服务器803。

客户节点801，用于向第三方设备802发送包含密码学参数、根据密码学参数和自身私钥x生成的客户节点801公钥PKa的第一消息，并对第一消息进行安全保护；对第三方设备802发送的包含PKa或PKb的响应消息进行安全性验证，验证通过后，按照预设的第二方式，利用PKa或PKb以及自身私钥x计算Kab。

第三方设备802，用于接收到第一消息后，向验证服务器803发送包含第一消息、以及利用密码学参数和自身私钥y生成的第三方设备802公钥PKb的第二消息，并对该第二消息进行安全保护；对验证服务器803发送的响应消息进行安全性验证，验证通过后，按照预设的第一方式，利用PKa或PKb以及自

身私钥 y 计算客户节点 801 和第三方设备 802 的共享密钥 Kab，将包含 PKa 或 PKb 的响应消息发送给客户节点 801。

验证服务器 803，用于对接收到的第二消息和第二消息中包含的第一消息进行安全性验证，验证通过后，向第三方设备 802 发送包含 PKa 和 PKb 的响应消息，并对该响应消息的内容进行安全性保护。

图 9 为本发明实施例提供的第二种验证服务器的结构图，如图 9 所示，该验证服务器包括：接收单元 901、安全性验证单元 902、发送单元 903 和安全保护单元 904。

接收单元 901，用于接收第三方设备发送的包含客户节点公钥 PKa 和第三方设备公钥 PKb 的第二消息。

安全性验证单元 902，用于对接收单元 901 接收到的第二消息和第二消息中包含的第一消息进行安全性验证。

发送单元 903，用于在安全性验证单元 902 验证通过后，向第三方设备发送包含客户节点公钥 PKa 和第三方设备公钥 PKb 的响应消息。

安全保护单元 904，用于对发送单元 903 发送的响应消息进行安全保护。

该验证服务器还可以包括：比较单元 905 和 Na 存储单元 906。

比较单元 905，用于将接收单元 901 接收到的第二消息中包含的临时值 Na 与 Na 存储单元存储的 Na 值进行比较，如果满足验证条件，则触发发送单元 903 执行发送响应消息的操作，如果不满足验证条件，则禁止发送单元 903 执行发送响应消息的操作。

Na 存储单元 906，用于在比较单元 905 的比较结果为满足验证条件时，存储第二消息中包含的 Na。

图 10 为本发明实施例提供的第三方设备的结构图，如图 10 所示，该第三方设备可以包括：接收单元 1001、发送单元 1002、安全保护单元 1003、安全性验证单元 1004 和计算单元 1005。

接收单元 1001，用于接收客户节点发送的第一消息，接收验证服务器发送的响应消息。

发送单元 1002，用于在接收单元 1001 接收到第一消息后，向验证服务器发送包含第一消息、以及利用密码学参数和自身私钥 y 生成的第三方设备公钥 PKb 的第二消息，在安全性验证单元 1004 验证通过后，将包含客户节点公钥 PKa 和 PKb 的响应消息发送给客户节点。

安全保护单元 1003，用于对发送单元 1002 发送的第二消息进行安全保护。

安全性验证单元 1004，对接收单元 1001 接收的响应消息进行安全性验证。

计算单元 1005，用于在安全性验证单元 1004 验证通过后，按照预设的第一方式，利用 PKa 或 PKb 以及自身私钥 y 计算客户节点和第三方设备的共享密钥 Kab。

第三方设备还可以包括：Na 存储单元 1006 和比较单元 1007;

Na 存储单元 1006，用于存储第一消息中包含的 Na 值。

比较单元 1007，用于比较响应消息中包含的 Na 值与自身存储的 Na 值，如果满足验证条件，则触发计算单元 1005 执行计算的步骤，如果不满足验证条件，则禁止计算单元 1005 执行计算的步骤。

该第三方设备还可以包括：公钥生成单元 1008，用于利用第一消息中包含的密码学参数、以及自身私钥 y 生成第三方设备公钥 PKb。

图 11 为本发明实施例提供的第二种客户节点结构图，如图 11 所示，该客户节点包括：发送单元 1101、安全保护单元 1102、接收单元 1103、安全性验证单元 1104、和计算单元 1105。

发送单元 1101，用于向第三方设备发送包含密码学参数、以及根据该密码学参数和自身私钥 x 生成的客户节点公钥 PKa 的第一消息。

安全保护单元 1102，用于对发送单元 1101 发送的第一消息进行安全保护。

接收单元 1103，用于接收第三方设备发送的包含 PKa 或 PKb 的响应消息。

安全性验证单元 1104，用于对接收单元 1103 接收到的响应消息进行安全性验证。

计算单元 1105，用于在安全性验证单元 1104 验证通过后，按照预设的第二方式，利用 PKa 或 PKb 以及自身私钥 x 计算客户节点和第三方设备的共享密钥

Kab。

该客户节点还可以包括：密码学参数生成单元 1106 和公钥生成单元 1107。

密码学参数生成单元 1106，用于生成密码学参数。

公钥生成单元 1107，用于根据密码学参数生成单元 1106 生成的密码学参数计算和自身私钥 x 生成客户节点公钥 PKa。

该客户节点还可以包括：Na 存储单元 1108 和比较单元 1109。

Na 存储单元 1108，用于存储自身所在客户节点生成的 Na 值。

比较单元 1109，用于将响应消息中包含的临时值 Na 与 Na 存储单元 1108 存储的 Na 值进行比较，如果满足验证条件，则触发计算单元 1105 执行计算 Kab 的操作，否则，禁止计算单元 1105 执行计算 Kab 的操作。

由以上描述可以看出，在本发明实施例提供的第一种方法、系统和设备中，客户节点向第三方设备发送第一密钥分发请求；第三方设备接收到所述第一密钥分发请求后，向验证服务器发送第二密钥分发请求；验证服务器接收到第二密钥分发请求后，利用包含可变参数的密钥材料计算客户节点和第三方设备之间的共享密钥 Kab，向第三方设备发送包含 Kab 和密钥材料的密钥分发应答；第三方设备接收到该密钥分发应答后，获取该 Kab，并将密钥材料转发给客户节点；客户节点接收到该密钥材料后，利用该密钥材料，采用和验证服务器相同的方法计算 Kab。通过这种方式，验证服务器将可变参数引入密钥材料来计算 Kab，而不是全部采用固定不变的参数，使得一旦 Kab 泄漏，也能够利用该可变参数及时对 Kab 进行更新，从而提高了消息传输的安全性；并且，验证服务器将密钥材料提供给客户节点，使得客户节点能够通过相同的密钥计算方法，采用该密钥材料计算 Kab，这更进一步提高了消息传输的安全性。另外，第三方设备在将密钥材料转发给客户节点时，可以同时使用该 Kab 生成密钥材料的 MIC，客户节点在利用该密钥材料计算出 Kab 后，可以利用该 Kab 验证 MIC，从而确认第三方设备接收到 Kab，更进一步增强了密钥分发的安全性。

在本发明实施例提供的第二种方法、系统和设备中，客户节点和第三方

设备根据相同的密码学参数和自身的私钥生成各自的公钥，并将该公钥发送给验证服务器进行安全性验证，验证通过后，客户节点和第三方设备按照预先设定的方式，利用验证服务器回复的响应中包含的客户节点的公钥或第三方节点的公钥，以及自身的私钥生成相同的共享密钥 Kab。该方法通过在计算 Kab 的过程中引入可变的私钥，而不是全部采用固定不变的参数，使得一旦 Kab 泄漏，能够利用该可变的私钥及时对 Kab 进行更新，从而提高了消息传输的安全性。并且，更进一步地，可以将各设备生成的临时值作为可变的密钥材料计算 Kab，更加方便地对 Kab 进行更新，更进一步提高了消息传输的安全性。

并且，本发明实施例结合多种防止密钥泄漏和防止重放攻击的安全性措施，例如，采用对发送的密钥分发请求和密钥分发响应进行加密和生成完整性校验码的方式，利用将接收到的临时值与自身存储的临时值进行比较的方式等，更进一步地提高了消息传输的安全性。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

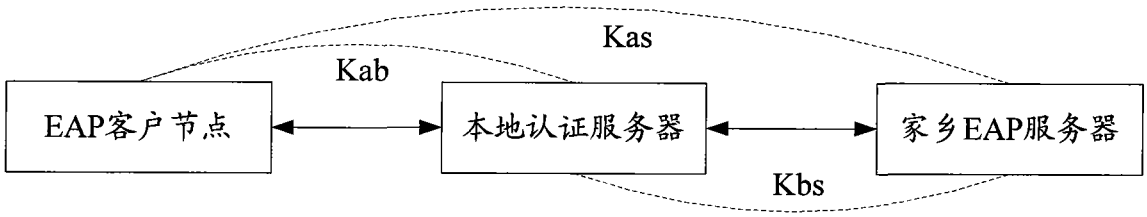

Kas
Kab
EAP客户节点
本地认证服务器
家乡EAP服务器
Kbs

图 1

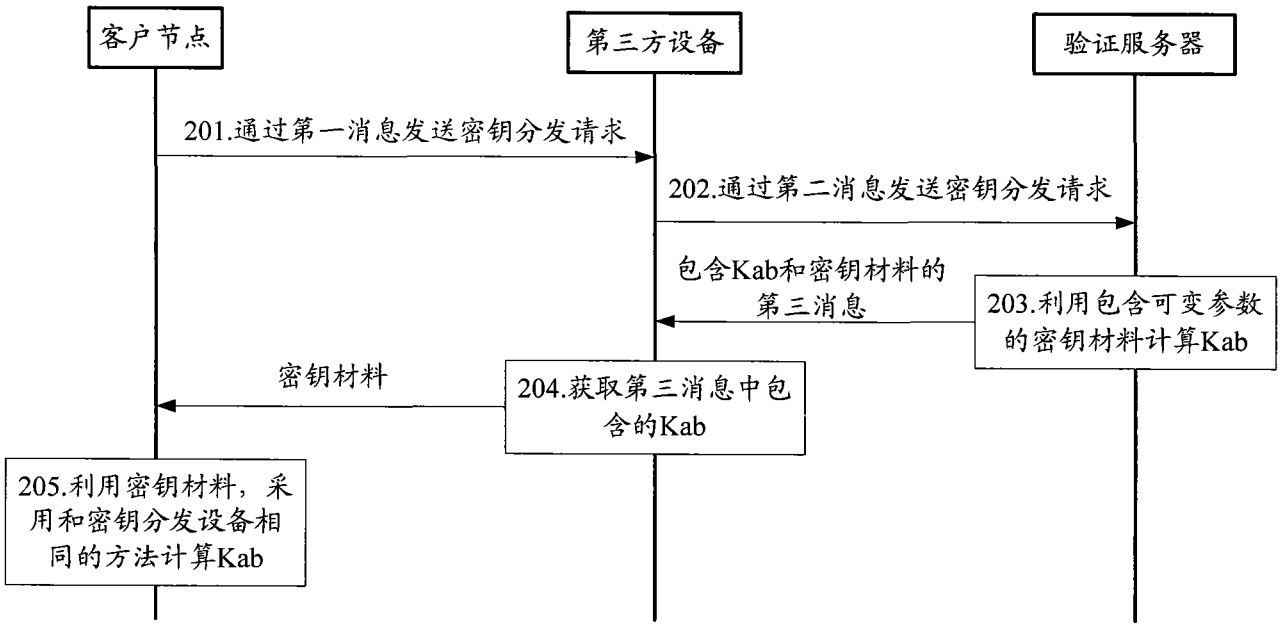

客户节点
第三方设备
验证服务器
201.通过第一消息发送密钥分发请求
202.通过第二消息发送密钥分发请求
包含Kab和密钥材料的第三消息
203.利用包含可变参数的密钥材料计算Kab
密钥材料
204.获取第三消息中包含的Kab
205.利用密钥材料，采用和密钥分发设备相同的方法计算Kab

图 2

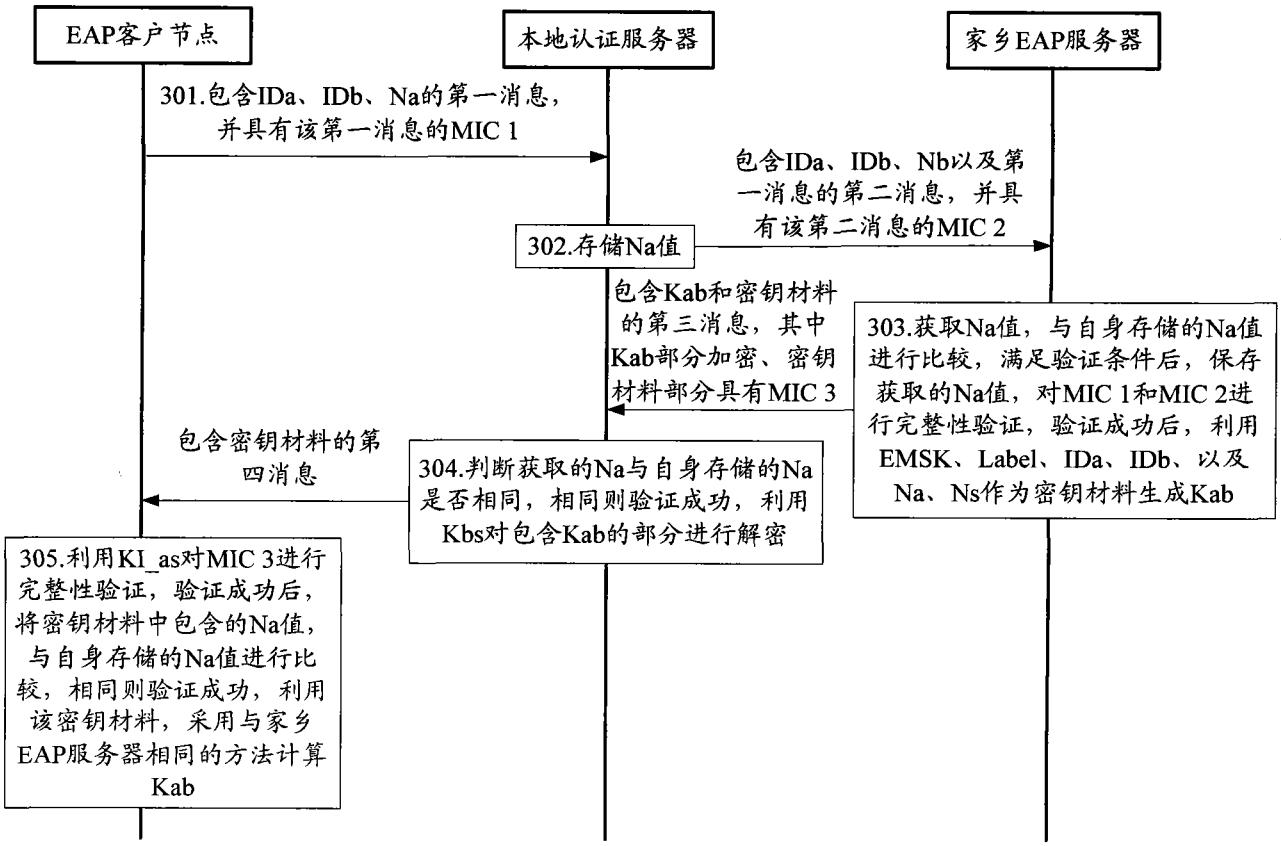

EAP客户节点
本地认证服务器
家乡EAP服务器
301.包含IDa、IDb、Na的第一消息，并具有该第一消息的MIC 1
包含IDa、IDb、Nb以及第一消息的第二消息，并具有该第二消息的MIC 2
302.存储Na值
包含Kab和密钥材料的第三消息，其中Kab部分加密、密钥材料部分具有MIC 3
303.获取Na值，与自身存储的Na值进行比较，满足验证条件后，保存获取的Na值，对MIC 1和MIC 2进行完整性验证，验证成功后，利用EMSK、Label、IDa、IDb、以及Na、Ns作为密钥材料生成Kab
包含密钥材料的第四消息
304.判断获取的Na与自身存储的Na是否相同，相同则验证成功，利用Kbs对包含Kab的部分进行解密
305.利用KI_as对MIC 3进行完整性验证，验证成功后，将密钥材料中包含的Na值，与自身存储的Na值进行比较，相同则验证成功，利用该密钥材料，采用与家乡EAP服务器相同的方法计算Kab

图 3

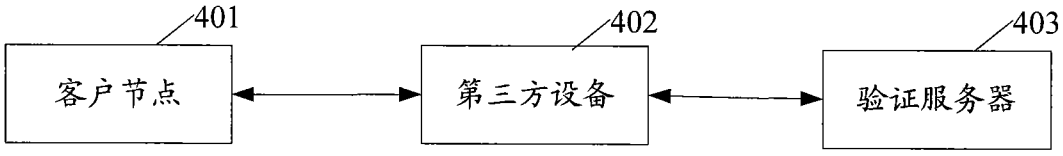

401
402
403
客户节点
第三方设备
验证服务器

图 4

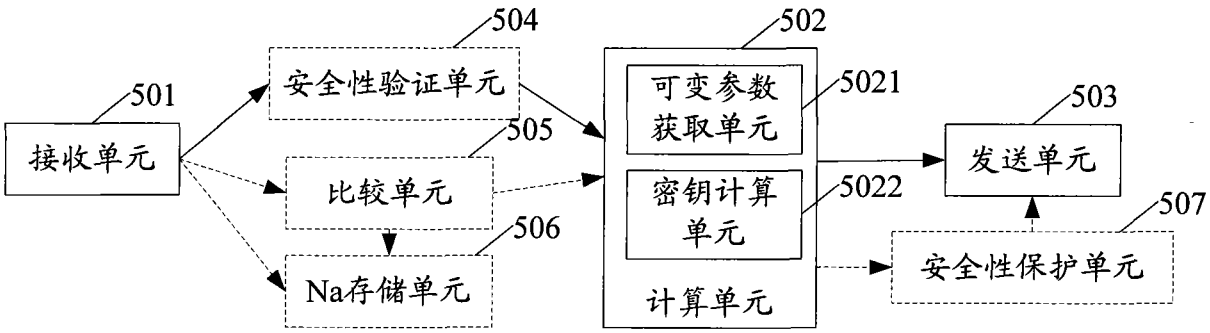

504
502
501
安全性验证单元
可变参数获取单元
5021
503
接收单元
505
比较单元
密钥计算单元
5022
发送单元
507
506
Na存储单元
安全性保护单元
计算单元

图 5

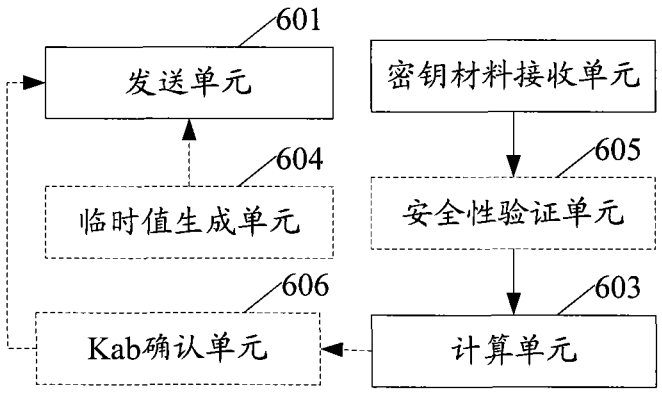

601
发送单元
密钥材料接收单元
604
605
临时值生成单元
安全性验证单元
606
603
Kab确认单元
计算单元

图 6

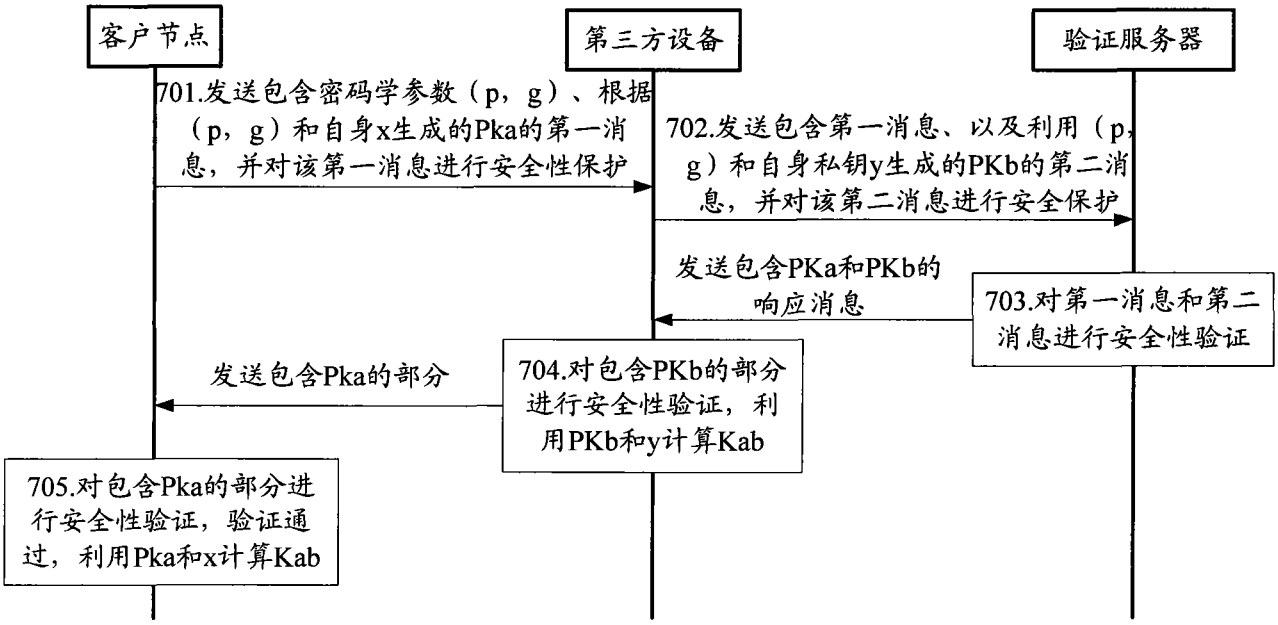

客户节点
第三方设备
验证服务器
701.发送包含密码学参数（p，g）、根据（p，g）和自身x生成的Pka的第一消息，并对该第一消息进行安全性保护
702.发送包含第一消息、以及利用（p，g）和自身私钥y生成的PKb的第二消息，并对该第二消息进行安全保护
发送包含PKa和PKb的响应消息
703.对第一消息和第二消息进行安全性验证
发送包含Pka的部分
704.对包含PKb的部分进行安全性验证，利用PKb和y计算Kab
705.对包含Pka的部分进行安全性验证，验证通过，利用Pka和x计算Kab

图 7

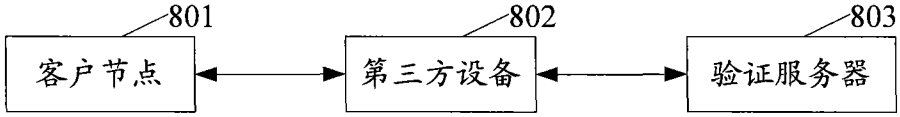

801
802
803
客户节点
第三方设备
验证服务器

图 8

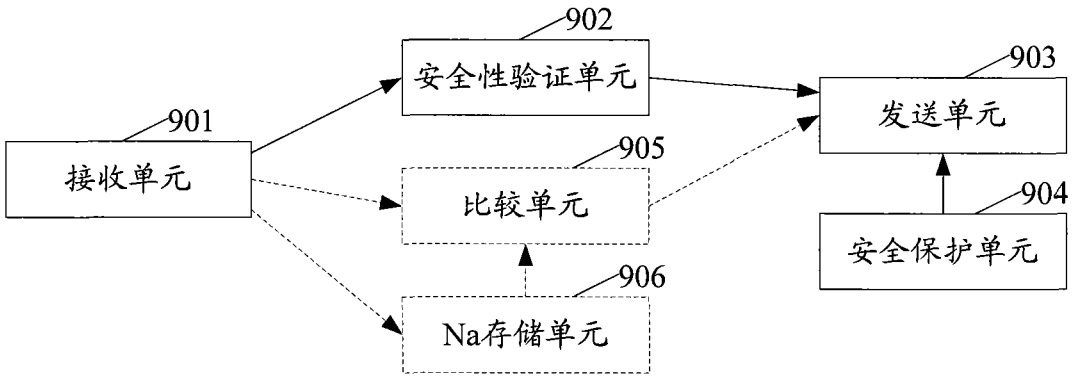

902
903
901
905
904
906
安全性验证单元
发送单元
接收单元
比较单元
安全保护单元
Na存储单元

图 9

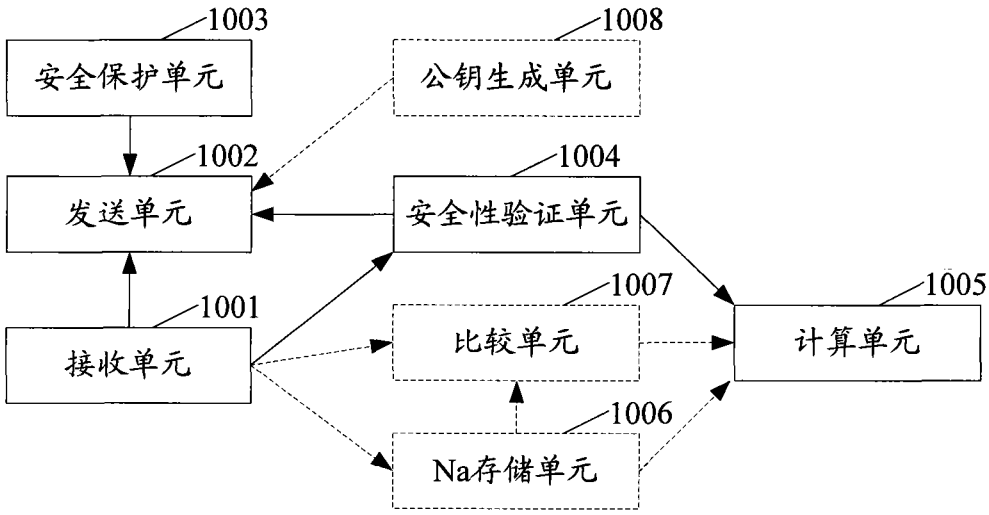

1003
安全保护单元
1008
公钥生成单元
1002
发送单元
1004
安全性验证单元
1001
接收单元
1007
比较单元
1005
计算单元
1006
Na存储单元

图 10

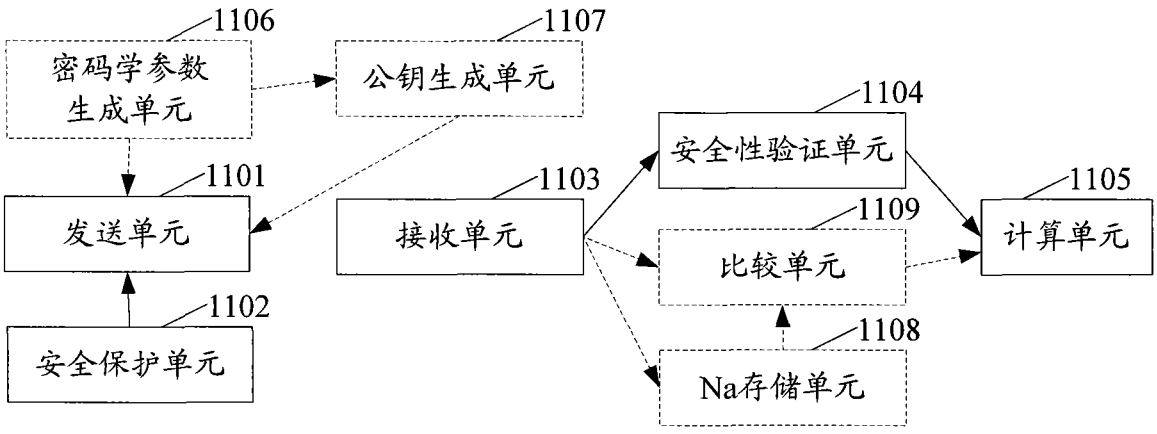

1106
密码学参数
生成单元
1107
公钥生成单元
1104
安全性验证单元
1101
发送单元
1103
接收单元
1105
计算单元
1109
比较单元
1102
安全保护单元
1108
Na存储单元

图 11