(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 104852911 A
(43)申请公布日 2015.08.19

(21)申请号 201510206054.8

(22)申请日 2015.04.27

(71)申请人 小米科技有限责任公司
地址 100085 北京市海淀区清河中街68号华润五彩城购物中心二期13层

(72)发明人 林俊琦 池玉博 余新浪

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 祝亚男

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

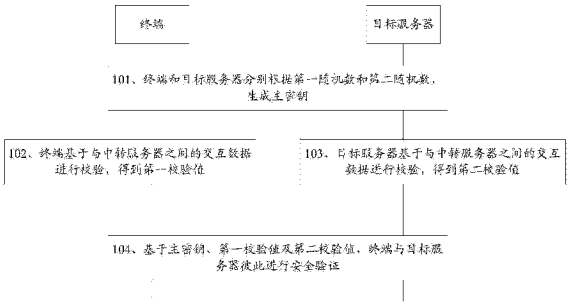
权利要求书5页 说明书20页 附图5页

(54)发明名称

安全验证方法、装置及系统

(57)摘要

本公开是关于一种安全验证方法、装置及系统，属于互联网技术领域。方法包括：终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥；终端基于与中转服务器之间的交互数据进行校验，得到第一校验值；目标服务器基于与中转服务器之间的交互数据进行校验，得到第二校验值；基于主密钥、第一校验值及第二校验值，终端与目标服务器彼此进行安全验证。本公开中终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。



CN 104852911 A

1. 一种安全验证方法，其特征在于，所述方法包括：

终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥；

所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值；

所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证。

2. 根据权利要求 1 所述方法，所述主密钥至少包括终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器的交互过程中包括以下步骤：

所述终端使用所述终端密钥对待发送数据进行加密，所述终端使用所述终端签名密钥对待发送数据进行签名；

所述目标服务器使用所述服务器密钥对待发送数据进行加密，所述目标服务器使用所述服务器签名密钥对待发送数据进行加密；

所述终端使用所述服务器密钥对接收到的数据进行解密，所述终端使用所述服务器签名密钥对接收到的数据的签名进行验证；

所述目标服务器使用所述终端密钥对接收到的数据进行解密，所述目标服务器使用所述终端签名密钥对接收到的数据的签名进行验证。

3. 根据权利要求 1 所述的方法，其特征在于，所述终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥之前，所述方法还包括：

所述终端向所述中转服务器发送验证请求，所述验证请求中至少携带第一交互信息，所述第一交互信息至少包括所述终端对应的安全设备的设备标识、所述第一随机数及目标服务器的地址；

所述中转服务器根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥；

所述中转服务器将所述公钥及所述第一交互信息发送至所述目标服务器地址对应的目标服务器；

所述目标服务器根据所述公钥对生成的第二随机数进行加密，得到第一密文；

所述目标服务器将所述第一密文发送至所述中转服务器，由所述中转服务器发送至所述终端；

所述终端将所述第一密文发送至所述安全设备；

所述安全设备根据存储的私钥对所述第一密文进行解密，得到所述第二随机数；

所述安全设备将所述第二随机数发送至所述终端。

4. 根据权利要求 3 所述的方法，其特征在于，所述中转服务器根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥之前，所述方法还包括：

所述安全设备接收设备生产商发送的密钥生成请求；

基于所述密钥生成请求，所述安全设备生成一对非对称密钥，所述非对称密钥包括所述公钥和私钥；

所述安全设备存储所述私钥，并将所述公钥与设备标识发送至所述中转服务器；

基于接收到的所述公钥与设备标识，所述中转服务器存储所述公钥与设备标识之间的

对应关系。

5. 根据权利要求 3 所述的方法，其特征在于，所述验证请求中还携带所述终端支持的加密算法信息、所述终端支持的签名算法信息，所述方法还包括：

所述目标服务器根据本端支持的加密算法及所述终端支持的加密算法信息，确定指定加密算法；

所述目标服务器根据本端支持的签名算法及所述终端支持的签名算法信息，确定指定签名算法；

所述目标服务器向所述中转服务器发送通知消息，由所述中转服务器将所述通知消息发送至所述终端，所述通知消息用于通知所述终端将所述指定加密算法作为加密算法、将所述指定签名算法作为签名算法。

6. 根据权利要求 5 所述的方法，其特征在于，所述目标服务器向所述中转服务器发送通知消息之后，所述方法还包括：

在所述终端与所述中转服务器、所述目标服务器与所述中转服务器之间的交互过程中，所述指定加密算法用于对待发送的交互数据进行加密运算，所述指定签名算法用于对待发送的交互数据进行签名运算。

7. 根据权利要求 1 所述的方法，其特征在于，所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值，包括：

所述终端按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第一拼接结果；

所述终端采用指定校验算法对所述第一拼接结果进行校验，得到第一校验值。

8. 根据权利要求 1 所述的方法，其特征在于，所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值，包括：

所述目标服务器按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第二拼接结果；

所述目标服务器采用指定校验算法对所述第二拼接结果进行校验，得到第二校验值。

9. 根据权利要求 2 所述的方法，其特征在于，所述基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证，包括：

所述终端根据所述终端签名密钥，对所述第一校验值进行签名，得到第一签名信息；

所述终端根据所述终端密钥，对所述第一签名信息进行加密，得到第一加密信息；

所述终端将所述第一加密信息发送至所述中转服务器，由所述中转服务器将所述第一加密信息发送至所述目标服务器；

所述目标服务器根据本地存储的终端密钥，对所述第一加密信息进行解密；

当对所述第一签名信息成功解密时，所述目标服务器获取所述第一签名信息；

所述目标服务器根据本地存储的终端签名密钥，对所述第一签名信息的签名进行验证；

当对所述第一签名信息的签名成功验证时，所述目标服务器获取所述第一校验值；

所述目标服务器将所述第一校验值与所述第二校验值进行比对；

如果所述第一校验值与所述第二校验值一致，则所述目标服务器生成验证成功信息；

所述目标服务器根据所述服务器签名密钥，对所述验证成功信息进行签名，得到第二

签名信息；

所述目标服务器根据所述服务器密钥，对所述第二签名信息进行加密，得到第二加密信息；

所述目标服务器将所述第二加密信息发送至所述中转服务器，由所述中转服务器将所述第二加密信息发送至所述终端；

所述终端根据本地存储的服务器密钥，对所述第二加密信息进行解密；

当对所述第二加密信息成功解密时，所述终端获取所述第二签名信息；

所述终端根据本地存储的服务器签名密钥，对所述第二签名信息的签名进行验证；

当对所述第二签名信息的签名成功验证时，所述终端确定与所述目标服务器彼此通过安全验证。

10. 根据权利要求 1 至 9 中任一权利要求所述的方法，其特征在于，所述方法应用于所述安全设备、所述终端、所述中转服务器及所述目标服务器进行数值转移的场景。

11. 一种安全验证系统，其特征在于，所述系统包括：终端、目标服务器及中转服务器；

所述终端，用于根据第一随机数和第二随机数，生成主密钥；

所述目标服务器，用于根据第一随机数和第二随机数，生成主密钥；

所述终端，用于基于与中转服务器之间的交互数据进行校验，得到第一校验值；

所述目标服务器，用于基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

所述终端，用于基于所述主密钥、所述第一校验值及所述第二校验值，与所述目标服务器进行安全验证；

所述目标服务器，用于基于所述主密钥、所述第一校验值及所述第二校验值，与所述终端进行安全验证。

12. 根据权利要求 11 所述系统，所述主密钥至少包括终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器的交互过程中包括以下步骤：

所述终端使用所述终端密钥对待发送数据进行加密，所述终端使用所述终端签名密钥对待发送数据进行签名；

所述目标服务器使用所述服务器密钥对待发送数据进行加密，所述目标服务器使用所述服务器签名密钥对待发送数据进行加密；

所述终端使用所述服务器密钥对接收到的数据进行解密，所述终端使用所述服务器签名密钥对接收到的数据的签名进行验证；

所述目标服务器使用所述终端密钥对接收到的数据进行解密，所述目标服务器使用所述终端签名密钥对接收到的数据的签名进行验证。

13. 根据权利要求 11 所述的系统，其特征在于，所述系统还包括：安全设备；

所述终端，还用于向所述中转服务器发送验证请求，所述验证请求中至少携带第一交互信息，所述第一交互信息至少包括所述终端对应的安全设备的设备标识、所述第一随机数及目标服务器的地址；

所述中转服务器，用于根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥；

所述中转服务器，用于将所述公钥及所述第一交互信息发送至所述目标服务器地址对应的目标服务器；

所述目标服务器，还用于根据所述公钥对生成的第二随机数进行加密，得到第一密文；

所述目标服务器，还用于将所述第一密文发送至所述中转服务器，由所述中转服务器发送至所述终端；

所述终端，还用于将所述第一密文发送至所述安全设备；

所述安全设备，用于根据存储的私钥对所述第一密文进行解密，得到所述第二随机数；

所述安全设备，用于将所述第二随机数发送至所述终端。

14. 根据权利要求 13 所述的系统，其特征在于，所述安全设备，还用于接收设备生产商发送的密钥生成请求；

所述安全设备，还用于基于所述密钥生成请求，生成一对非对称密钥，所述非对称密钥包括所述公钥和私钥；

所述安全设备，还用于存储所述私钥，并将所述公钥与设备标识发送至所述中转服务器；

基于接收到的所述公钥与设备标识，所述中转服务器存储所述公钥与设备标识之间的对应关系。

15. 根据权利要求 13 所述的系统，其特征在于，所述验证请求中还携带所述终端支持的加密算法信息、所述终端支持的签名算法信息；

所述目标服务器，还用于根据本端支持的加密算法及所述终端支持的加密算法信息，确定指定加密算法；

所述目标服务器，还用于根据本端支持的签名算法及所述终端支持的签名算法信息，确定指定签名算法；

所述目标服务器，还用于向所述中转服务器发送通知消息，由所述中转服务器将所述通知消息发送至所述终端，所述通知消息用于通知所述终端将所述指定加密算法作为加密算法、将所述指定签名算法作为签名算法。

16. 根据权利要求 15 所述的系统，其特征在于，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器之间的交互过程中，所述指定加密算法用于对待发送的交互数据进行加密运算，所述指定签名算法用于对待发送的交互数据进行签名运算。

17. 根据权利要求 11 所述的系统，其特征在于，所述终端，还用于按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第一拼接结果；

所述终端，还用于采用指定校验算法对所述第一拼接结果进行校验，得到第一校验值。

18. 根据权利要求 11 所述的系统，其特征在于，所述目标服务器，还用于按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第二拼接结果；

所述目标服务器采用指定校验算法对所述第二拼接结果进行校验，得到第二校验值。

19. 根据权利要求 12 所述的系统，其特征在于，所述终端，还用于根据所述终端签名密钥，对所述第一校验值进行签名，得到第一签名信息；

所述终端，还用于根据所述终端密钥，对所述第一签名信息进行加密，得到第一加密信

息；

所述终端，还用于将所述第一加密信息发送至所述中转服务器，由所述中转服务器将所述第一加密信息发送至所述目标服务器；

所述目标服务器，还用于根据本地存储的终端密钥，对所述第一加密信息进行解密；

所述目标服务器，还用于当对所述第一签名信息成功解密时，获取所述第一签名信息；

所述目标服务器，还用于根据本地存储的终端签名密钥，对所述第一签名信息的签名进行验证；

所述目标服务器，还用于当对所述第一签名信息的签名成功验证时，获取所述第一校验值；

所述目标服务器，还用于将所述第一校验值与所述第二校验值进行比对；

所述目标服务器，还用于当所述第一校验值与所述第二校验值一致时，生成验证成功信息；

所述目标服务器，还用于根据所述服务器签名密钥，对所述验证成功信息进行签名，得到第二签名信息；

所述目标服务器，还用于根据所述服务器密钥，对所述第二签名信息进行加密，得到第二加密信息；

所述目标服务器，还用于将所述第二加密信息发送至所述中转服务器，由所述中转服务器将所述第二加密信息发送至所述终端；

所述终端，还用于根据本地存储的服务器密钥，对所述第二加密信息进行解密；

所述终端，还用于当对所述第二加密信息成功解密时，获取所述第二签名信息；

所述终端，还用于根据本地存储的服务器签名密钥，对所述第二签名信息的签名进行验证；

所述终端，还用于当对所述第二签名信息的签名成功验证时，确定与所述目标服务器彼此通过安全验证。

20. 根据权利要求 11 至 19 中任一权利要求所述的系统，其特征在于，所述系统用于所述安全设备、所述终端、所述中转服务器及所述目标服务器进行数值转移的场景。

21. 一种安全验证装置，其特征在于，包括：

处理器；

用于存储处理器可执行的指令；

其中，所述处理器被配置为：

终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥；

所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值；

所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证。

安全验证方法、装置及系统

技术领域

[0001] 本公开涉及互联网技术领域，尤其涉及一种安全验证方法、装置及系统。

背景技术

[0002] 在现代生活中，网络购物因其方便、快捷，受到越来越多用户的青睐。在网络购物场景下，当用户通过终端中安装的购物应用，访问购物网站，查找到心仪物品后，为了能够获取该物品，用户需要通过互联网从账户中转移相应的数值给商家。在此过程中，为了保障用户账户安全，常常需要对参与数据转移的终端及目标服务器进行安全验证。

[0003] 目前，在进行安全验证时，主要有以下两种安全验证形式：

[0004] 第一种形式：基于单向验证的 TLS(Transport Layer Security，传输层安全）协议，目标服务器在生成一对非对称密钥后，存储非对称密钥中私钥，并将非对称密钥中的公钥发送给终端进行存储。当终端想要与目标服务器进行信息交互时，该终端可借助接收到的公钥对目标服务器进行验证，当对目标服务器的验证通过时，终端与目标服务器可进行信息交互。

[0005] 第二种形式：基于双向验证的 TLS 协议，目标服务器生成一对非对称密钥，存储该非对称密钥，并将该非对称密钥发送给终端进行存储。当终端想要与目标服务器进行信息交互时，终端和服务器基于存储的非对称密钥彼此进行验证，当验证通过时，终端和目标服务器可进行信息交互。

发明内容

[0006] 为克服相关技术中存在的问题，本公开提供一种安全验证方法、装置及系统。

[0007] 根据本公开实施例的第一方面，提供一种安全验证方法，所述方法包括：

[0008] 终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥；

[0009] 所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值；

[0010] 所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

[0011] 基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证。

[0012] 可选地，所述主密钥至少包括终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器的交互过程中包括以下步骤：

[0013] 所述终端使用所述终端密钥对待发送数据进行加密，所述终端使用所述终端签名密钥对待发送数据进行签名；

[0014] 所述目标服务器使用所述服务器密钥对待发送数据进行加密，所述目标服务器使用所述服务器签名密钥对待发送数据进行加密；

[0015] 所述终端使用所述服务器密钥对接收到的数据进行解密，所述终端使用所述服务

器签名密钥对接收到的数据的签名进行验证；

[0016] 所述目标服务器使用所述终端密钥对接收到的数据进行解密，所述目标服务器使用所述终端签名密钥对接收到的数据的签名进行验证。

[0017] 可选地，所述终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥之前，所述方法还包括：

[0018] 所述终端向所述中转服务器发送验证请求，所述验证请求中至少携带第一交互信息，所述第一交互信息至少包括所述终端对应的安全设备的设备标识、所述第一随机数及目标服务器的地址；

[0019] 所述中转服务器根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥；

[0020] 所述中转服务器将所述公钥及所述第一交互信息发送至所述目标服务器地址对应的目标服务器；

[0021] 所述目标服务器根据所述公钥对生成的第二随机数进行加密，得到第一密文；

[0022] 所述目标服务器将所述第一密文发送至所述中转服务器，由所述中转服务器发送至所述终端；

[0023] 所述终端将所述第一密文发送至所述安全设备；

[0024] 所述安全设备根据存储的私钥对所述第一密文进行解密，得到所述第二随机数；

[0025] 所述安全设备将所述第二随机数发送至所述终端。

[0026] 可选地，所述中转服务器根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥之前，所述方法还包括：

[0027] 所述安全设备接收设备生产商发送的密钥生成请求；

[0028] 基于所述密钥生成请求，所述安全设备生成一对非对称密钥，所述非对称密钥包括所述公钥和私钥；

[0029] 所述安全设备存储所述私钥，并将所述公钥与设备标识发送至所述中转服务器；

[0030] 基于接收到的所述公钥与设备标识，所述中转服务器存储所述公钥与设备标识之间的对应关系。

[0031] 可选地，所述验证请求中还携带所述终端支持的加密算法信息、所述终端支持的签名算法信息，所述方法还包括：

[0032] 所述目标服务器根据本端支持的加密算法及所述终端支持的加密算法信息，确定指定加密算法；

[0033] 所述目标服务器根据本端支持的签名算法及所述终端支持的签名算法信息，确定指定签名算法；

[0034] 所述目标服务器向所述中转服务器发送通知消息，由所述中转服务器将所述通知消息发送至所述终端，所述通知消息用于通知所述终端将所述指定加密算法作为加密算法、将所述指定签名算法作为签名算法。

[0035] 可选地，所述目标服务器向所述中转服务器发送通知消息之后，所述方法还包括：

[0036] 在所述终端与所述中转服务器、所述目标服务器与所述中转服务器之间的交互过程中，所述指定加密算法用于对待发送的交互数据进行加密运算，所述指定签名算法用于

对待发送的交互数据进行签名运算。

[0037] 可选地，所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值，包括：

[0038] 所述终端按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第一拼接结果；

[0039] 所述终端采用指定校验算法对所述第一拼接结果进行校验，得到第一校验值。

[0040] 可选地，所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值，包括：

[0041] 所述目标服务器按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第二拼接结果；

[0042] 所述目标服务器采用指定校验算法对所述第二拼接结果进行校验，得到第二校验值。

[0043] 可选地，所述基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证，包括：

[0044] 所述终端根据所述终端签名密钥，对所述第一校验值进行签名，得到第一签名信息；

[0045] 所述终端根据所述终端密钥，对所述第一签名信息进行加密，得到第一加密信息；

[0046] 所述终端将所述第一加密信息发送至所述中转服务器，由所述中转服务器将所述第一加密信息发送至所述目标服务器；

[0047] 所述目标服务器根据本地存储的终端密钥，对所述第一加密信息进行解密；

[0048] 当对所述第一签名信息成功解密时，所述目标服务器获取所述第一签名信息；

[0049] 所述目标服务器根据本地存储的终端签名密钥，对所述第一签名信息的签名进行验证；

[0050] 当对所述第一签名信息的签名成功验证时，所述目标服务器获取所述第一校验值；

[0051] 所述目标服务器将所述第一校验值与所述第二校验值进行比对；

[0052] 如果所述第一校验值与所述第二校验值一致，则所述目标服务器生成验证成功信息；

[0053] 所述目标服务器根据所述服务器签名密钥，对所述验证成功信息进行签名，得到第二签名信息；

[0054] 所述目标服务器根据所述服务器密钥，对所述第二签名信息进行加密，得到第二加密信息；

[0055] 所述目标服务器将所述第二加密信息发送至所述中转服务器，由所述中转服务器将所述第二加密信息发送至所述终端；

[0056] 所述终端根据本地存储的服务器密钥，对所述第二加密信息进行解密；

[0057] 当对所述第二加密信息成功解密时，所述终端获取所述第二签名信息；

[0058] 所述终端根据本地存储的服务器签名密钥，对所述第二签名信息的签名进行验证；

[0059] 当对所述第二签名信息的签名成功验证时，所述终端确定与所述目标服务器彼此通过安全验证。

[0060] 可选地，其特征在于，所述方法应用于所述安全设备、所述终端、所述中转服务器及所述目标服务器进行数值转移的场景。

[0061] 根据本公开实施例的第二方面，提供一种安全验证系统，所述系统包括：终端、目标服务器及中转服务器；

[0062] 所述终端，用于根据第一随机数和第二随机数，生成主密钥；

[0063] 所述目标服务器，用于根据第一随机数和第二随机数，生成主密钥；

[0064] 所述终端，用于基于与中转服务器之间的交互数据进行校验，得到第一校验值；

[0065] 所述目标服务器，用于基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

[0066] 所述终端，用于基于所述主密钥、所述第一校验值及所述第二校验值，与所述目标服务器进行安全验证；

[0067] 所述目标服务器，用于基于所述主密钥、所述第一校验值及所述第二校验值，与所述终端进行安全验证。

[0068] 可选地，所述主密钥至少包括终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器的交互过程中包括以下步骤：

[0069] 所述终端使用所述终端密钥对待发送数据进行加密，所述终端使用所述终端签名密钥对待发送数据进行签名；

[0070] 所述目标服务器使用所述服务器密钥对待发送数据进行加密，所述目标服务器使用所述服务器签名密钥对待发送数据进行加密；

[0071] 所述终端使用所述服务器密钥对接收到的数据进行解密，所述终端使用所述服务器签名密钥对接收到的数据的签名进行验证；

[0072] 所述目标服务器使用所述终端密钥对接收到的数据进行解密，所述目标服务器使用所述终端签名密钥对接收到的数据的签名进行验证。

[0073] 可选地，所述系统还包括：安全设备；

[0074] 所述终端，还用于向所述中转服务器发送验证请求，所述验证请求中至少携带第一交互信息，所述第一交互信息至少包括所述终端对应的安全设备的设备标识、所述第一随机数及目标服务器的地址；

[0075] 所述中转服务器，用于根据所述设备标识，从设备标识与公钥之间的对应关系中，获取所述设备标识对应的公钥；

[0076] 所述中转服务器，用于将所述公钥及所述第一交互信息发送至所述目标服务器地址对应的目标服务器；

[0077] 所述目标服务器，还用于根据所述公钥对生成的第二随机数进行加密，得到第一密文；

[0078] 所述目标服务器，还用于将所述第一密文发送至所述中转服务器，由所述中转服务器发送至所述终端；

[0079] 所述终端，还用于将所述第一密文发送至所述安全设备；

[0080] 所述安全设备，用于根据存储的私钥对所述第一密文进行解密，得到所述第二随机数；

[0081] 所述安全设备，用于将所述第二随机数发送至所述终端。

[0082] 可选地，所述安全设备，还用于接收设备生产商发送的密钥生成请求；

[0083] 所述安全设备，还用于基于所述密钥生成请求，生成一对非对称密钥，所述非对称密钥包括所述公钥和私钥；

[0084] 所述安全设备，还用于存储所述私钥，并将所述公钥与设备标识发送至所述中转服务器；

[0085] 基于接收到的所述公钥与设备标识，所述中转服务器存储所述公钥与设备标识之间的对应关系。

[0086] 可选地，所述验证请求中还携带所述终端支持的加密算法信息、所述终端支持的签名算法信息；

[0087] 所述目标服务器，还用于根据本端支持的加密算法及所述终端支持的加密算法信息，确定指定加密算法；

[0088] 所述目标服务器，还用于根据本端支持的签名算法及所述终端支持的签名算法信息，确定指定签名算法；

[0089] 所述目标服务器，还用于向所述中转服务器发送通知消息，由所述中转服务器将所述通知消息发送至所述终端，所述通知消息用于通知所述终端将所述指定加密算法作为加密算法、将所述指定签名算法作为签名算法。

[0090] 可选地，在所述终端与所述中转服务器、所述目标服务器与所述中转服务器之间的交互过程中，所述指定加密算法用于对待发送的交互数据进行加密运算，所述指定签名算法用于对待发送的交互数据进行签名运算。

[0091] 可选地，所述终端，还用于按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第一拼接结果；

[0092] 所述终端，还用于采用指定校验算法对所述第一拼接结果进行校验，得到第一校验值。

[0093] 可选地，所述目标服务器，还用于按照时间顺序，将与所述中转服务器之间的交互数据进行拼接，得到第二拼接结果；

[0094] 所述目标服务器采用指定校验算法对所述第二拼接结果进行校验，得到第二校验值。

[0095] 可选地，所述终端，还用于根据所述终端签名密钥，对所述第一校验值进行签名，得到第一签名信息；

[0096] 所述终端，还用于根据所述终端密钥，对所述第一签名信息进行加密，得到第一加密信息；

[0097] 所述终端，还用于将所述第一加密信息发送至所述中转服务器，由所述中转服务器将所述第一加密信息发送至所述目标服务器；

[0098] 所述目标服务器，还用于根据本地存储的终端密钥，对所述第一加密信息进行解密；

[0099] 所述目标服务器，还用于当对所述第一签名信息成功解密时，获取所述第一签名

信息；

[0100] 所述目标服务器，还用于根据本地存储的终端签名密钥，对所述第一签名信息的签名进行验证；

[0101] 所述目标服务器，还用于当对所述第一签名信息的签名成功验证时，获取所述第一校验值；

[0102] 所述目标服务器，还用于将所述第一校验值与所述第二校验值进行比对；

[0103] 所述目标服务器，还用于当所述第一校验值与所述第二校验值一致时，生成验证成功信息；

[0104] 所述目标服务器，还用于根据所述服务器签名密钥，对所述验证成功信息进行签名，得到第二签名信息；

[0105] 所述目标服务器，还用于根据所述服务器密钥，对所述第二签名信息进行加密，得到第二加密信息；

[0106] 所述目标服务器，还用于将所述第二加密信息发送至所述中转服务器，由所述中转服务器将所述第二加密信息发送至所述终端；

[0107] 所述终端，还用于根据本地存储的服务器密钥，对所述第二加密信息进行解密；

[0108] 所述终端，还用于当对所述第二加密信息成功解密时，获取所述第二签名信息；

[0109] 所述终端，还用于根据本地存储的服务器签名密钥，对所述第二签名信息的签名进行验证；

[0110] 所述终端，还用于当对所述第二签名信息的签名成功验证时，确定与所述目标服务器彼此通过安全验证。

[0111] 可选地，所述系统用于所述安全设备、所述终端、所述中转服务器及所述目标服务器进行数值转移的场景。

[0112] 根据本公开实施例的第三方面，提供一种安全验证装置，所述装置包括：

[0113] 处理器；

[0114] 用于存储处理器可执行的指令；

[0115] 其中，所述处理器被配置为：

[0116] 终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥；

[0117] 所述终端基于与中转服务器之间的交互数据进行校验，得到第一校验值；

[0118] 所述目标服务器基于与所述中转服务器之间的交互数据进行校验，得到第二校验值；

[0119] 基于所述主密钥、所述第一校验值及所述第二校验值，所述终端与所述目标服务器彼此进行安全验证。

[0120] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0121] 终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0122] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0123] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0124] 图 1A 是根据一示例性实施例示出的一种安全验证方法所涉及到的实施环境的流程图；

[0125] 图 1 是根据一示例性实施例示出的一种安全验证方法的流程图。

[0126] 图 2 是根据一示例性实施例示出的一种安全验证方法的流程图。

[0127] 图 3 是根据一示例性实施例示出的一种安全验证系统的装置结构示意图。

[0128] 图 4 是根据一示例性实施例示出的一种安全验证系统的装置结构示意图。

[0129] 图 5 是根据一示例性实施例示出的一种安全验证装置的框图。

[0130] 图 6 是根据一示例性实施例示出的一种安全验证装置的框图。

具体实施方式

[0131] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0132] 请参见图 1A，其示出了本公开实施例提供的安全验证方法所涉及的实施环境的示意图。该实施环境包括安全设备 1001、终端 1002、中转服务器 1003 及目标服务器 1004。

[0133] 其中，安全设备 1001 是指具有独立运算资源、有严格的数据访问权限的运行环境，该安全设备 1001 可以为金融领域使用的安全芯片等，例如 SE(Secure Element，安全元件)、TEE(Trusted Execution Environment，可信任执行环境)、eUICC(Embedded Universal Integrated Circuit Card，嵌入式通用集成电路卡)等。

[0134] 终端 1002 可以为 POS 机、手机、电脑等，本实施例不对终端作具体的限定。该终端具有数据处理功能，可对发送的数据进行加密并签名，对接收到的数据进行解密并验证签名。

[0135] 中转服务器 1003 具有数据读取、发送功能。

[0136] 目标服务器 1004 具有数据处理功能，可对发送的数据进行加密并签名，对接收到的数据进行解密并验证签名。

[0137] 上述终端 1002 与中转服务器 1003 可通过无线网络或者有线网络进行通信，中转服务器 1003 与目标服务器 1004 可通过无线网络或有线网络进行通信。

[0138] 图 1 是根据一示例性实施例示出的一种安全验证方法的流程图，如图 1 所示，安全验证方法用于终端中，包括以下步骤。

[0139] 在步骤 101 中，终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥。

[0140] 在步骤 102 中，终端基于与中转服务器之间的交互数据进行校验，得到第一校验值。

[0141] 在步骤 103 中，目标服务器基于与中转服务器之间的交互数据进行校验，得到第

二校验值。

[0142] 在步骤 104 中，基于主密钥、第一校验值及第二校验值，终端与目标服务器彼此进行安全验证。

[0143] 本公开实施例提供的方法，终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0144] 在本公开的另一个实施中，主密钥至少包括终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，在终端与中转服务器、目标服务器与中转服务器的交互过程中包括以下步骤：

[0145] 终端使用终端密钥对待发送数据进行加密，终端使用终端签名密钥对待发送数据进行签名；

[0146] 目标服务器使用服务器密钥对待发送数据进行加密，目标服务器使用服务器签名密钥对待发送数据进行加密；

[0147] 终端使用服务器密钥对接收到的数据进行解密，终端使用服务器签名密钥对接收到的数据的签名进行验证；

[0148] 目标服务器使用终端密钥对接收到的数据进行解密，目标服务器使用终端签名密钥对接收到的数据的签名进行验证。

[0149] 在本公开的另一个实施例中，终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥之前，方法还包括：

[0150] 终端向中转服务器发送验证请求，验证请求中至少携带第一交互信息，第一交互信息至少包括终端对应的安全设备的设备标识、第一随机数及目标服务器的地址；

[0151] 中转服务器根据设备标识，从设备标识与公钥之间的对应关系中，获取设备标识对应的公钥；

[0152] 中转服务器将公钥及第一交互信息发送至目标服务器地址对应的目标服务器；

[0153] 目标服务器根据公钥对生成的第二随机数进行加密，得到第一密文；

[0154] 目标服务器将第一密文发送至中转服务器，由中转服务器发送至终端；

[0155] 终端将第一密文发送至安全设备；

[0156] 安全设备根据存储的私钥对第一密文进行解密，得到第二随机数；

[0157] 安全设备将第二随机数发送至终端。

[0158] 在本公开的另一个实施例中，中转服务器根据设备标识，从设备标识与公钥之间的对应关系中，获取设备标识对应的公钥之前，方法还包括：

[0159] 安全设备接收设备生产商发送的密钥生成请求；

[0160] 基于密钥生成请求，安全设备生成一对非对称密钥，非对称密钥包括公钥和私钥；

[0161] 安全设备存储私钥，并将公钥与设备标识发送至中转服务器；

[0162] 基于接收到的公钥与设备标识，中转服务器存储公钥与设备标识之间的对应关系。

[0163] 在本公开的另一个实施例中，验证请求中还携带终端支持的加密算法信息、终端

支持的签名算法信息，方法还包括：

[0164] 目标服务器根据本端支持的加密算法及终端支持的加密算法信息，确定指定加密算法；

[0165] 目标服务器根据本端支持的签名算法及终端支持的签名算法信息，确定指定签名算法；

[0166] 目标服务器向中转服务器发送通知消息，由中转服务器将通知消息发送至终端，通知消息用于通知终端将指定加密算法作为加密算法、将指定签名算法作为签名算法。

[0167] 在本公开的另一个实施例中，目标服务器向中转服务器发送通知消息之后，方法还包括：

[0168] 在终端与中转服务器、目标服务器与中转服务器之间的交互过程中，指定加密算法用于对待发送的交互数据进行加密运算，指定签名算法用于对待发送的交互数据进行签名运算。

[0169] 在本公开的另一个实施例中，终端基于与中转服务器之间的交互数据进行校验，得到第一校验值，包括：

[0170] 终端按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第一拼接结果；

[0171] 终端采用指定校验算法对第一拼接结果进行校验，得到第一校验值。

[0172] 在本公开的另一个实施例中，目标服务器基于与中转服务器之间的交互数据进行校验，得到第二校验值，包括：

[0173] 目标服务器按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第二拼接结果；

[0174] 目标服务器采用指定校验算法对第二拼接结果进行校验，得到第二校验值。

[0175] 在本公开的另一个实施例中，基于主密钥、第一校验值及第二校验值，终端与目标服务器彼此进行安全验证，包括：

[0176] 终端根据终端签名密钥，对第一校验值进行签名，得到第一签名信息；

[0177] 终端根据终端密钥，对第一签名信息进行加密，得到第一加密信息；

[0178] 终端将第一加密信息发送至中转服务器，由中转服务器将第一加密信息发送至目标服务器；

[0179] 目标服务器根据本地存储的终端密钥，对第一加密信息进行解密；

[0180] 当对第一签名信息成功解密时，目标服务器获取第一签名信息；

[0181] 目标服务器根据本地存储的终端签名密钥，对第一签名信息的签名进行验证；

[0182] 当对第一签名信息的签名成功验证时，目标服务器获取第一校验值；

[0183] 目标服务器将第一校验值与第二校验值进行比对；

[0184] 如果第一校验值与第二校验值一致，则目标服务器生成验证成功信息；

[0185] 目标服务器根据服务器签名密钥，对验证成功信息进行签名，得到第二签名信息；

[0186] 目标服务器根据服务器密钥，对第二签名信息进行加密，得到第二加密信息；

[0187] 目标服务器将第二加密信息发送至中转服务器，由中转服务器将第二加密信息发送至终端；

[0188] 终端根据本地存储的服务器密钥，对第二加密信息进行解密；

[0189] 当对第二加密信息成功解密时，终端获取第二签名信息；

[0190] 终端根据本地存储的服务器签名密钥，对第二签名信息的签名进行验证；

[0191] 当对第二签名信息的签名成功验证时，终端确定与目标服务器彼此通过安全验证。

[0192] 在本公开的另一个实施例中，该方法应用于安全设备、终端、中转服务器及目标服务器进行数值转移的场景。

[0193] 上述所有可选技术方案，可以采用任意结合形成本公开的可选实施例，在此不再一一赘述。

[0194] 图 2 是根据一示例性实施例示出的一种安全验证方法的流程图，如图 2 所示，安全验证方法应用于安全设备、终端、目标服务器及中转服务器进行数值转移的场景中，包括以下步骤。

[0195] 在步骤 201 中，终端向中转服务器发送验证请求，该验证请求中至少携带第一交互信息，该第一交互信息至少包括终端对应的安全设备的设备标识、第一随机数及目标服务器的地址。

[0196] 随着互联网技术的发展，网络购物作为一种新的购物形式，成为用户购物的首选方式。在网络购物场景下，当用户通过互联网访问购物网站，查找到心仪物品之后，为了获取到该物品，用户需要从账户中转移相应的数值给商家。由于用户账户具有较高的价值，在数值转移过程中，如果运行环境并不安全，可能会导致用户账户被盗取，这不仅会使用户蒙受巨大的经济损失，而且用户重要的个人信息也会随之丢失，给用户带来极大的安全隐患。

[0197] 在数值转移场景下，为了保证用户账户安全，通常会为每个用户账户配备一个安全设备，该安全设备是指具有独立运算资源、有严格的数据访问权限的运行环境，该安全设备可以为金融领域使用的安全芯片等，例如 SE(Secure Element，安全元件）、TEE(Trusted Execution Environment，可信任执行环境）、eUICC(Embedded Universal Integrated Circuit Card，嵌入式通用集成电路卡）等。在数值转移过程中，安全设备需要插入到终端中进行使用。

[0198] 在本实施例中，安全设备中存储着用于对数值转移场景的运行环境进行验证的公钥，该公钥由设备生产商在安全设备的生产过程中触发安全设备生成。关于设备生产商在安全设备的生产过程中触发安全设备的方式，包括但不限于：在安全设备的生产过程中，设备生产商向安全设备发送密钥生成请求，当接收到该密钥生成请求时，在该密钥生成请求的触发下，安全设备生成一对非对称密钥，该非对称密钥由公钥和私钥组成。之后，安全设备存储该非对称密钥中的私钥，并将设备标识及公钥发送给中转服务器。当接收安全设备发送的公钥和设备标识，中转服务器将存储公钥与设备标识之间的对应关系。

[0199] 在数值转移场景下，为了保证用户账户安全，当终端接收到数值转移指令时，终端将生成第一随机数，进而基于该第一随机数对当前的运行环境进行验证。其中，终端具有网络连接功能，可通过有线网络、无线网络与中转服务器进行交互。该终端可以为 POS 机、手机、电脑等，本实施例不对终端作具体的限定。

[0200] 终端基于该第一随机数对当前的运行环境进行验证时，可先向中转服务器发送验证请求，该验证请求中至少携带第一交互信息。该第一交互信息至少包括安全设备的设备

标识、第一随机数、目标服务器的地址。当然，验证请求中还可以携带终端支持的加密算法信息、终端支持的签名算法信息，该加密算法信息中携带了终端能够使用的加密算法的相关信息，例如，加密算法的版本号、加密算法的名称等等，该签名信息中携带了终端能够使用的签名算法的相关信息，例如，签名算法的版本号、签名算法的名称等等。

[0201] 在步骤 202 中，当接收到验证请求，中转服务器根据设备标识，从设备标识与公钥之间的对应关系中，获取设备标识对应的公钥。

[0202] 当接收到终端发送的验证请求，基于预先存储的设备标识与公钥之间的对应关系，中转设备可以获取安全设备的设备标识对应的公钥。

[0203] 在步骤 203 中，中转服务器将公钥及第一交互信息发送至目标地址对应的目标服务器。

[0204] 由于在本实施例中的中转服务器具有对数据读取、发送功能，不具有对数据的验证功能，因此，当获取到公钥之后，中转服务器会将公钥、第一交互信息以及终端支持的加密算法信息、终端支持的签名算法信息等一同发送至目标地址对应的目标服务器，由目标服务器进行验证。

[0205] 在步骤 204 中，当接收到公钥及第一交互信息，目标服务器确定指定加密算法及指定签名算法，并根据公钥对生成的第二随机数进行加密，得到第一密文。

[0206] 由于终端和目标服务器支持的加密算法可能是不同的，因此，当接收到终端支持的加密算法信息，目标服务器需要根据本端支持的加密算法及终端支持的加密算法信息，确定一个指定加密算法，该指定加密算法应为目标服务器与终端均支持的加密算法。在具体确定时，目标服务器可先将本端支持的加密算法与终端支持的加密算法进行比对，通过比对从中选取二者均支持的加密算法，之后，按照选取标准，从中选取满足需求的加密算法作为指定加密算法。其中，目标服务器选取指定加密算法的选取标准可以为加密时长，还可以为加密精度等。例如，终端支持的加密算法为加密算法 A、加密算法 B、加密算法 C 及加密算法 D，目标服务器支持的加密算法为加密算法 A、加密算法 D、加密算法 E，通过对终端支持的加密算法和本端支持的加密算法进行比对，服务器从中选取出二者均支持的加密算法为加密算法 A、加密算法 D，其中，加密算法 A 的加密精度较低、加密时间较短，加密算法 D 的加密精度较高、加密时间较长，如果设定的选取标准为加密精度，则目标服务器可选取加密算法 D 作为指定加密算法。

[0207] 由于终端和目标服务器支持的签名算法可能是不同的，因此，当接收到终端支持的签名算法信息，目标服务器需要根据本端支持的签名算法及终端支持的签名算法信息，确定一个指定签名算法，该指定签名算法应为目标服务器与终端均支持的签名算法。在具体确定时，目标服务器可先将本端支持的签名算法与终端支持的签名算法进行比对，通过比对从中选取二者均支持的签名算法，之后，按照选取标准，从中选取满足需求的签名算法作为指定签名算法。其中，目标服务器选取指定签名算法的选取标准可以为签名时长，还可以为加密精度等。例如，终端支持的签名算法为签名算法 A、签名算法 B、签名算法 C 及签名算法 D，目标服务器支持的签名算法为签名算法 B、签名算法 D、签名算法 E，通过对终端支持的签名算法和本端支持的签名算法进行比对，服务器从中选取出二者均支持的签名算法为签名算法 B、签名算法 D，其中，签名算法 B 的加密精度较高、签名时间较短，签名算法 D 的加密精度较低、签名时间较长，如果设定的选取标准为加密精度，则目标服务器可选取签名算

法 B 作为指定签名算法。

[0208] 另外，当接收到上述信息时，目标服务器还将生成一个第二随机数，并根据接收到的公钥对生成的第二随机数进行加密，得到第一密文。

[0209] 在步骤 205 中，目标服务器向中转服务器发送第一密文及通知消息，该公知消息用于通知终端将指定加密算法作为加密算法、将指定签名算法作为签名算法。

[0210] 当确定了指定加密算法及指定签名算法，目标服务器还将生成通知消息，该通知消息用于通知终端将指定签名算法作为加密算法、将指定签名算法作为签名算法。进一步地，目标服务器还将第一密文及通知消息发送至中转服务器。

[0211] 在步骤 206 中，当接收到第一密文及通知消息，中转服务器将该第一密文及通知消息发送给终端。

[0212] 当接收到第一密文及通知消息时，中转服务器将接收到的第一密文及通知消息发送给终端。

[0213] 在步骤 207 中，当接收到第一密文及通知消息，终端根据通知消息将指定短发确定为加密算法、将指定签名算法确定为签名算法，并将第一密文发送至安全设备。

[0214] 当接收到通知消息时，终端根据通知消息，将指定加密算法确定为加密算法、将指定签名算法确定为签名算法，进而在终端与中转服务器、目标服务器与中转服务器之间的交互过程中，均使用该指定加密算法对待发送的交互数据进行加密运算，使用该指定签名算法对待发送的交互数据进行签名运算。

[0215] 由于非对称密钥中的私钥存储在安全设备中，当接收到第一密文，终端无法对接收到的第一密文进行解密。为了获取到第一密文中的对应明文，终端需要将第一密文发送至安全设备，由安全设备进行解密。

[0216] 在步骤 208 中，当接收到第一密文，安全设备根据预先存储的私钥对第一密文进行解密，得到第二随机数。

[0217] 基于存储的私钥，安全设备在接收到第一密文之后，即可对第一密文进行解密，从而得到第一密文对应的明文，也即是第二随机数。

[0218] 在步骤 209 中，安全设备将第二随机数发送至终端。

[0219] 由于安全设备插入在终端中，因此，安全设备在将第二随机数发送至终端时，无需借助网络，可直接发送。

[0220] 在步骤 210 中，当接收到第二随机数，终端根据第一随机数和第二随机数，生成主密钥，并基于与中转服务器之间的交互数据进行校验，得到第一校验值。

[0221] 基于生成的第一随机数及接收到的第二随机数，终端可采用密钥生成算法对第一随机数和第二随机数进行计算，得到一个主密钥。在得到主密钥之后，终端还需要对该主密钥进行分解。在此过程中，该主密钥至少可分解为终端密钥、服务器密钥、终端签名密钥、服务器签名密钥。在终端与中转服务器的交互过程中，终端可使用终端密钥对待发送数据进行加密，使用终端签名密钥对待发送数据进行签名；终端可使用服务器密钥对接收到的数据进行解密，使用服务器签名密钥对接收到的数据的签名进行验证。

[0222] 除了上述终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，终端还可将主密钥分解为终端加密初始向量、服务器加密初始向量。在终端与中转服务器、目标服务器与中转服务器的交互过程中，该终端加密初始向量可用于终端在使用指定加密算法及终端加

密密钥进行加密时，确定加密初始值；该服务器加密初始向量可用于服务器在使用指定加密算法及服务器加密密钥进行加密时，确定加密初始值。

[0223] 另外，终端通过对与中转服务器之间的交互数据进行校验，可得到第一校验值。其中，终端与中转服务器之间的交互数据既包括终端向中转服务器发送的数据，也包括终端从中转服务器接收到的数据。终端在对与中转服务器之间的交互数据进行校验时，可先按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第一拼接结果，然后采用指定校验算法对第一拼接结果进行校验，得到第一校验值。其中，指定校验算法可以为PRF(Pseudo Random Function，伪随机函数）等，本实施例不对指定校验算法作具体的限定。

[0224] 在步骤211中，目标服务器根据第一随机数和第二随机数，生成主密钥，并基于与中转服务器之间的交互数据进行校验，得到第二校验值。

[0225] 基于生成的第二随机数及接收到的第一随机数，目标服务器可采用密钥生成算法对第一随机数和第二随机数进行计算，得到一个主密钥。在得到主密钥之后，目标服务器还需要对该主密钥进行分解。在此过程中，该主密钥至少可分解为终端密钥、服务器密钥、终端签名密钥、服务器签名密钥。在目标服务器与中转服务器的交互过程中，目标服务器可使用服务器密钥对待发送数据进行加密，使用服务器签名密钥对待发送数据进行加密；目标服务器可使用终端密钥对接收到的数据进行解密，使用终端签名密钥对接收到的数据的签名进行验证。

[0226] 除了上述终端密钥、服务器密钥、终端签名密钥、服务器签名密钥，目标服务器还可将主密钥分解为终端加密初始向量、服务器加密初始向量。在终端与中转服务器、目标服务器与中转服务器的交互过程中，该终端加密初始向量可用于终端在使用指定加密算法及终端加密密钥进行加密时，确定加密初始值；该服务器加密初始向量可用于服务器在使用指定加密算法及服务器加密密钥进行加密时，确定加密初始值。

[0227] 另外，目标服务器通过对与中转服务器之间的交互数据进行校验，可得到第二校验值。其中，目标服务器与中转服务器之间的交互数据既包括目标服务器向中转服务器发送的数据，也包括目标服务器从中转服务器接收到的数据。目标服务器在对与中转服务器之间的交互数据进行校验时，可先按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第二拼接结果，然后采用指定校验算法对第二拼接结果进行校验，得到第二校验值。该指定校验算法与终端在对与中转服务器之间的交互数据进行校验时采用的校验算法相同，可以为PRF函数等。

[0228] 需要说明的是，上述终端根据第一随机数和第二随机数，生成第一校验值的过程，以及目标服务器根据第一随机数和第二随机随机数，生成第二校验值的过程，可以同时进行，也可以为不同时进行，本实施例仅将终端根据第一随机数和第二随机数，生成第一校验值作为步骤210，将目标服务器根据第一随机数和第二随机随机数，生成第二校验值作为步骤211为例进行说明，上述步骤210和上述步骤211并不代表具体的执行顺序。

[0229] 在步骤212中，基于主密钥、第一校验值和第二校验值，终端与目标服务器彼此进行安全验证。

[0230] 基于主密钥、第一校验值及第二校验值，终端与目标服务器彼此进行安全验证时，可分为目标服务器对终端的安全验证过程及终端对目标服务器的安全验证过程。

[0231] 关于目标服务器对终端的安全验证过程，可参见下述步骤（1）～（8）：

[0232] （1）、终端根据终端签名密钥，对第一校验值进行签名，得到第一签名信息。

[0233] 为了提高传输的数据安全，终端在获取到第一校验值之后，还将采用指定签名算法，根据主密钥分解得到的终端签名密钥，对第一校验值进行签名。通过对第一校验值进行签名，可得到第一签名信息。

[0234] （2）、终端根据终端密钥，对第一签名信息进行加密，得到第一加密信息。

[0235] 终端还将采用指定加密算法，根据主密钥分解得到的终端密钥，对第一签名信息进行加密，以得到第一加密信息。

[0236] （3）、终端将第一加密信息发送至中转服务器，由中转服务器将第一加密信息发送至目标服务器。

[0237] 终端将第一加密信息发送至中转服务器的方式，包括但不限于通过有线网络或无线网络的方式将第一加密信息发送至中转服务器，本实施例对此不作具体的限定。当中转服务器接收到的第一加密信息之后，中转服务器还将第一加密信息发送至目标服务器。

[0238] （4）、目标服务器根据本地存储的终端密钥，对第一加密信息进行解密。

[0239] 当接收到的第一加密信息，目标服务器将根据本地存储的终端密钥，对第一加密信息进行解密，如果发送第一加密信息的终端为合法终端，则目标服务器根据本地存储的终端密钥，可对第一加密信息成功解密；如果发送第一加密信息的终端为不合法终端，则目标服务器根据本地存储的终端密钥，不能对第一加密信息成功解密。

[0240] （5）、当对第一签名信息成功解密时，目标服务器获取第一签名信息。

[0241] （6）、目标服务器根据本地存储的终端签名密钥，对第一签名信息的签名进行验证。

[0242] 为了进一步保证终端的合法性，目标服务器还将根据本地存储的终端签名密钥，对第一签名信息的签名进行验证。

[0243] （7）当对第一签名信息的签名成功验证时，目标服务器获取第一校验值。

[0244] （8）、目标服务器将第一校验值与第二校验值进行比对，如果第一校验值与第二校验值一致，则目标服务器确定对终端的校验通过，并生成验证成功信息。

[0245] 在目标服务器将第一校验值与第二校验值进行比对，如果第一校验值与第二校验值一致，说明终端与中转服务器之间的交互数据以及目标服务器与中转服务器之间的交互数据相同，也即是，该终端为本次目标服务器需要进行数据交互的终端，此时目标服务器确定对终端的校验通过，同时生成验证成功信息。

[0246] 关于终端对目标服务器的安全验证过程，可参见下述步骤（1）～（7）：

[0247] （1）、目标服务器根据服务器签名密钥，对验证成功信息进行签名，得到第二签名信息。

[0248] 基于生成的验证成功信息，目标服务器还将采用指定加密算法，根据主密钥分解得到的服务器密钥，对验证成功信息进行加密，从而得到第二签名信息。

[0249] （2）、目标服务器根据服务器密钥，对第二签名信息进行加密，得到第二加密信息。

[0250] 目标服务器还将采用指定加密算法，根据主密钥分解得到的服务器密钥，对第二签名信息进行加密，从而得到第二加密信息。

[0251] （3）、目标服务器将第二加密信息发送至中转服务器，由中转服务器将第二加密信

息发送至终端。

[0252] 目标服务器将第二加密信息发送至中转服务器的方式，包括但不限于目标服务器通过有线网络或无线网络的方式将第二加密信息发送至中转服务器等，本实施例对此不作具体的限定。当中转服务器接收到的第二加密信息之后，中转服务器还将第二加密信息发送至终端。

[0253] (4)、终端根据本地存储的服务器密钥，对第二加密信息进行解密。

[0254] 当接收到的第二加密信息，终端将根据本地存储的服务器密钥，对第二加密信息进行解密，如果发送第二加密信息的目标服务器为合法服务器，则终端根据本地存储的服务器密钥，可对第二加密信息成功解密；如果发送第二加密信息的目标服务器为不合法服务器，则终端器根据本地存储的服务器密钥，不能对第二加密信息成功解密。

[0255] (5)、当对第二加密信息成功解密时，终端获取第二签名信息。

[0256] (6)、终端根据本地存储的服务器签名密钥，对第二签名信息的签名进行验证。

[0257] 为了进一步保证目标服务器的合法性，终端还将根据本地存储的服务器签名密钥，对第二签名信息的签名进行验证。

[0258] (7)、当对第二签名信息的签名成功验证时，终端确定与目标服务器彼此通过安全验证。

[0259] 当终端与目标服务器彼此通过安全验证之后，终端即可安全地与目标服务器进行交互，在交互过程中包括如下步骤：

[0260] 终端经过中转服务器向目标服务器发送的所有数据，都需要使用指定加密算法及终端加密密钥进行加密，并使用指定签名算法及终端签名密钥进行签名；

[0261] 目标服务器经过中转服务器向终端发送的所有数据，都需要使用指定加密算法及服务器加密密钥进行加密，并使用指定签名算法及服务器签名密钥进行签名。

[0262] 本发明实施例提供的方法，终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0263] 图 3 是根据一示例性实施例示出的一种安全验证系统的装置结构示意图。参照图 3，该系统包括：终端 301、目标服务器 302 及中转服务器 303。

[0264] 该终端 301 被配置为目标服务器根据第一随机数和第二随机数，生成主密钥；

[0265] 该目标服务器 302 被配置为根据第一随机数和第二随机数，生成主密钥；

[0266] 该终端 301 被配置为基于与中转服务器 303 之间的交互数据进行校验，得到第一校验值；

[0267] 该目标服务器 302 被配置为基于与中转服务器 302 之间的交互数据进行校验，得到第二校验值；

[0268] 该终端 301 被配置为基于主密钥、第一校验值及第二校验值，与目标服务器 303 进行安全验证；

[0269] 该目标服务器 302 被配置为基于主密钥、第一校验值及第二校验值，与终端进行安全验证。

[0270] 在本公开的另一个实施例中，主密钥至少包括终端密钥、服务器密钥、终端签名密

钥、服务器签名密钥，在终端与中转服务器、目标服务器与中转服务器的交互过程中包括以下步骤：

[0271] 终端 301 使用终端密钥对待发送数据进行加密，终端 301 使用终端签名密钥对待发送数据进行签名；

[0272] 目标服务器 302 使用服务器密钥对待发送数据进行加密，目标服务器 302 使用服务器签名密钥对待发送数据进行加密；

[0273] 终端 301 使用服务器密钥对接收到的数据进行解密，终端 301 使用服务器签名密钥对接收到的数据的签名进行验证；

[0274] 目标服务器 302 使用终端密钥对接收到的数据进行解密，目标服务器 302 使用终端签名密钥对接收到的数据的签名进行验证。

[0275] 参见图 4，该系统还包括：安全设备 304。

[0276] 该终端 301 被配置为向中转服务器 303 发送验证请求，验证请求中至少携带第一交互信息，第一交互信息至少包括终端对应的安全设备的设备标识、第一随机数及目标服务器的地址；

[0277] 该中转服务器 303 被配置为根据设备标识，从设备标识与公钥之间的对应关系中，获取设备标识对应的公钥；

[0278] 该中转服务器 303 被配置为将公钥及第一交互信息发送至目标服务器地址对应的目标服务器；

[0279] 该目标服务器 302 被配置为根据公钥对生成的第二随机数进行加密，得到第一密文；

[0280] 该目标服务器 302 被配置为将第一密文发送至中转服务器，由中转服务器发送至终端；

[0281] 该终端 301 被配置为将第一密文发送至安全设备；

[0282] 该安全设备 304 被配置为根据存储的私钥对第一密文进行解密，得到第二随机数；

[0283] 该安全设备 304 被配置为将第二随机数发送至终端。

[0284] 在本公开的另一个实施例中，该安全设备 304 被配置为接收设备生产商发送的密钥生成请求；

[0285] 该安全设备 304 被配置为基于密钥生成请求，生成一对非对称密钥，非对称密钥包括公钥和私钥；

[0286] 该安全设备 304 被配置为存储私钥，并将公钥与设备标识发送至中转服务器 303；

[0287] 基于接收到的公钥与设备标识，中转服务器 303 存储公钥与设备标识之间的对应关系。

[0288] 在本发明的另一个实施例中，验证请求中还携带终端支持的加密算法信息、终端支持的签名算法信息；

[0289] 该目标服务器 302 被配置为根据本端支持的加密算法及终端支持的加密算法信息，确定指定加密算法；

[0290] 该目标服务器 302 被配置为根据本端支持的签名算法及终端支持的签名算法信息，确定指定签名算法；

[0291] 该目标服务器 302 被配置为向中转服务器发送通知消息，由中转服务器将通知消息发送至终端，通知消息用于通知终端将指定加密算法作为加密算法、将指定签名算法作为签名算法。

[0292] 在本公开的另一个实施例中，在终端 301 与中转服务器 303、目标服务器 302 与中转服务器 303 之间的交互过程中，指定加密算法用于对待发送的交互数据进行加密运算，指定签名算法用于对待发送的交互数据进行签名运算。

[0293] 在本公开的另一个实施例中，该终端 301 被配置为按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第一拼接结果；

[0294] 该终端 301 被配置为采用指定校验算法对第一拼接结果进行校验，得到第一校验值。

[0295] 在本公开的另一个实施例中，该目标服务器 302 被配置为按照时间顺序，将与中转服务器之间的交互数据进行拼接，得到第二拼接结果；

[0296] 该目标服务器 302 被配置为采用指定校验算法对第二拼接结果进行校验，得到第二校验值。

[0297] 在本公开的另一个实施例中，该终端 301 被配置为根据终端签名密钥，对第一校验值进行签名，得到第一签名信息；

[0298] 该终端 301 被配置为根据终端密钥，对第一签名信息进行加密，得到第一加密信息；

[0299] 该终端 301 被配置为将第一加密信息发送至中转服务器，由中转服务器将第一加密信息发送至目标服务器；

[0300] 该目标服务器 302 被配置为根据本地存储的终端密钥，对第一加密信息进行解密；

[0301] 该目标服务器 302 被配置为当对第一签名信息成功解密时，获取第一签名信息；

[0302] 该目标服务器 302 被配置为根据本地存储的终端签名密钥，对第一签名信息的签名进行验证；

[0303] 该目标服务器 302 被配置为当对第一签名信息的签名成功验证时，获取第一校验值；

[0304] 该目标服务器 302 被配置为将第一校验值与第二校验值进行比对；

[0305] 该目标服务器 302 被配置为当第一校验值与第二校验值一致时，生成验证成功信息；

[0306] 该目标服务器 302 被配置为根据服务器签名密钥，对验证成功信息进行签名，得到第二签名信息；

[0307] 该目标服务器 302 被配置为根据服务器密钥，对第二签名信息进行加密，得到第二加密信息；

[0308] 该目标服务器 302 被配置为将第二加密信息发送至中转服务器，由中转服务器将第二加密信息发送至终端；

[0309] 该终端 301 被配置为根据本地存储的服务器密钥，对第二加密信息进行解密；

[0310] 该终端 301 被配置为当对第二加密信息成功解密时，获取第二签名信息；

[0311] 该终端 301 被配置为根据本地存储的服务器签名密钥，对第二签名信息的签名进

行验证；

[0312] 该终端 301 被配置为当对第二签名信息的签名成功验证时，确定与目标服务器彼此通过安全验证。

[0313] 在本公开的另一个实施例中，该系统用于安全设备 304、终端 301、目标服务器 302 及中转服务器 303 进行数值转移的场景。

[0314] 本公开实施例提供的系统，终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0315] 关于上述实施例中的系统，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0316] 图 5 是根据一示例性实施例示出的一种用于安全验证的装置 500 的框图。例如，装置 500 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

[0317] 参照图 5，装置 500 可以包括以下一个或多个组件：处理组件 502，存储器 504，电源组件 506，多媒体组件 508，音频组件 510，输入 / 输出 (I/O) 接口 512，传感器组件 514，以及通信组件 516。

[0318] 处理组件 502 通常控制装置 500 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 502 可以包括一个或多个处理器 520 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 502 可以包括一个或多个模块，便于处理组件 502 和其他组件之间的交互。例如，处理组件 502 可以包括多媒体模块，以方便多媒体组件 508 和处理组件 508 之间的交互。

[0319] 存储器 504 被配置为存储各种类型的数据以支持在装置 500 的操作。这些数据的示例包括用于在装置 500 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 504 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器 (SRAM)，电可擦除可编程只读存储器 (EEPROM)，可擦除可编程只读存储器 (EPROM)，可编程只读存储器 (PROM)，只读存储器 (ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0320] 电源组件 506 为装置 500 的各种组件提供电力。电源组件 506 可以包括电源管理系统，一个或多个电源，及其他与为装置 500 生成、管理和分配电力相关联的组件。

[0321] 多媒体组件 508 包括在所述装置 500 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器 (LCD) 和触摸面板 (TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 508 包括一个前置摄像头和 / 或后置摄像头。当装置 500 处于操作模式，如拍摄模式或视频模式时，前置摄像头和 / 或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0322] 音频组件 510 被配置为输出和 / 或输入音频信号。例如，音频组件 510 包括一个

麦克风 (MIC)，当装置 500 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 504 或经由通信组件 516 发送。在一些实施例中，音频组件 510 还包括一个扬声器，用于输出音频信号。

[0323] I/O 接口 512 为处理组件 502 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

[0324] 传感器组件 514 包括一个或多个传感器，用于为装置 500 提供各个方面的状态评估。例如，传感器组件 514 可以检测到装置 500 的打开 / 关闭状态，组件的相对定位，例如所述组件为装置 500 的显示器和小键盘，传感器组件 514 还可以检测装置 500 或装置 500 一个组件的位置改变，用户与装置 500 接触的存在或不存在，装置 500 方位或加速 / 减速和装置 500 的温度变化。传感器组件 514 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 514 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 514 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

[0325] 通信组件 516 被配置为便于装置 500 和其他设备之间有线或无线方式的通信。装置 500 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 516 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 516 还包括近场通信 (NFC) 模块，以促进短程通信。例如，在 NFC 模块可基于射频识别 (RFID) 技术，红外数据协会 (IrDA) 技术，超宽带 (UWB) 技术，蓝牙 (BT) 技术和其他技术来实现。

[0326] 在示例性实施例中，装置 500 可以被一个或多个应用专用集成电路 (ASIC)、数字信号处理器 (DSP)、数字信号处理设备 (DSPD)、可编程逻辑器件 (PLD)、现场可编程门阵列 (FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

[0327] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 504，上述指令可由装置 500 的处理器 520 执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0328] 一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种上述安全验证方法中安全设备或终端所执行的功能。

[0329] 本公开实施例提供的非临时性计算机可读存储介质，终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0330] 图 6 是根据一示例性实施例示出的一种用于安全验证的装置 600 的框图。例如，装置 600 可以被提供为一服务器。参照图 6，装置 500 包括处理组件 622，其进一步包括一个或多个处理器，以及由存储器 632 所代表的存储器资源，用于存储可由处理组件 622 的执行的指令，例如应用程序。存储器 632 中存储的应用程序可以包括一个或一个以上的每一

个对应于一组指令的模块。此外，处理组件 622 被配置为执行指令，以执行上述方法安全验证方法中中转服务器或目标服务器所执行的功能。

[0331] 装置 600 还可以包括一个电源组件 626 被配置为执行装置 600 的电源管理，一个有线或无线网络接口 650 被配置为将装置 600 连接到网络，和一个输入输出 (I/O) 接口 658。装置 1900 可以操作基于存储在存储器 632 的操作系统，例如 Windows ServerTM，Mac OS XTM，UnixTM，LinuxTM，FreeBSDTM 或类似。

[0332] 本公开实施例提供的装置，终端和目标服务器在彼此进行安全验证时，并不仅依赖于由第一随机数和第二随机数生成的主密钥，而是根据校验值及主密钥协同进行校验，由于该校验值是根据数据验证过程中与中转服务器之间的交互数据生成的，其他终端即使获取到主密钥，也无法获取到校验值，因而有效地保证了数据安全。

[0333] 本领域技术人员在考虑说明书及实践这里公开的公开后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

[0334] 应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

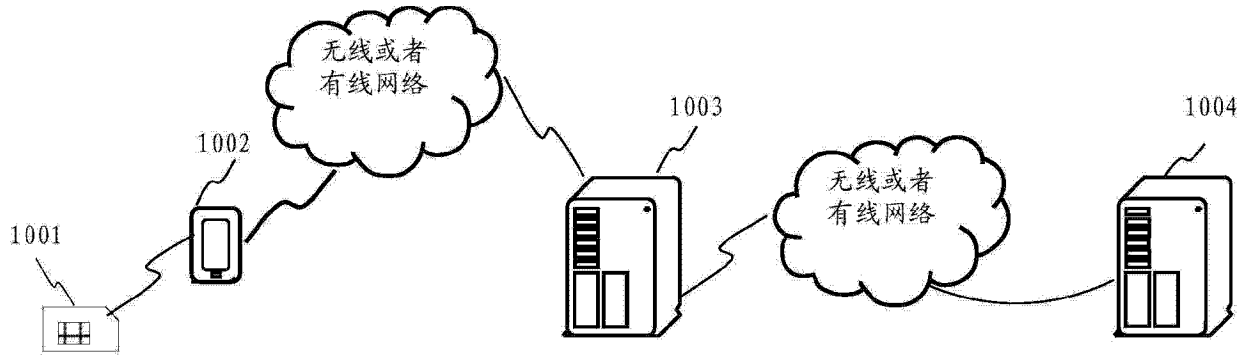

无线或者
有线网络
1002
1003
1004
1001
无线或者
有线网络

图 1A

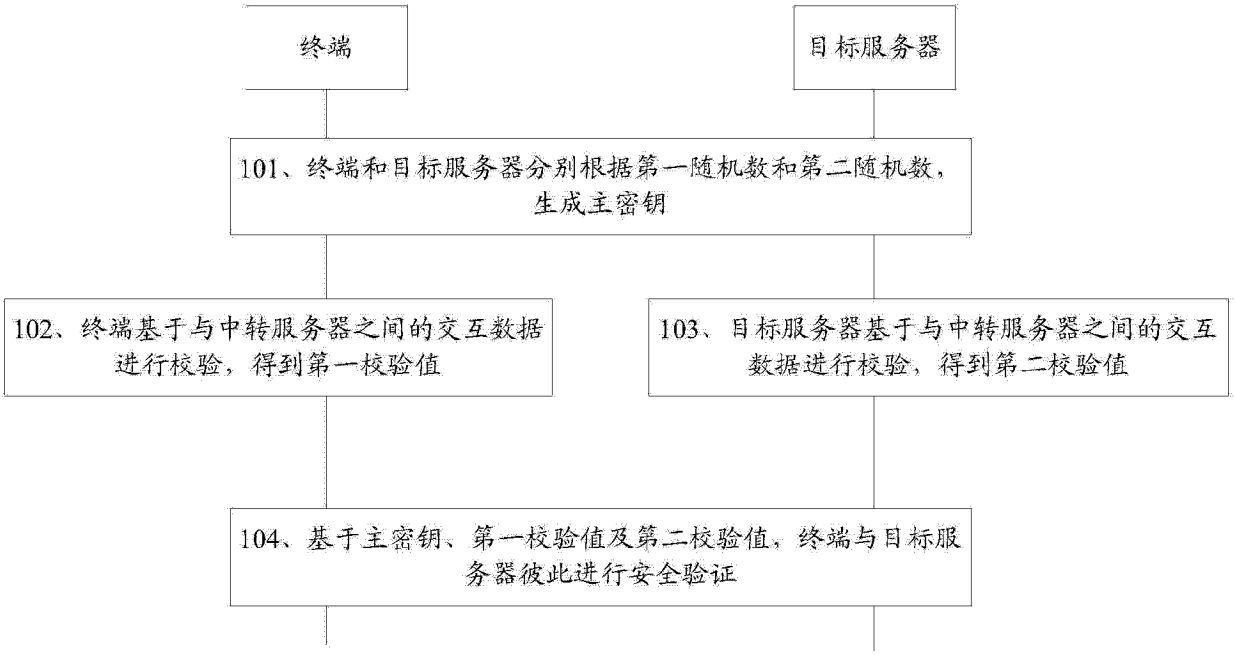

终端
目标服务器
101、终端和目标服务器分别根据第一随机数和第二随机数，生成主密钥
102、终端基于与中转服务器之间的交互数据进行校验，得到第一校验值
103、目标服务器基于与中转服务器之间的交互数据进行校验，得到第二校验值
104、基于主密钥、第一校验值及第二校验值，终端与目标服务器彼此进行安全验证

图 1

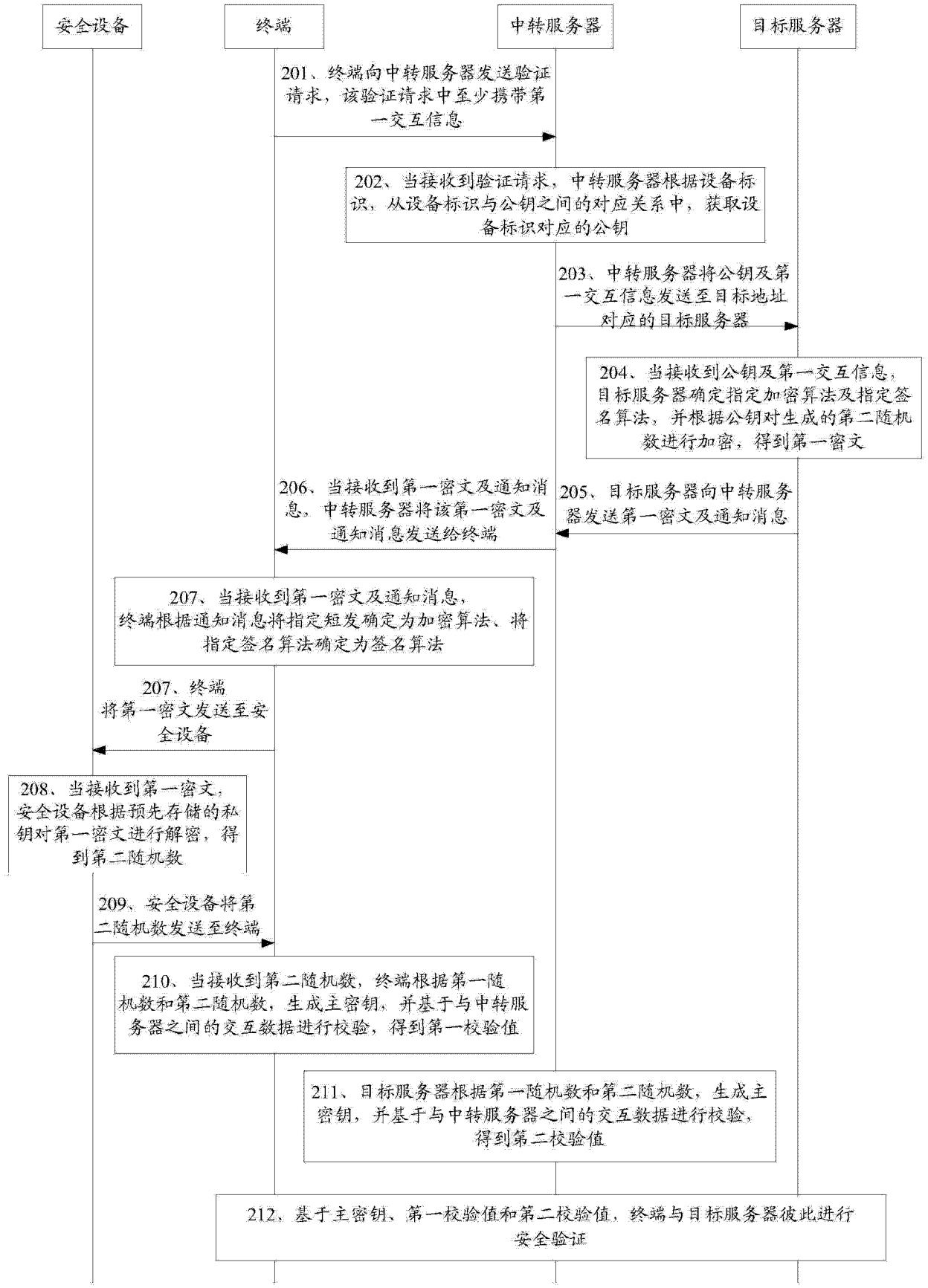

安全设备
终端
中转服务器
目标服务器
201、终端向中转服务器发送验证请求，该验证请求中至少携带第一交互信息
202、当接收到验证请求，中转服务器根据设备标识，从设备标识与公钥之间的对应关系中，获取设备标识对应的公钥
203、中转服务器将公钥及第一交互信息发送至目标地址对应的目标服务器
204、当接收到公钥及第一交互信息，目标服务器确定指定加密算法及指定签名算法，并根据公钥对生成的第二随机数进行加密，得到第一密文
205、目标服务器向中转服务器发送第一密文及通知消息
206、当接收到第一密文及通知消息，中转服务器将该第一密文及通知消息发送给终端
207、当接收到第一密文及通知消息，终端根据通知消息将指定短发确定为加密算法、将指定签名算法确定为签名算法
207、终端将第一密文发送至安全设备
208、当接收到第一密文，安全设备根据预先存储的私钥对第一密文进行解密，得到第二随机数
209、安全设备将第二随机数发送至终端
210、当接收到第二随机数，终端根据第一随机数和第二随机数，生成主密钥，并基于与中转服务器之间的交互数据进行校验，得到第一校验值
211、目标服务器根据第一随机数和第二随机数，生成主密钥，并基于与中转服务器之间的交互数据进行校验，得到第二校验值
212、基于主密钥、第一校验值和第二校验值，终端与目标服务器彼此进行安全验证

图 2

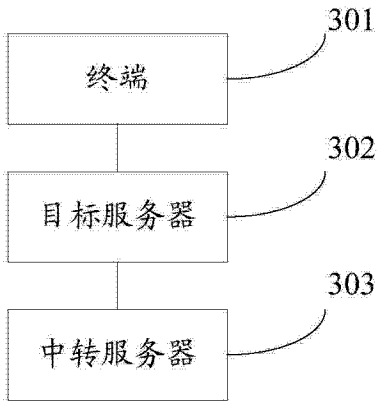


图 3

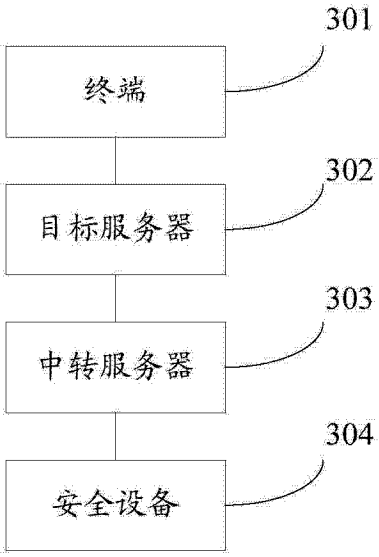


图 4

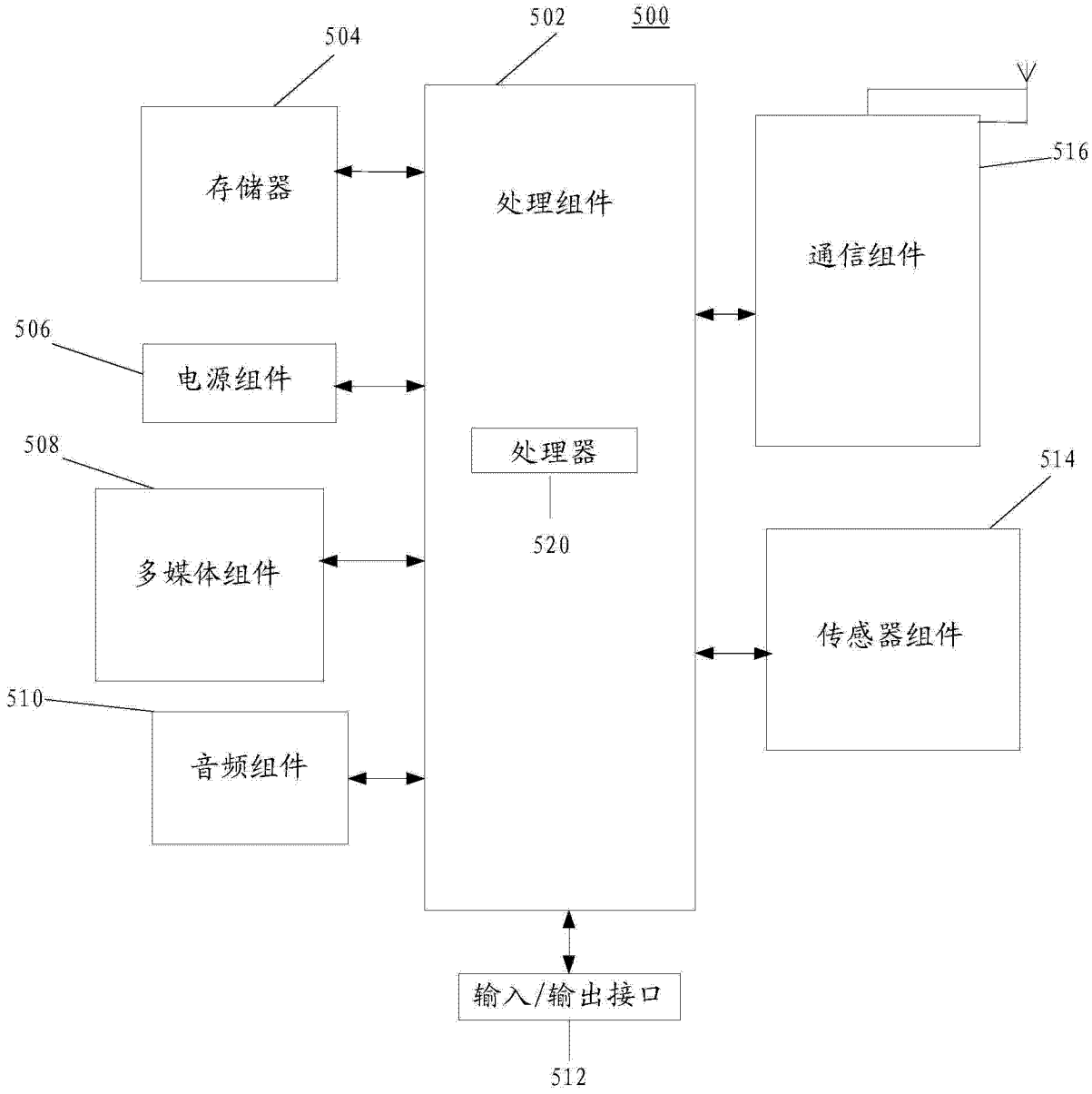

502
500
504
存储器
处理组件
通信组件
516
506
电源组件
处理器
520
508
多媒体组件
514
传感器组件
510
音频组件
输入/输出接口
512

图 5

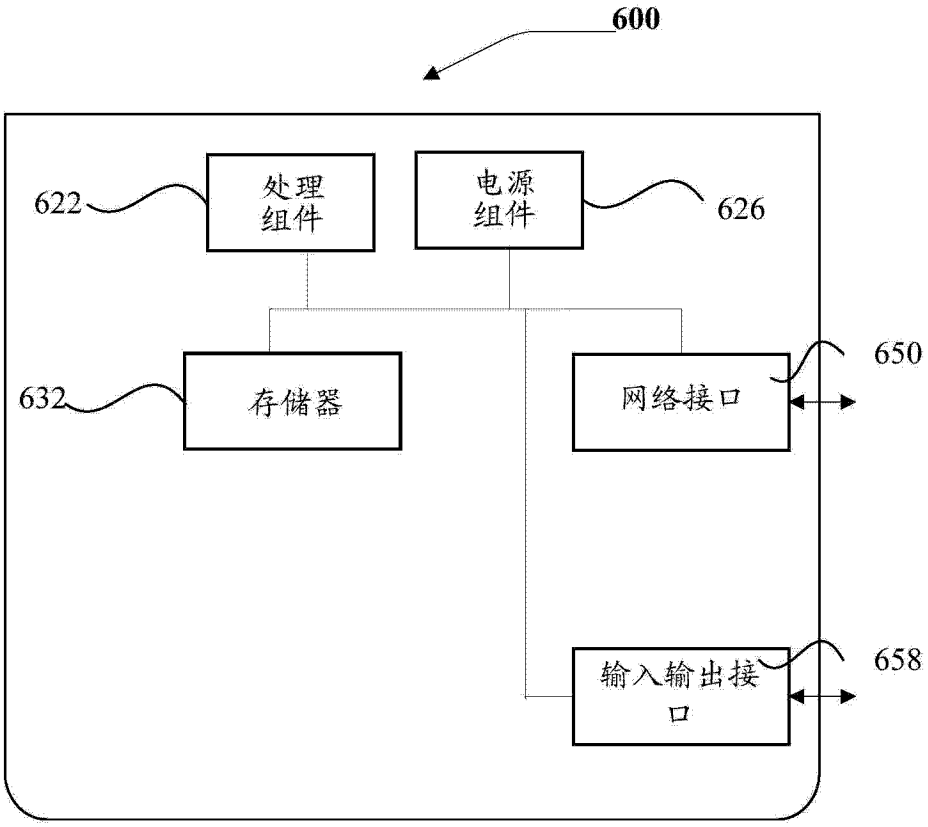


图 6