(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 104753682 A
(43)申请公布日 2015.07.01

(21)申请号 201510158953.5

(22)申请日 2015.04.03

(71)申请人 北京云安世纪科技有限公司
地址 100090 北京市海淀区中关村大街18号8层04-1668

(72)发明人 李勇奇

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

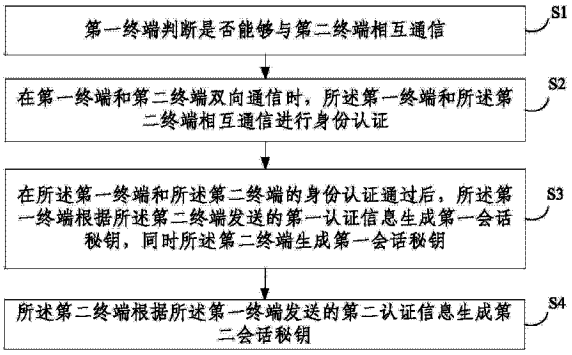
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种会话秘钥的生成系统及方法

(57)摘要

本发明公开了一种会话秘钥的生成系统及方法，该方法包括：S1、第一终端判断是否能够与第二终端相互通信；S2、在第一终端和第二终端双向通信时，所述第一终端和所述第二终端相互通信进行身份认证；S3、在所述第一终端和所述第二终端的身份认证通过后，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，同时所述第二终端生成第一会话秘钥；S4、所述第二终端根据所述第一终端发送的第二认证信息生成第二会话秘钥；其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。该会话秘钥为终端之间的通信提供了安全保障。



CN 104753682 A

1. 一种会话秘钥的生成方法，其特征在于，包括：

S1、第一终端判断是否能够与第二终端相互通信；

S2、在第一终端和第二终端双向通信时，所述第一终端和所述第二终端相互通信进行身份认证；

S3、在所述第一终端和所述第二终端的身份认证通过后，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，同时所述第二终端生成第一会话秘钥；

S4、所述第二终端根据所述第一终端发送的第二认证信息生成第二会话秘钥；

其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S3 中，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，包括：

所述第一终端根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥；

相应的，所述第二终端根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

3. 根据权利要求 2 所述的方法，其特征在于，所述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

4. 根据权利要求 1 所述的方法，其特征在于，在所述步骤 S1 中，所述第一终端判断不能够与所述第二终端相互通信时，所述方法包括：

S5、所述第一终端生成所述第二认证信息；

S6、所述第一终端根据所述第二认证信息生成第一认证口令和第一会话秘钥；

S7、所述第一终端对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端；

S8、所述第二终端通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

5. 根据权利要求 4 所述的方法，其特征在于，所述第二认证信息包括时间或事件信息。

6. 一种会话秘钥的生成系统，其特征在于，包括：第一终端和第二终端；

所述第一终端，用于在能够与第二终端相互通信时，和所述第二终端相互通信进行身份认证；

所述第一终端，还用于在和所述第二终端的身份认证通过后，根据所述第二终端发送的第一认证信息生成第一会话秘钥；

所述第二终端，用于生成第一会话秘钥；

所述第二终端，用于根据所述第一终端发送的第二认证信息生成第二会话秘钥；

其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

7. 根据权利要求 6 所述的系统，其特征在于，

所述第一终端，还用于根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥；

相应的，所述第二终端，还用于根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

8. 根据权利要求 7 所述的系统，其特征在于，所述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

9. 根据权利要求 6 所述的系统，其特征在于，

所述第一终端，用于不能够与所述第二终端相互通信时，生成所述第二认证信息 ；

所述第一终端，用于根据所述第二认证信息生成第一认证口令和第一会话秘钥 ；

所述第一终端，还用于对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端 ；

所述第二终端，用于通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

10. 根据权利要求 9 所述的系统，其特征在于，所述第二认证信息包括时间或事件信息。

一种会话秘钥的生成系统及方法

技术领域

[0001] 本发明涉及安全通信技术领域，具体涉及一种会话秘钥的生成系统及方法。

背景技术

[0002] OTP(One Time Password，一次性动态口令)是一种基于伪随机虚列的动态口令认证方法。OTP 通常分为时间同步、事件同步和挑战 / 应答三种认证方式。OTP 的基本原理是将自身保存的一个独一无二的种子 (Seed)，加入时间 (Time) 或事件 (Counter) 或挑战 (Challenge) 参数，采用单向哈希算法生成一次性的动态口令。

[0003] 目前终端之间进行通信时，OTP 只提供了身份认证方法，并未协商一种使两个终端进行安全通信的秘钥，因此，在某些场合下并不能够保证通信的安全。

发明内容

[0004] 针对现有技术中的缺陷，本发明提供一种会话秘钥的生成系统及方法，为终端之间的通信提供了安全保障。

[0005] 第一方面，本发明提供一种会话秘钥的生成方法，包括：

[0006] S1、第一终端判断是否能够与第二终端相互通信；

[0007] S2、在第一终端和第二终端双向通信时，所述第一终端和所述第二终端相互通信进行身份认证；

[0008] S3、在所述第一终端和所述第二终端的身份认证通过后，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，同时所述第二终端生成第一会话秘钥；

[0009] 具体的，在双方认证通过后，第一终端再生成第一会话秘钥，节省了运算的时间，防止在双方身份认证未通过时，浪费了大量的计算时间。

[0010] S4、所述第二终端根据所述第一终端发送的第二认证信息生成第二会话秘钥；

[0011] 其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

[0012] 可选的，所述步骤 S3 中，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，包括：

[0013] 所述第一终端根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥；

[0014] 相应的，所述第二终端根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

[0015] 可选的，所述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

[0016] 可选的，在所述步骤 S1 中，所述第一终端判断不能够与所述第二终端相互通信时，所述方法包括：

[0017] S5、所述第一终端在不能够与所述第二终端相互通信时，生成所述第二认证信

息；

[0018] S6、所述第一终端根据所述第二认证信息生成第一认证口令和第一会话秘钥；

[0019] S7、所述第一终端对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端；

[0020] S8、所述第二终端通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

[0021] 可选的，所述第二认证信息包括时间或事件信息。

[0022] 第二方面，本发明还提供了一种会话秘钥的生成系统，包括：第一终端和第二终端；

[0023] 所述第一终端，用于在能够与第二终端相互通信时，和所述第二终端相互通信进行身份认证；

[0024] 所述第一终端，还用于在和所述第二终端的身份认证通过后，根据所述第二终端发送的第一认证信息生成第一会话秘钥；

[0025] 所述第二终端，用于生成第一会话秘钥；

[0026] 所述第二终端，用于根据所述第一终端发送的第二认证信息生成第二会话秘钥；

[0027] 其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

[0028] 可选的，所述第一终端，还用于根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥；

[0029] 相应的，所述第二终端，还用于根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

[0030] 可选的，所述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

[0031] 可选的，所述第一终端，用于不能够与所述第二终端相互通信时，生成所述第二认证信息；

[0032] 所述第一终端，用于根据所述第二认证信息生成第一认证口令和第一会话秘钥；

[0033] 所述第一终端，还用于对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端；

[0034] 所述第二终端，用于通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

[0035] 可选的，所述第二认证信息包括时间或事件信息。

[0036] 由上述技术方案可知，本发明提供的一种会话秘钥的生成系统及方法，该方法针对终端通信的不同的情况，分别提供了如何生成一种会话秘钥，为终端之间的通信提供安全保障。

附图说明

[0037] 图 1 为本发明一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0038] 图 2 为本发明另一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0039] 图 3 为本发明另一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0040] 图 4 为本发明另一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0041] 图 5 为本发明一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0042] 图 6 为本发明一实施例提供的一种会话秘钥的生成方法的流程示意图；

[0043] 图 7 为本发明一实施例提供的一种会话秘钥的生成方法的流程示意图。

具体实施方式

[0044] 下面结合附图，对发明的具体实施方式作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案，而不能以此来限制本发明的保护范围。

[0045] 为了更清楚的说明本发明，下面首先对一次性会话秘钥 (One Time Key，OTK) 生成方法进行简单说明。

[0046] 假设通信的双方已经完成了 OTP 身份认证，其中 X 为 OTP 验证成功的计数器、时间因子、或挑战信息。

[0047] 方法 1 ：双方共享有序列号 SN 和种子 Seed，同时双方还共享有种子 Seed2，计算 Hash(Seed2,X)，得到会话秘钥。

[0048] 方法 2 ：双方共享有序列号 SN 和种子 Seed，Y 为双方事先协商一致的常量，或者为 SN 本身或其某种变换，或者 Y 为 Seed 本身或其某种变换，或者 Y 为 X 本身或其某种变换。计算 Hash(Seed,X,Y)，得到会话秘钥。

[0049] 方法 3 ：双方共享有序列号 SN 和种子 Seed，采用与 OTP 不同的 Hash 算法，计算 Hash(Seed,X)，得到会话秘钥。

[0050] 计算会话秘钥时，也可以使用对称加密算法，使用 Seed、X 和 Y 中的一个或两个变量作为秘钥，加密种子 Seed、X 和 Y 中的其他变量，结果作为会话秘钥。

[0051] 会话秘钥可直接生成为后续通信的数据加密秘钥以及加密 IV，或者按某变换方式生成为后续通信的数据加密秘钥以及加密 IV。

[0052] 图 1 为本发明实施例提供的一种会话秘钥的生成方法的流程示意图，如图 1 所示，在第一终端和第二终端双向通信且共享序列号和种子时，该方法包括如下步骤 ：

[0053] S1、第一终端判断是否能够与第二终端相互通信 ；

[0054] S2、在第一终端和第二终端双向通信时，所述第一终端和所述第二终端相互通信进行身份认证 ；

[0055] S3、在所述第一终端和所述第二终端的身份认证通过后，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，同时所述第二终端生成第一会话秘钥 ；

[0056] S4、所述第二终端根据所述第一终端发送的第二认证信息生成第二会话秘钥 ；

[0057] 其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

[0058] 具体的，所述第一终端根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥 ；

[0059] 相应的，所述第二终端根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

[0060] 举例来说，如图 2 所示，假设通信的双方 A 和 B 可以双向通信，A 和 B 共享有序列号 SN 和种子 Seed，可选共享 Seed2。

[0061] 第一步，A 生成挑战 C1 ；发送 SN 和 C1 给 B ；

[0062] 第二步，B 使用 OTP 基于 C1 生成 P1，使用 OTK 基于 C1 生成会话秘钥 K1，生成挑战 C2 ；

[0063] 第三步，B 返回 P1、C2 给 A ；

[0064] 第四步，A 使用 OTP 验证 P1，使用 OTK 基于 C1 生成会话秘钥 K1，使用 OTP 基于 C2 生成 P2，A 使用 OTK 基于 C2 生成会话秘钥 K2 ；

[0065] 第五步，A 发送 P2 给 B ；

[0066] 第六步，B 使用 OTP 验证 P2，使用 OTK 基于 C2 生成会话秘钥 K2 ；

[0067] 第七步，B 返回结果给 A，完成身份认证，最终会话秘钥为 K1 或 K2 或 K1+K2。

[0068] 在另一个可实现的方式中，如图 3 所示，假设通信的双方 A 和 B 可以双向通信，B 可以和认证服务器 S 双向通信。A 和 S 共享有序列号 SNa 和种子 Seeda，可选共享种子 Seeda2 ；B 和 S 共享有序列号 SNb 和种子 Seedb，可选共享种子 Seedb2。

[0069] 第一步，A 产生挑战 C1，使用 OTK 基于 C1 生成会话秘钥 K1 ；

[0070] 第二步，A 发送 SNa 和 C1 给 B ；

[0071] 第三步，B 产生挑战 C2，使用 OTK 基于 C2 生成会话秘钥 K2 ；

[0072] 第四步，B 发送 SNa、C1、SNb 和 C2 给 S ；

[0073] 第五步，S 使用 OTP 基于 C1 生成 P1，使用 OTP 基于 C2 生成 P2，使用 OTK 基于 C1 生成会话秘钥 K1，使用 OTK 基于 C2 生成会话秘钥 K2。生成会话秘钥 Kx，使用 K1 加密 Kx 和验证结果为 Ky，使用 K2 加密 Kx 和验证结果为 Kz ；

[0074] 第六步，S 返回给 P1、P2、Ky 和 Kz 给 B ；

[0075] 第七步，B 验证 P2，解密 Kz 得到 Kx 和验证结果 ；

[0076] 第八步，B 将 P2 和 Ky 返回给 A ；

[0077] 第九步，A 验证 P1，解密 Ky 得到 Kx 和验证结果，完成双向认证，且会话秘钥为 Kx。

[0078] 其中第一步或第四步，可选生成并附带一个随机数 R，则最终会话秘钥为 Hash(Kx,R)，或为 Kx 对 R 的对称加密结果，或为 R 对 Kx 的对称加密结果。

[0079] 在上述方法中，所述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

[0080] 图 4 示出了本发明提供了一种会话秘钥的生成方法的流程示意图，如图 4 所示，在所述步骤 S1 中，所述第一终端判断不能够与所述第二终端相互通信时，所述方法包括 ：

[0081] S5、所述第一终端生成所述第二认证信息 ；

[0082] S6、所述第一终端根据所述第二认证信息生成第一认证口令和第一会话秘钥 ；

[0083] S7、所述第一终端对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端 ；

[0084] S8、所述第二终端通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

[0085] 具体的，所述第二认证信息包括时间或事件信息。

[0086] 举例来说，如图 5 所示，假设通信的双方 A 到 B 只能单向通信，双方共享有序列号 SN 和种子 Seed，可选共享种子 Seed2。

[0087] 第一步，A 使用 OTP 基于计数器 T（时间或者事件）生成 P，使用 OTK 基于 T 生成会话秘钥 K，使用会话秘钥 K 加密数据 D 得到；

[0088] 第二步，A 发送 SN、P 和 E 给 B；

[0089] 第三步，B 使用 OTP 验证 P，使用 OTK 基于 T 生成会话秘钥 K。使用 K 解密 E 得到数据 D，完成认证和数据加密传输。

[0090] 在另一个可实现的方式中，如图 6 所示，假设通信的双方 A 到 B 只能单向通信，B 和认证服务器 S 可以双向通信。A 和 S 共享有序列号 SNa 和种子 Seeda，可选共享种子 Seeda2。B 和 S 共享有序列号 SNb 和种子 Seedb，可选共享种子 Seedb2。

[0091] 第一步，A 使用 OTP 基于计数器 T1（时间或者事件）生成 P1，使用 OTK 基于 T1 生成会话秘钥 K1，生成会话秘钥 Kx，使用会话秘钥 K1 加密 Kx 得到 Ky，使用 Kx 加密数据 D 得到 E；

[0092] 第二步，A 发送 SNa、P1、Ky 和 E 给 B；

[0093] 第三步，B 使用 OTP 基于计数器 T2（时间或者事件）生成 P2，使用 OTK 基于 T2 生成会话秘钥 K2；

[0094] 第四步，B 发送 SNa、P1、Ky、SNb 和 P2 给 S；

[0095] 第五步，S 验证 P1 和 P2，使用 OTK 基于 T1 生成会话秘钥 K1，使用 OTK 基于 T2 生成会话秘钥 K2，使用 K1 解密 Ky 得到 Kx，使用 K2 加密 Kx 得到 Kz；

[0096] 第六步，S 返回 Kz 和验证结果给 B；

[0097] 第七步，B 解密 Kz 得到 Kx，使用 Kx 解密 E 得到数据 D；完成认证和数据加密传输。

[0098] 第一步可选生成并附带一个随机数 R，加密数据 D 的会话秘钥为 Hash(Kx,R)，或为 Kx 对 R 的对称加密结果，或为 R 对 Kx 的对称加密结果。

[0099] 在另一个可实现的方式中，如图 7 所示，假设通信的双方 A 到 B 只能单向通信，A 和认证服务器 S 可以双向通信。A 和 S 共享有序列号 SNa 和种子 Seeda，可选共享种子 Seeda2。B 和 S 共享有序列号 SNb 和种子 Seedb，可选共享种子 Seedb2。

[0100] 第一步，A 使用 OTP 基于计数器 T1（时间或者事件）生成 P1，使用 OTK 基于 T1 生成会话秘钥 K1，生成会话秘钥 Kx，使用会话秘钥 K1 加密 Kx 得到 Ky，使用 Kx 加密数据 D 得到 E；

[0101] 第二步，A 发送 SNa、P1、Ky 给 S；

[0102] 第三步，S 验证 P1，使用 OTK 基于 T1 生成会话秘钥 K1，使用 OTP 基于计数器 T2（时间或者事件）生成 P2，使用 OTK 基于 T2 生成会话秘钥 K2，使用 K1 解密 Ky 得到 Kx，使用 K2 加密 Kx 得到 Kz；

[0103] 第四步，S 返回 P2、Kz 和验证结果给 A；

[0104] 第五步，A 发送 P2、Kz 和 E 给 B；

[0105] 第六步，B 验证 P2，使用 OTK 基于 T2 生成会话秘钥 K2，解密 Kz 得到 Kx，使用 Kx 解密 E 得到数据 D，完成认证和数据加密传输。

[0106] 第一步可选生成并附带一个随机数 R，加密数据 D 的会话秘钥为 Hash(Kx,R)，或为 Kx 对 R 的对称加密结果，或为 R 对 Kx 的对称加密结果。

[0107] Kx 也可以由 S 产生，并使用 K1 加密，传给 A，然后 A 解密出 Kx。

[0108] 上述单向通信的情况下，OTP 不能使用挑战 / 应答模式；双向通信的情况下，OTP 可以使用时间、时间或挑战 / 应答模式；安全通信过程中不局限于特定的时间、时间或挑战 / 应答模式。

[0109] 本发明实施例还提供了一种会话秘钥的生成系统，包括：第一终端和第二终端；

[0110] 所述第一终端，用于在能够与第二终端相互通信时，和所述第二终端相互通信进行身份认证；

[0111] 所述第一终端，还用于在和所述第二终端的身份认证通过后，根据所述第二终端发送的第一认证信息生成第一会话秘钥；

[0112] 所述第二终端，用于生成第一会话秘钥；

[0113] 所述第二终端，用于根据所述第一终端发送的第二认证信息生成第二会话秘钥；

[0114] 其中，所述第一终端和所述第二终端的通信的会话秘钥为所述第一会话秘钥或所述第二会话秘钥或二者之和。

[0115] 具体的，所述第一终端，还用于根据所述第一认证信息、序列号和 / 或种子，通过单向哈希算法生成第一会话秘钥；

[0116] 相应的，所述第二终端，还用于根据所述第二认证信息、序列号和 / 或种子，通过单向哈希算法生成第二会话秘钥。

[0117] 上述第一认证信息和所述第二认证信息包括时间、事件和挑战信息中的一种。

[0118] 具体的，所述第一终端，用于不能够与所述第二终端相互通信时，生成所述第二认证信息；

[0119] 所述第一终端，用于根据所述第二认证信息生成第一认证口令和第一会话秘钥；

[0120] 所述第一终端，还用于对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端；

[0121] 所述第二终端，用于通过 OTP 验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据。

[0122] 上述第二认证信息包括时间或事件信息。

[0123] 本发明的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0124] 本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0125] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围，其均应涵盖在本发明的权利要求和说明书的范围当中。

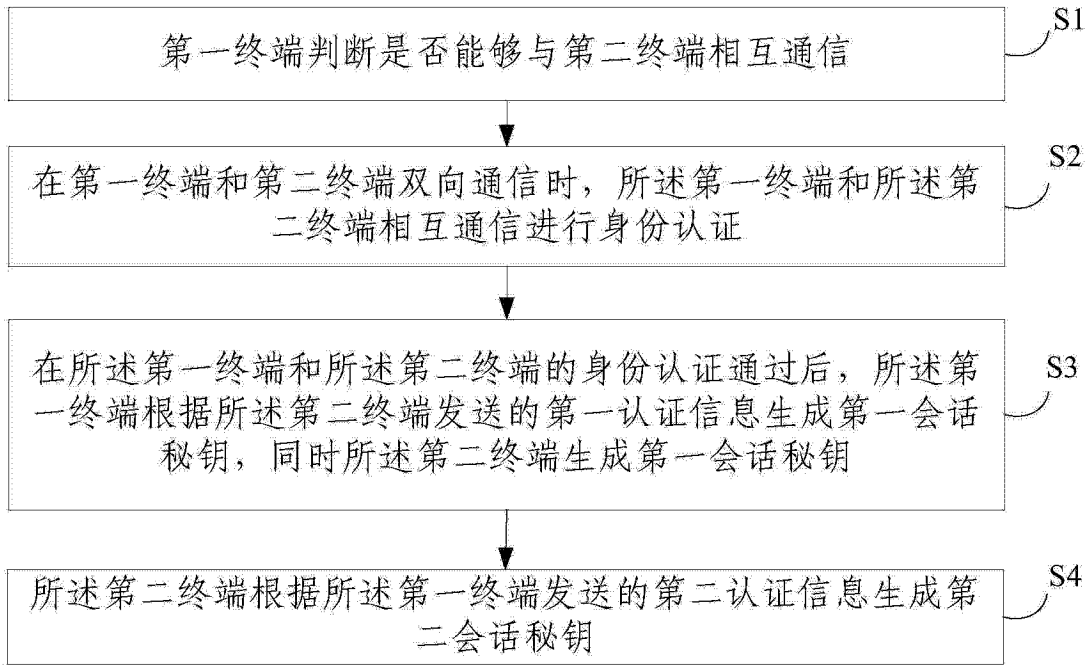

第一终端判断是否能够与第二终端相互通信
S1
在第一终端和第二终端双向通信时，所述第一终端和所述第二终端相互通信进行身份认证
S2
在所述第一终端和所述第二终端的身份认证通过后，所述第一终端根据所述第二终端发送的第一认证信息生成第一会话秘钥，同时所述第二终端生成第一会话秘钥
S3
所述第二终端根据所述第一终端发送的第二认证信息生成第二会话秘钥
S4

图 1

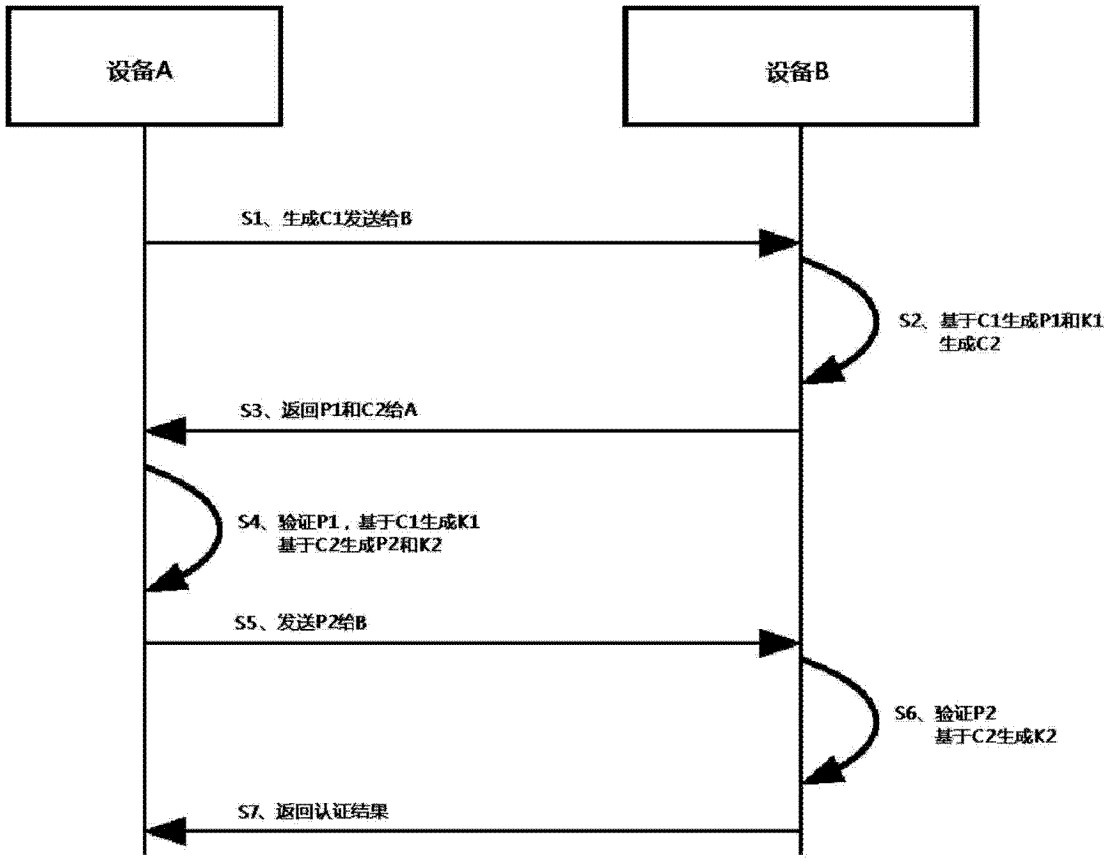

设备A
设备B
S1、生成C1发送给B
S2、基于C1生成P1和K1
生成C2
S3、返回P1和C2给A
S4、验证P1，基于C1生成K1
基于C2生成P2和K2
S5、发送P2给B
S6、验证P2
基于C2生成K2
S7、返回认证结果

图 2

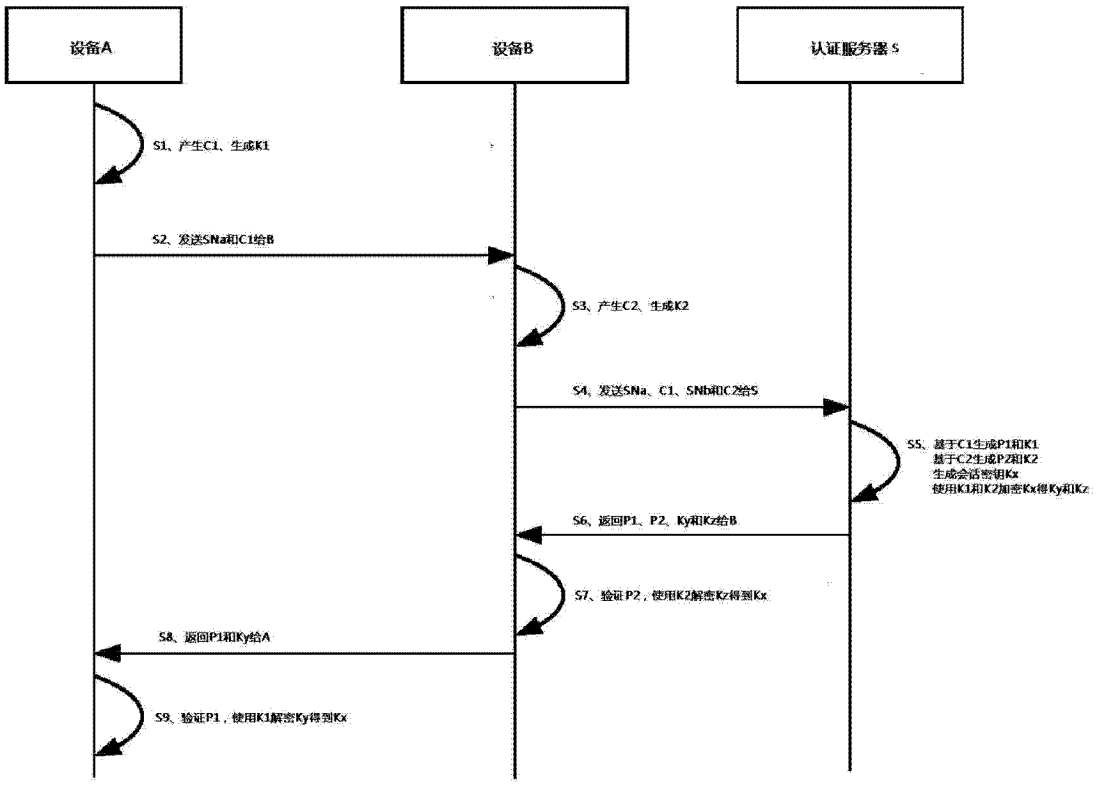

设备A
设备B
认证服务器S
S1、产生C1、生成K1
S2、发送SNa和C1给B
S3、产生C2、生成K2
S4、发送SNa、C1、SNb和C2给S
S5、基于C1生成P1和K1
基于C2生成P2和K2
生成会话密钥Kx
使用K1和K2加密Kx得Ky和Kz
S6、返回P1、P2、Ky和Kz给B
S7、验证P2，使用K2解密Kz得到Kx
S8、返回P1和Ky给A
S9、验证P1，使用K1解密Ky得到Kx

图 3

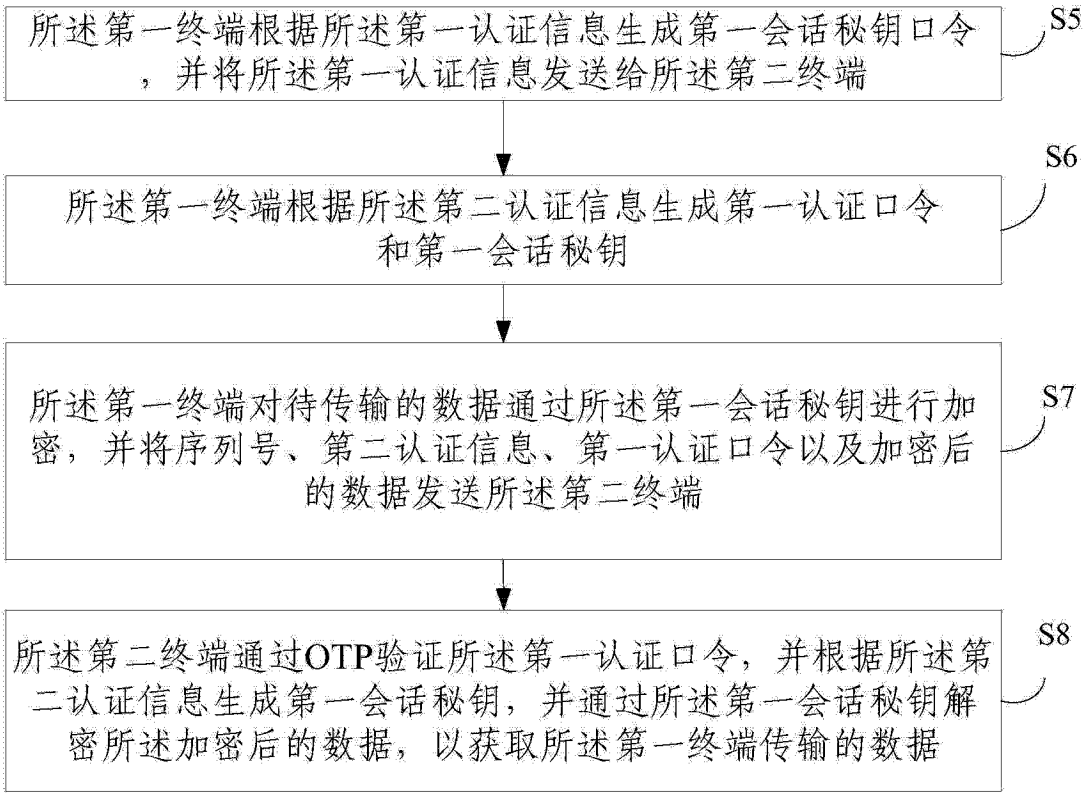

所述第一终端根据所述第一认证信息生成第一会话秘钥口令，并将所述第一认证信息发送给所述第二终端
S5
所述第一终端根据所述第二认证信息生成第一认证口令和第一会话秘钥
S6
所述第一终端对待传输的数据通过所述第一会话秘钥进行加密，并将序列号、第二认证信息、第一认证口令以及加密后的数据发送所述第二终端
S7
所述第二终端通过OTP验证所述第一认证口令，并根据所述第二认证信息生成第一会话秘钥，并通过所述第一会话秘钥解密所述加密后的数据，以获取所述第一终端传输的数据
S8

图 4

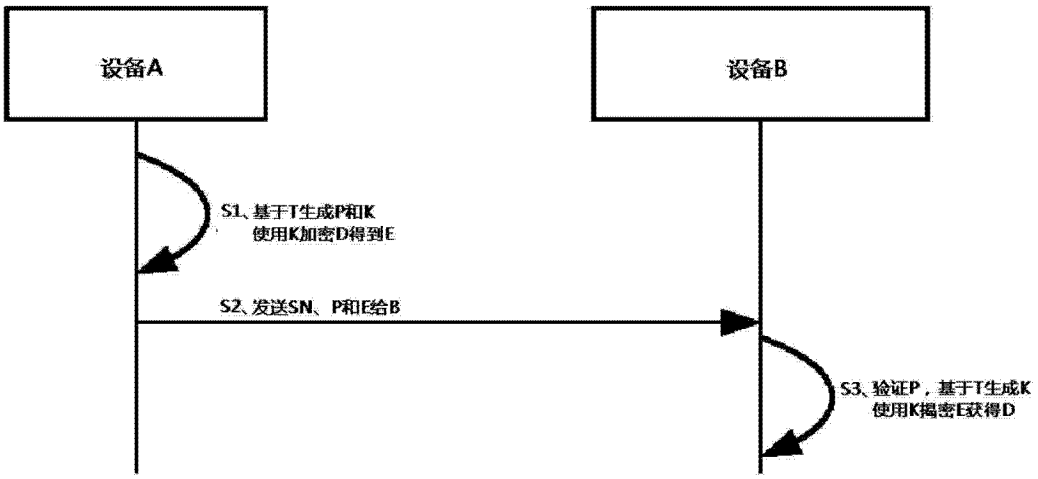

设备A
设备B
S1、基于T生成P和K
使用K加密D得到E
S2、发送SN、P和E给B
S3、验证P，基于T生成K
使用K揭密E获得D

图 5

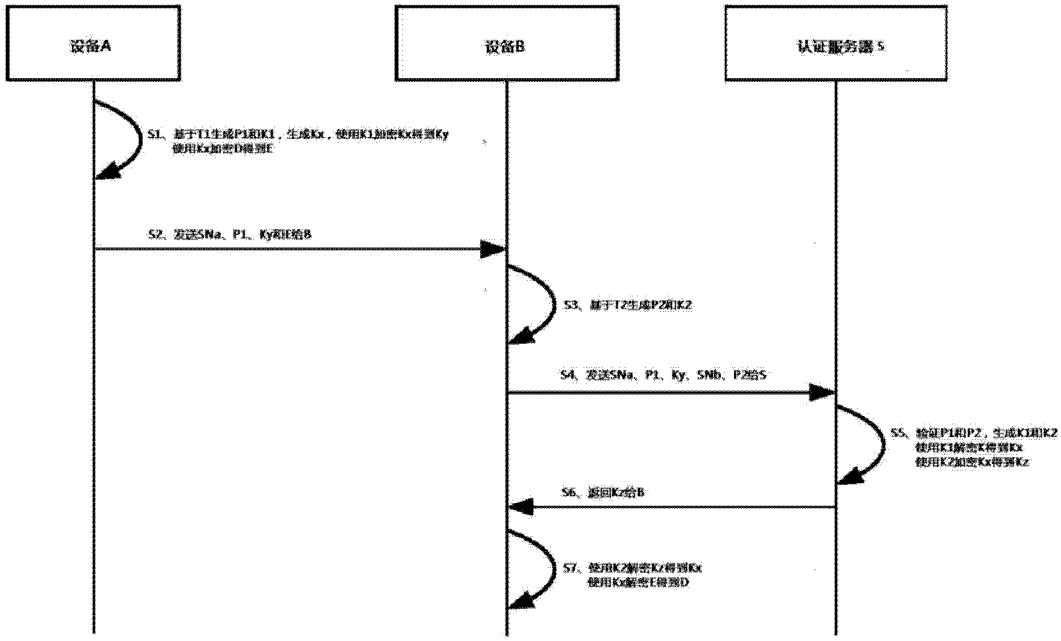

设备A
设备B
认证服务器 S
S1、基于T1生成P1和K1，生成Kx，使用K1加密Kx得到Ky
使用Kx加密D得到E
S2、发送SNa、P1、Ky和E给B
S3、基于T2生成P2和K2
S4、发送SNa、P1、Ky、SNb、P2给S
S5、验证P1和P2，生成K1和K2
使用K1解密K得到Kx
使用K2加密Kx得到Kz
S6、返回Kz给B
S7、使用K2解密Kz得到Kx
使用Kx解密E得到D

图 6

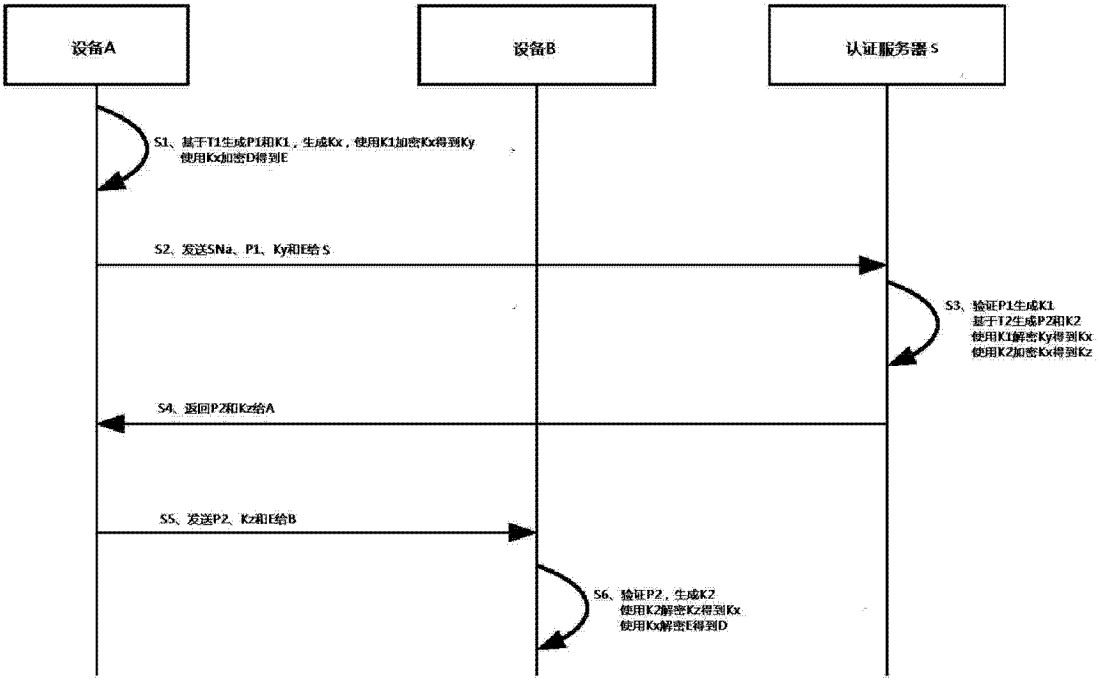

设备A
设备B
认证服务器 S
S1、基于T1生成P1和K1，生成Kx，使用K1加密Kx得到Ky
使用Kx加密D得到E
S2、发送SNa、P1、Ky和E给 S
S3、验证P1生成K1
基于T2生成P2和K2
使用K1解密Ky得到Kx
使用K2加密Kx得到Kz
S4、返回P2和Kz给A
S5、发送P2、Kz和E给B
S6、验证P2，生成K2
使用K2解密Kz得到Kx
使用Kx解密E得到D

图 7