(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110690956 B
(45)授权公告日 2022.09.06

(21)申请号 201910927499.3
(22)申请日 2019.09.27
(65)同一申请的已公布的文献号
申请公布号 CN 110690956 A
(43)申请公布日 2020.01.14
(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号
(72)发明人 王国云 陈逸恺 陈思
(74)专利代理机构 北京汇思诚业知识产权代理有限公司 11444
专利代理师 冯伟
(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)

审查员 马超

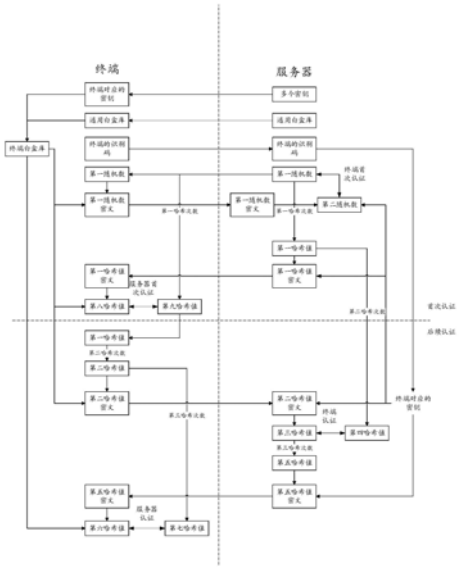
权利要求书3页 说明书16页 附图5页

(54)发明名称

双向认证方法及系统、服务器和终端

(57)摘要

本发明公开了一种双向认证方法及系统、服务器和终端。其中，该方法分别在服务器和终端上实现，该方法包括：终端将包括第二校验信息密文的第一认证信息发送给服务器，第二校验信息密文与第一校验信息相关。服务器对第一认证信息中的第二校验信息密文进行白盒解密，以生成第三校验信息，当第一校验信息与第三校验信息匹配时，服务器完成对终端的认证。服务器将包括第五校验信息密文的第二认证信息发送给终端，第五校验信息密文与第三校验信息相关。终端在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。由此，能够避免认证信息在公开信道上传输时被第三方获取，对认证系统进行仿冒攻击，提高了认证系统的安全性。



CN 110690956 B

1.一种双向认证方法,其特征在于,所述方法在服务器上实现,所述方法包括:

接收第一认证信息;其中,所述第一认证信息包括第二校验信息密文,所述第二校验信息密文由第二校验信息经过白盒加密后生成,所述第二校验信息与第一校验信息相关,所述第一校验信息存储在终端和所述服务器上;

对所述第二校验信息密文进行白盒解密,以生成第三校验信息;

在所述第一校验信息和所述第三校验信息匹配时,完成对所述终端的认证;

将第二认证信息发送给所述终端,以便所述终端对所述服务器进行认证;其中,所述第二认证信息包括第五校验信息密文,所述第五校验信息密文由所述第五校验信息经过白盒加密后生成,所述第五校验信息与所述第三校验信息相关,且所述第二认证信息与所述第一认证信息不同;

其中,所述校验信息为哈希值,所述校验信息密文为哈希值密文,所述第一校验信息为第一哈希值,所述第二校验信息为第二哈希值,所述第二校验信息密文为第二哈希值密文,所述第三校验信息为第三哈希值,所述第五校验信息为第五哈希值,所述第五校验信息密文为第五哈希值密文;

所述第一认证信息还包括第二哈希次数,所述第二哈希值由所述第一哈希值经过所述第二哈希次数的哈希运算后生成,

所述在所述第一校验信息和所述第三校验信息匹配时,完成对所述终端的认证,包括:

对所述第一哈希值进行所述第二哈希次数的哈希运算,以生成第四哈希值;

在所述第四哈希值和所述第三哈希值相等时,完成对所述终端的认证。

2.如权利要求1所述的方法,其特征在于,所述第一认证信息还包括所述终端的识别码,

所述对所述第二校验信息密文进行白盒解密,以生成第三校验信息,包括:

根据所述终端的识别码,确定所述终端对应的密钥;

使用所述终端对应的密钥,对所述第二哈希值密文进行白盒解密,以生成所述第三哈希值。

3.如权利要求2所述的方法,其特征在于,在所述接收第一认证信息之前,还包括:

生成第一随机数,并将所述第一随机数发送给所述终端;

接收第一随机数密文;其中,所述第一随机数密文由所述第一随机数经过白盒加密后生成;

对所述第一随机数密文进行白盒解密,以生成第二随机数;

在所述第一随机数和所述第二随机数相等时,完成对所述终端的首次认证;

将第一哈希值密文发送给所述终端,以便所述终端对所述服务器进行首次认证;其中,所述第一哈希值密文由所述第一哈希值经过白盒加密后生成,所述第一哈希值由所述第一随机数经过第一哈希次数的哈希运算后生成。

4.如权利要求3所述的方法,其特征在于,在所述生成所述第一随机数之前,还包括:

生成多个密钥和通用白盒库,并将所述多个密钥和所述通用白盒库分别发送给对应的所述终端。

5.一种双向认证方法,其特征在于,所述方法在终端上实现,所述方法包括:

获取第一校验信息;其中,所述第一校验信息存储在所述终端和服务器上;

将第一认证信息发送给所述服务器，以便所述服务器对所述终端进行认证；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与所述第一校验信息相关；

接收第二认证信息；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由第五校验信息经过白盒加密后生成，所述第五校验信息与所述第二校验信息相关，且所述第二认证信息与所述第一认证信息不同；

在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证；

其中，所述校验信息为哈希值，所述校验信息密文为哈希值密文，所述第一校验信息为第一哈希值，所述第二校验信息为第二哈希值，所述第二校验信息密文为第二哈希值密文，所述第五校验信息为第五哈希值，所述第五校验信息密文为第五哈希值密文；

所述第二认证信息还包括第三哈希次数，所述第五哈希值由第三哈希值经过所述第三哈希次数的哈希运算后生成，所述第三哈希值由所述第二哈希值密文经过白盒解密后生成，

所述在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证，包括：

对所述第五哈希值密文进行白盒解密，以生成第六哈希值；

对所述第二哈希值进行所述第三哈希次数的哈希运算，以生成第七哈希值；

在所述第六哈希值和所述第七哈希值相等时，完成对所述服务器的认证。

6.如权利要求5所述的方法，其特征在于，在所述获取第一校验信息之前，还包括：

将所述终端的识别码发送给所述服务器；

接收第一随机数；

使用所述终端白盒库，对所述第一随机数进行白盒加密，以生成第一随机数密文；

将所述第一随机数密文发送给所述服务器，以便所述服务器进行对所述终端的首次认证；

接收第一哈希值密文和第一哈希次数；其中，所述第一哈希值密文由所述第一哈希值经过白盒加密后生成；所述第一哈希值由所述第一随机数经过第一哈希次数的哈希运算后生成；

使用所述终端白盒库，对所述第一哈希值密文进行白盒解密，以生成第八哈希值；

对所述第一随机数进行所述第一哈希次数的哈希运算，以生成第九哈希值；

在所述第八哈希值和所述第九哈希值相等的情况下，完成对所述服务器的首次认证。

7.如权利要求6所述的方法，其特征在于，在所述将所述终端的识别码发送给所述服务器之前，还包括：

接收所述终端对应的密钥和通用白盒库，并根据所述终端对应的密钥和所述通用白盒库，生成所述终端白盒库。

8.一种服务器，其特征在于，所述服务器用于，

接收第一认证信息；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与第一校验信息相关，所述第一校验信息存储在终端和所述服务器上；

对所述第二校验信息密文进行白盒解密，以生成第三校验信息；

在所述第一校验信息和所述第三校验信息匹配时，完成对所述终端的认证；

将第二认证信息发送给所述终端，以便所述终端对所述服务器进行认证；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由所述第五校验信息经过白盒加密后生成，所述第五校验信息与所述第三校验信息相关，且所述第二认证信息与所述第一认证信息不同；

其中，所述校验信息为哈希值，所述校验信息密文为哈希值密文，所述第一校验信息为第一哈希值，所述第二校验信息为第二哈希值，所述第二校验信息密文为第二哈希值密文，所述第三校验信息为第三哈希值，所述第五校验信息为第五哈希值，所述第五校验信息密文为第五哈希值密文；

所述第一认证信息还包括第二哈希次数，所述第二哈希值由所述第一哈希值经过所述第二哈希次数的哈希运算后生成，

所述在所述第一校验信息和所述第三校验信息匹配时，完成对所述终端的认证，包括：

对所述第一哈希值进行所述第二哈希次数的哈希运算，以生成第四哈希值；

在所述第四哈希值和所述第三哈希值相等时，完成对所述终端的认证。

9.一种终端，其特征在于，所述终端用于，

获取第一校验信息；其中，所述第一校验信息存储在所述终端和服务器上；

将第一认证信息发送给所述服务器，以便所述服务器对所述终端进行认证；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与所述第一校验信息相关；

接收第二认证信息；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由第五校验信息经过白盒加密后生成，所述第五校验信息与所述第二校验信息相关，且所述第二认证信息与所述第一认证信息不同；

在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证；

其中，所述校验信息为哈希值，所述校验信息密文为哈希值密文，所述第一校验信息为第一哈希值，所述第二校验信息为第二哈希值，所述第二校验信息密文为第二哈希值密文，所述第五校验信息为第五哈希值，所述第五校验信息密文为第五哈希值密文；

所述第二认证信息还包括第三哈希次数，所述第五哈希值由第三哈希值经过所述第三哈希次数的哈希运算后生成，所述第三哈希值由所述第二哈希值密文经过白盒解密后生成，

所述在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证，包括：

对所述第五哈希值密文进行白盒解密，以生成第六哈希值；

对所述第二哈希值进行所述第三哈希次数的哈希运算，以生成第七哈希值；

在所述第六哈希值和所述第七哈希值相等时，完成对所述服务器的认证。

10.一种双向认证系统，其特征在于，所述系统包括如权利要求8所述的服务器，以及如权利要求9所述的终端。

双向认证方法及系统、服务器和终端

【技术领域】

[0001] 本发明涉及信息安全技术领域，尤其涉及一种双向认证方法及系统、服务器和终端。

【背景技术】

[0002] 在物联网中，终端与服务器进行通信前，需要进行身份认证，认证通过后，才允许终端和服务器之间进行数据传输。

[0003] 考虑到物联网的终端通常部署于室外，第三方能够轻易接触到终端，对终端进行白盒攻击，甚至窃取终端，将合法终端替换为非法终端。

[0004] 相关技术中，终端与服务器每次进行通信前，发送的身份认证信息保持不变，很容易被第三方截获后进行仿冒攻击。即第三方截获终端(或者服务器)发送的加密信息后，无需对加密信息进行破解，直接利用非法设备向服务器(或者终端)发送该加密信息，仿冒合法终端(或者服务器)，与服务器(或者终端)进行通信，窃取机密信息。

【发明内容】

[0005] 有鉴于此，本发明实施例提供了一种双向认证方法及系统、服务器和终端，让终端和服务器在每次通信前发送的身份认证信息动态变化，避免认证信息在公开信道上传输时被第三方获取，对认证系统进行仿冒攻击，提高了认证系统的安全性。

[0006] 一方面，本发明实施例提供了一种双向认证方法，所述方法在服务器上实现，所述方法包括：接收第一认证信息；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与第一校验信息相关，所述第一校验信息存储在终端和所述服务器上；对所述第二校验信息密文进行白盒解密，以生成第三校验信息；在所述第一校验信息和所述第三校验信息匹配时，完成对所述终端的认证；将第二认证信息发送给所述终端，以便所述终端对所述服务器进行认证；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由所述第五校验信息经过白盒加密后生成，所述第五校验信息与所述第三校验信息相关，且所述第二认证信息与所述第一认证信息不同。

[0007] 可选地，所述校验信息为哈希值，所述校验信息密文为哈希值密文，所述第一校验信息为第一哈希值，所述第二校验信息为第二哈希值，所述第二校验信息密文为第二哈希值密文，所述第三校验信息为第三哈希值，所述第五校验信息为第五哈希值，所述第五校验信息密文为第五哈希值密文。

[0008] 可选地，所述第一认证信息还包括所述终端的识别码，所述对所述第二校验信息密文进行白盒解密，以生成第三校验信息，包括：根据所述终端的识别码，确定所述终端对应的密钥；使用所述终端对应的密钥，对所述第二哈希值密文进行白盒解密，以生成所述第三哈希值。

[0009] 可选地，所述第一认证信息还包括第二哈希次数，所述第二哈希值由所述第一哈

希值经过所述第二哈希次数的哈希运算后生成，所述在所述第一校验信息和所述第三校验信息匹配时，完成对所述终端的认证，包括：对所述第一哈希值进行所述第二哈希次数的哈希运算，以生成第四哈希值；在所述第四哈希值和所述第三哈希值相等时，完成对所述终端的认证。

[0010] 可选地，在所述接收第一认证信息之前，还包括：生成第一随机数，并将所述第一随机数发送给所述终端；接收第一随机数密文；其中，所述第一随机数密文由所述第一随机数经过白盒加密后生成；对所述第一随机数密文进行白盒解密，以生成第二随机数；在所述第一随机数和所述第二随机数相等时，完成对所述终端的首次认证；将所述第一哈希值密文发送给所述终端，以便所述终端对所述服务器进行首次认证；其中，所述第一哈希值密文由所述第一哈希值经过白盒加密后生成，所述第一哈希值由所述第一随机数经过第一哈希次数的哈希运算后生成。

[0011] 可选地，在所述生成所述第一随机数之前，还包括：生成多个密钥和通用白盒库，并将所述多个密钥和所述通用白盒库分别发送给对应的所述终端。

[0012] 一方面，本发明实施例提供了一种双向认证方法，所述方法在终端上实现，所述方法包括：获取第一校验信息；其中，所述第一校验信息存储在所述终端和服务器上；将第一认证信息发送给所述服务器，以便所述服务器对所述终端进行认证；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与所述第一校验信息相关；接收第二认证信息；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由第五校验信息经过白盒加密后生成，所述第五校验信息与所述第二校验信息相关，且所述第二认证信息与所述第一认证信息不同；在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证。

[0013] 可选地，所述校验信息为哈希值，所述校验信息密文为哈希值密文，所述第一校验信息为第一哈希值，所述第二校验信息为第二哈希值，所述第二校验信息密文为第二哈希值密文，所述第五校验信息为第五哈希值，所述第五校验信息密文为第五哈希值密文。

[0014] 可选地，所述第二认证信息还包括第三哈希次数，所述第五哈希值由第三哈希值经过所述第三哈希次数的哈希运算后生成，所述第三哈希值由所述第二哈希值密文经过白盒解密后生成，所述在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证，包括：对所述第五哈希值密文进行白盒解密，以生成第六哈希值；对所述第二哈希值进行所述第三哈希次数的哈希运算，以生成第七哈希值；在所述第六哈希值和所述第七哈希值相等时，完成对所述服务器的认证。

[0015] 可选地，在所述获取第一校验信息之前，还包括：将所述终端的识别码发送给所述服务器；接收所述第一随机数；使用所述终端白盒库，对所述第一随机数进行白盒加密，以生成第一随机数密文；将所述第一随机数密文发送给所述服务器，以便所述服务器进行对所述终端的首次认证；接收第一哈希值密文和第一哈希次数；其中，所述第一哈希值密文由所述第一哈希值经过白盒加密后生成；所述第一哈希值由所述第一随机数经过第一哈希次数的哈希运算后生成；使用所述终端白盒库，对所述第一哈希值密文进行白盒解密，以生成第八哈希值；对所述第一随机数进行所述第一哈希次数的哈希运算，以生成第九哈希值；在所述第八哈希值和所述第九哈希值相等的情况下，完成对所述服务器的首次认证。

[0016] 可选地，在所述将所述终端的识别码发送给所述服务器之前，还包括：接收所述终

端对应的密钥和通用白盒库，并根据所述终端对应的密钥和所述通用白盒库，生成所述终端白盒库。

[0017] 一方面，本发明实施例提供了一种服务器，所述服务器用于，接收第一认证信息；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与第一校验信息相关，所述第一校验信息存储在终端和所述服务器上；对所述第二校验信息密文进行白盒解密，以生成第三校验信息；在所述第一校验信息和所述第三校验信息匹配时，完成对所述终端的认证；将第二认证信息发送给所述终端，以便所述终端对所述服务器进行认证；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由所述第五校验信息经过白盒加密后生成，所述第五校验信息与所述第三校验信息相关，且所述第二认证信息与所述第一认证信息不同。

[0018] 一方面，本发明实施例提供了一种终端，所述终端用于，获取第一校验信息；其中，所述第一校验信息存储在所述终端和服务器上；将第一认证信息发送给所述服务器，以便所述服务器对所述终端进行认证；其中，所述第一认证信息包括第二校验信息密文，所述第二校验信息密文由第二校验信息经过白盒加密后生成，所述第二校验信息与所述第一校验信息相关；接收第二认证信息；其中，所述第二认证信息包括第五校验信息密文，所述第五校验信息密文由第五校验信息经过白盒加密后生成，所述第五校验信息与所述第二校验信息相关，且所述第二认证信息与所述第一认证信息不同；在所述第二校验信息和所述第五校验信息密文匹配时，完成对所述服务器的认证。

[0019] 一方面，本发明实施例提供了一种系统，所述系统包括前述的服务器，以及前述的终端。

[0020] 在本发明实施例中，每一次认证过程中，在公开信道上传输不同的认证信息，避免认证信息在公开信道上传输时被第三方获取，对认证系统进行仿冒攻击，提高了认证系统的安全性。并且，服务器和终端发送的认证信息经过了白盒加密，可以抵抗白盒攻击。此外，服务器和终端双向认证过程仅包含一次交互，方便认证系统部署于带宽有限的网络系统中。

【附图说明】

[0021] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其它的附图。

[0022] 图1为本发明实施例所提供的一种双向认证方法的流程示意图；

[0023] 图2为本发明实施例所提供的另一种双向认证方法的流程示意图；

[0024] 图3为本发明实施例所提供的又一种双向认证方法的流程示意图；

[0025] 图4为本发明实施例所提供的双向认证方法的一个示例的流程图；

[0026] 图5为本发明实施例所提供的一种服务器的结构示意图；以及

[0027] 图6为本发明实施例所提供的一种终端的结构示意图。

【具体实施方式】

[0028] 为了更好的理解本发明的技术方案，下面结合附图对本发明实施例进行详细描述。

[0029] 应当明确，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0030] 在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[0031] 应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的相同的字段，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0032] 应当理解，尽管在本发明实施例中可能采用术语第一、第二、第三等来描述预设范围等，但这些预设范围不应限于这些术语。这些术语仅用来将预设范围彼此区分开。例如，在不脱离本发明实施例范围的情况下，第一预设范围也可以被称为第二预设范围，类似地，第二预设范围也可以被称为第一预设范围。

[0033] 取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测(陈述的条件或事件)”可以被解释成为“当确定时”或“响应于确定”或“当检测(陈述的条件或事件)时”或“响应于检测(陈述的条件或事件)”。

[0034] 基于前述现有技术的说明，可以知道，相关技术中，终端与服务器每次进行通信前，发送的身份认证信息保持不变，很容易被第三方截获后进行仿冒攻击。即第三方截获终端(或者服务器)发送的加密信息后，无需对加密信息进行破解，直接利用非法设备向服务器(或者终端)发送该加密信息，仿冒合法终端(或者服务器)，与服务器(或者终端)进行通信，窃取机密信息。

[0035] 为了解决这一问题，本发明实施例提出了一种双向认证方法及系统、服务器和终端。让终端和服务器在每次通信前发送的身份认证信息动态变化，避免认证信息在公开信道上传输时被第三方获取，对认证系统进行仿冒攻击，提高了认证系统的安全性。

[0036] 其中，终端的认证方法在服务器上实现，由服务器完成对终端的单向认证，服务器的认证方法在终端上实现，由终端完成对服务器的单向认证，当服务器完成对终端的认证，且终端完成对服务器的认证时，服务器和终端便完成了双向认证。并且，服务器和终端发送的认证信息经过了白盒加密，可以抵抗白盒攻击。此外，服务器和终端双向认证过程仅包含一次交互，方便认证系统部署于带宽有限的网络系统中。

[0037] 为了便于说明，首先对双向认证方法进行说明，该方法在服务器和终端上实现，图1为本发明实施例所提供的一种双向认证方法的流程示意图。如图1所示，该方法包括以下步骤：

[0038] 步骤S101，终端获取第一校验信息。

[0039] 其中，第一校验信息存储在终端和服务器上。

[0040] 本发明实施例所提供的双向认证方法为终端和服务器完成首次双向认证之后，终

端后续访问服务器时，终端和服务器之间进行双向认证的步骤。换句话说，终端已经与服务器进行过至少一次双向认证，终端和服务器在上一次双向认证过程中，进行过信息传输。

[0041] 相应地，第一校验信息是指在上一次双向认证完成后，终端和服务器同步存储的校验信息。

[0042] 需要说明的是，在终端与服务器进行首次双向认证时，首次生成第一校验信息，在之后的双向校验信息过程中，当终端与服务器每一次完成双向认证后，会对第一校验信息进行更新，以保证每次双向认证时使用的第一校验信息不同。

[0043] 步骤S102，终端将第一认证信息发送给服务器，以便服务器对终端进行认证。

[0044] 其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关。

[0045] 需要首先说明的是，为了让第一校验信息能够在终端和服务器上同时存储，在上一次的双向认证过程中，第一校验信息对应的第一校验信息密文已经在公开信道上进行过传输，为了让每一次在公开信道上传输的信息不同，以抵抗仿冒攻击，在本次双向认证过程中，需要对第一校验信息进行处理，以得到不同于第一校验信息的第二校验信息。

[0046] 此外，考虑到第二校验信息在公开信道上进行传输时，会被第三方拦截，为了增强认证系统的安全性，本发明实施例终端在将第二校验信息进行传输之前，需要对第二校验信进行加密，生成第二校验信息密文，将第二校验信息密文发送给服务器，由服务器对第二校验信息密文进行解密。

[0047] 由于终端通常部署于室外，第三方能够轻易接触到终端，并获取终端中存储的信息，为了避免终端上存储的密钥被第三方获取，本发明实施例采用了白盒加密算法对第二校验信息进行白盒加密，以生成第二校验信息密文，相应地，服务器也采用白盒解密算法对第二校验信息密文进行解密。

[0048] 白盒加密算法是一种在运行环境中不出现完整密钥的算法，对密钥做尽量复杂的混淆，使得第三方无法从终端的存储介质中获取密钥。也就是说，终端上存储了终端对应的终端白盒库，终端白盒库根据密钥生成，但是终端白盒库中不存储密钥，要进行加密或者解密运算时，直接调用终端白盒库即可。

[0049] 服务器在接收到第二校验信息密文后，对存储的第一校验信息进行相同的处理，即可对接收的第二校验信息密文进行校验。

[0050] 步骤S103，服务器对第二校验信息密文进行白盒解密，以生成第三校验信息。

[0051] 可以理解，由于第二校验信息密文是由第二校验信息进行白盒加密后生成的，因此需要首先对接收到的第二校验信息密文进行白盒解密，以生成第三校验信息。

[0052] 步骤S104，服务器在第一校验信息和第三校验信息匹配时，完成对终端的认证。

[0053] 基于前述说明可以知道，若服务器对存储的第一校验信息采用与终端相同的处理方式进行处理，得到的第四校验信息，与第三校验信息相同，说明服务器接收到的第二校验信息密文与服务器上存储的第一校验信息匹配，第一认证信息确实是由终端发出的，终端访问请求并非仿冒攻击，服务器完成对终端的认证。

[0054] 步骤S105，服务器将第二认证信息发送给终端，以便终端对服务器进行认证。

[0055] 其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第三校验信息相关，且第二认证信息与第一认证信

息不同。

[0056] 可以理解，在服务器完成对终端的认证之后，终端还需要对服务器进行认证。

[0057] 此时，服务器上的第三校验信息，与第二校验信息、第四校验信息相同，而第二校验信息对应的第二校验信息密文在传输第一认证信息时，已经在公开信道上进行了传输。为了让每一次在公开信道上传输的信息不同，以抵抗仿冒攻击，需要对第三校验信息进行处理，以得到不同于第三校验信息的第五校验信息，并将第五校验信息白盒加密后生成的第五校验信息密文发送给服务器。

[0058] 步骤S106，终端在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。

[0059] 类似地，终端在收到第五校验信息密文后，先对第五校验信息进行白盒解密，以生成第六校验信息。

[0060] 对存储的第二校验信息进行与服务器相同的处理方式进行处理，以生成第七校验信息。

[0061] 基于前述说明可以知道，若终端对存储的第二校验信息采用与服务器相同的处理方式进行处理，得到的第七校验信息，与第六校验信息相同，则可完成终端对服务器的认证。

[0062] 综上所述，本发明实施例所提供的双向认证方法，分别在服务器和终端上实现，该方法包括：终端将包括第二校验信息密文的第一认证信息发送给服务器，第二校验信息密文与第一校验信息相关。服务器对第一认证信息中的第二校验信息密文进行白盒解密，以生成第三校验信息，当第一校验信息与第三校验信息匹配时，服务器完成对终端的认证。服务器将包括第五校验信息密文的第二认证信息发送给终端，第五校验信息密文与第三校验信息相关。终端在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。由此，能够避免认证信息在公开信道上传输时被第三方获取，对认证系统进行仿冒攻击，提高了认证系统的安全性。并且，服务器和终端发送的认证信息经过了白盒加密，可以抵抗白盒攻击。此外，服务器和终端双向认证过程仅包含一次交互，方便认证系统部署于带宽有限的网络系统中。

[0063] 进一步地，为了实现公开信道上传输的第一认证信息和第二认证信息不同，即第二校验信息密文和第五校验信息密文不同，并且终端和服务器采用相同的处理方式对第一校验信息进行处理后，生成的第二校验信息和第四校验信息相同，对第二校验信息进行处理后，生成的第五校验信息和第七校验信息相同。本发明实施例提出了一种可能的实现方式，采用哈希算法对校验信息进行处理，即校验信息为哈希值，校验信息密文为哈希值密文。相应地，第一校验信息为第一哈希值，第一校验信息密文为第一哈希值密文，第二校验信息为第二哈希值，第二校验信息密文为第二哈希值密文，第三校验信息为第三哈希值，第三校验信息密文为第三哈希值密文，第四校验信息为第四哈希值，第四校验信息密文为第四哈希值密文，第五校验信息为第五哈希值，第五校验信息密文为第五哈希值密文，第六校验信息为第六哈希值，第六校验信息密文为第六哈希值密文，第七校验信息为第七哈希值，第七校验信息密文为第七哈希值密文，第八校验信息为第八哈希值，第八校验信息密文为第八哈希值密文，第九校验信息为第九哈希值，第九校验信息密文为第九哈希值密文。

[0064] 需要说明的是，哈希运算是一种将任意长度的输入信息，通过散列算法变换成固

定长度的输出的函数运算，即将任意长度的信息压缩为固定长度的信息摘要的函数运算。哈希算法具有确定性的特点，即相同的信息，在不同的时间，使用相同的哈希算法进行相同次数的哈希运算，得到的哈希值相同。哈希算法还具有难以逆向运算的特点，即无法通过信息摘要，获取被压缩的信息。哈希算法有多种，本发明实施例所采用的哈希算法为SM3算法，主要用于数字签名及验证、消息认证码生成及验证、随机数生成等。

[0065] 需要说明的是，对于同一条信息，进行不同次数的哈希运算，得到的哈希值是不同的，比如对于信息A，进行一次哈希运算，得到信息A对应的哈希值B，再对哈希值B进行一次哈希运算，得到哈希值B对应的哈希值C，哈希值B和哈希值C的数值大小不同。要确认哈希值C的数值是否正确，可以对信息A进行两次哈希运算，或者对哈希值B进行一次哈希运算，看结果是否等于哈希值C。

[0066] 此外，考虑到终端和服务器采用白盒加密的方式生成哈希值对应的哈希值密文，而通常一个服务器需要与多个终端进行通信，而每个终端上进行白盒加密或者解密的终端白盒库都不相同，为了让服务器能够分别对不同的终端进行不同的白盒加密或者解密。本发明实施例提出了一种可能的实现方式，在服务器上存储每个终端对应的密钥，以及通用白盒库，与不同的终端进行双向认证时，结合终端对应的密钥和通用白盒库，进行白盒加密或者解密。

[0067] 需要解释的是，终端白盒库由终端对应的密钥和通用白盒库生成，在终端上，为了提高终端的安全性，在终端初始化时，就根据终端对应的密钥和通用白盒库，生成终端白盒库，终端上不存储密钥。在服务器上，由于密钥的存储空间小于终端白盒库的存储空间，为了减少系统占用的存储空间，仅存储一个通用白盒库和每个终端对应的密钥，与不同终端进行身份认证时，利用该终端对应的密钥和通用白盒库进行加密或者解密。

[0068] 因此，终端向服务器发送的第一认证信息中还需要包括终端的识别码，以便于服务器获知当前进行身份验证的终端是哪一个，以便使用对应的密钥进行加密或者解密。

[0069] 可以理解，终端的识别码与终端一一对应，与终端的密钥一一对应。

[0070] 基于前述对哈希算法的说明，可以知道，确定哈希算法的输出结果的因素包括输入信息以及哈希次数，若哈希次数不同，即便输入信息相同，也无法得到相同的输出结果。因此，对于哈希算法来说，要确认哈希值的数值是否正确，必须同时知道哈希运算的输入信息，以及哈希运算的次数。

[0071] 因此，终端向服务器发送的第一认证信息中还需要包括第二哈希次数，第一哈希值经过第二哈希次数的哈希运算后生成第二哈希值，服务器向终端发送的第二认证信息中还需要包括第三哈希次数，第三哈希值经过第三哈希次数的哈希运算后生成第五哈希值。

[0072] 相应地，本发明实施例还提出一种在服务器上实现的双向认证方法，该方法包括：

[0073] 步骤S11，接收第一认证信息。

[0074] 其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关，第一校验信息存储在终端和服务器上。

[0075] 步骤S12，对第二校验信息密文进行白盒解密，以生成第三校验信息。

[0076] 步骤S13，在第一校验信息和第三校验信息匹配时，完成对终端的认证。

[0077] 步骤S14，将第二认证信息发送给终端，以便终端对服务器进行认证。

[0078] 其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第三校验信息相关，且第二认证信息与第一认证信息不同。

[0079] 进一步地，为了实现公开信道上传输的第一认证信息和第二认证信息不同，即第二校验信息密文和第五校验信息密文不同，并且终端和服务器采用相同的处理方式对第一校验信息进行处理后，生成的第二校验信息和第四校验信息相同，对第二校验信息进行处理后，生成的第五校验信息和第七校验信息相同，一种可能的实现方式是，校验信息为哈希值，校验信息密文为哈希值密文，第一校验信息为第一哈希值，第二校验信息为第二哈希值，第二校验信息密文为第二哈希值密文，第三校验信息为第三哈希值，第五校验信息为第五哈希值，第五校验信息密文为第五哈希值密文。

[0080] 进一步地，为了让服务器能够分别对不同的终端进行不同的白盒加密或者解密，一种可能的实现方式是，第一认证信息还包括终端的识别码，步骤S12，对第二校验信息密文进行白盒解密，以生成第三校验信息，包括：根据终端的识别码，确定终端对应的密钥。使用终端对应的密钥，对第二哈希值密文进行白盒解密，以生成第三哈希值。

[0081] 进一步地，为了能够完成对终端的认证，一种可能的实现方式是，第一认证信息还包括第二哈希次数，第二哈希值由第一哈希值经过第二哈希次数的哈希运算后生成，步骤S13，在第一校验信息和第三校验信息匹配时，完成对终端的认证，包括：对第一哈希值进行第二哈希次数的哈希运算，以生成第四哈希值。在第四哈希值和第三哈希值相等时，完成对终端的认证。

[0082] 需要特别说明的是，前述对在服务器和终端上实现的一种双向认证方法实施例的解释说明，也适用于该实施例在服务器上实现的一种双向认证方法，本发明实施例对此不再赘述。

[0083] 相应地，本发明实施例还提出一种在终端上实现的双向认证方法，该方法包括：

[0084] 步骤S21，获取第一校验信息。

[0085] 其中，第一校验信息存储在终端和服务器上。

[0086] 步骤S22，将第一认证信息发送给服务器，以便服务器对终端进行认证。

[0087] 其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关。

[0088] 步骤S23，接收第二认证信息。

[0089] 其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第二校验信息相关，且第二认证信息与第一认证信息不同。

[0090] 步骤S24，在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。

[0091] 进一步地，为了实现公开信道上传输的第一认证信息和第二认证信息不同，即第二校验信息密文和第五校验信息密文不同，并且终端和服务器采用相同的处理方式对第一校验信息进行处理后，生成的第二校验信息和第四校验信息相同，对第二校验信息进行处理后，生成的第五校验信息和第七校验信息相同，一种可能的实现方式是，校验信息为哈希值，校验信息密文为哈希值密文，第一校验信息为第一哈希值，第二校验信息为第二哈希值，第二校验信息密文为第二哈希值密文，第五校验信息为第五哈希值，第五校验信息密文

为第五哈希值密文。

[0092] 进一步地，为了能够完成对服务器的认证，一种可能的实现方式是，第二认证信息还包括第三哈希次数，第五哈希值由第三哈希值经过第三哈希次数的哈希运算后生成，第三哈希值由第二哈希值密文经过白盒解密后生成，步骤S24，在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证，包括：对第五哈希值密文进行白盒解密，以生成第六哈希值。对第二哈希值进行第三哈希次数的哈希运算，以生成第七哈希值。在第六哈希值和第七哈希值相等时，完成对服务器的认证。

[0093] 需要特别说明的是，前述对在服务器和终端上实现的一种双向认证方法实施例的解释说明，也适用于该实施例在终端上实现的一种双向认证方法，本发明实施例对此不再赘述。

[0094] 基于前述说明，可以知道，本发明实施例所提供的双向认证方法，终端已经与服务器进行过至少一次双向认证，也就是说，终端和服务器还需要完成首次双向认证。为了更加清楚地说明本发明实施例所提供的双向认证方法，本发明实施例还提出了另一种双向认证方法，图2为本发明实施例所提供的另一种双向认证方法的流程示意图。如图2所示，该方法包括：

[0095] 步骤S201，终端将终端的识别码发送给服务器。

[0096] 需要说明的是，本发明实施例所提供的双向认证方法在终端和服务器首次进行身份认证时，需要将第一哈希值在终端和服务器上同时存储。

[0097] 具体地，由终端向服务器发送终端的认证码，来触发首次身份认证的过程。

[0098] 步骤S202，服务器生成第一随机数，并将第一随机数发送给终端。

[0099] 可以理解，服务器在从终端获取终端的识别码后，确定该终端为首次身份认证，为了能够在后续的身份认证中，使用统一的身份认证信息，本发明实施例在首次身份认证过程中，首先由服务器生成第一随机数，并由服务器将第一随机数发送至终端，使得服务器和终端能够存储有相同的第一随机数，作为身份认证的校验信息。

[0100] 步骤S203，终端使用终端白盒库，对第一随机数进行白盒加密，以生成第一随机数密文。

[0101] 步骤S204，终端将第一随机数密文发送给服务器，以便服务器进行对终端的首次认证。

[0102] 由于服务器在获取终端的识别码之前，服务器无法确定终端对应的密钥，因此步骤S201，终端将终端的识别码发送给服务器中，终端没有对发送的信息进行加密。

[0103] 而当终端第二次向服务器发送信息时，服务器已经获取了终端的识别码，能够确定终端对应的密钥，此时将第一随机数进行加密后发送给服务器。

[0104] 一方面，加密和解密的过程能够让服务器确定第一随机数已经被对应的终端接收，加密和解密实际上是终端的数字签名。

[0105] 另一方面，可以保证相同的信息不能在公开信道上传输两次，避免仿冒攻击。也就是说，即便第三方截获了服务器发送给终端的第一随机数，无法进行白盒加密的情况下，第三方根据第一随机数生成第一随机数密文，也就无法对终端进行仿冒。

[0106] 步骤S205，服务器对第一随机数密文进行白盒解密，以生成第二随机数。

[0107] 步骤S206，服务器在第一随机数和第二随机数相等时，完成对终端的首次认证。

[0108] 可以理解，服务器上存储有第一随机数，在从终端获取了第一随机数密文之后，使用终端对应的密钥对第一随机数密文进行解密，得到第二随机数。

[0109] 第一随机数的传输和加密没有出现问题，那么第一随机数的大小应当等于第二随机数。换句话说，如果第一随机数和第二随机数相等，则服务器完成了对终端的首次认证。

[0110] 步骤S207，服务器将第一哈希值密文发送给终端，以便终端对服务器进行首次认证。

[0111] 其中，第一哈希值密文由第一哈希值经过白盒加密后生成，第一哈希值由第一随机数经过第一哈希次数的哈希运算后生成。

[0112] 应当理解，在服务器完成了对终端的首次认证之后，终端还需要对服务器进行首次认证。

[0113] 此外，由于第一随机数密文已经在公开信道上传输过，不能再次传输第一随机数密文。

[0114] 本发明实施例采用了对第一随机数进行第一哈希次数的哈希运算的方式，生成第一哈希值，将第一哈希值作为新的认证信息。

[0115] 和前述说明相类似，由于终端上已经存储有第一随机数，只需要终端和服务器对第一随机数进行相同次数的哈希运算，对结果进行验证，即可完成终端对服务器的认证。

[0116] 步骤S208，终端使用终端白盒库，对第一哈希值密文进行白盒解密，以生成第八哈希值。

[0117] 步骤S209，终端对第一随机数进行第一哈希次数的哈希运算，以生成第九哈希值。

[0118] 步骤S210，终端在第八哈希值和第九哈希值相等的情况下，完成对服务器的首次认证。

[0119] 可以理解，在第八哈希值和第九哈希值相等的情况下，第一哈希值、第八哈希值和第九哈希值应当相同。

[0120] 步骤S211，终端获取第一哈希值。

[0121] 其中，第一哈希值存储在终端和服务器上。

[0122] 步骤S212，终端将第一认证信息发送给服务器，以便服务器对终端进行认证。

[0123] 其中，第一认证信息包括第二哈希值密文，第二哈希值密文由第二哈希值经过白盒加密后生成，第二哈希值由第一哈希值经过第一哈希次数的哈希运算后生成。

[0124] 步骤S213，服务器对第二哈希值密文进行白盒解密，以生成第三哈希值。

[0125] 步骤S214，服务器在第一哈希值和第三哈希值匹配时，完成对终端的认证。

[0126] 步骤S215，服务器将第二认证信息发送给终端，以便终端对服务器进行认证。

[0127] 其中，第二认证信息包括第五哈希值密文，第五哈希值密文由第五哈希值经过白盒加密后生成，第五哈希值由第三哈希值经过第三哈希次数的哈希运算后生成。

[0128] 步骤S216，终端在第二哈希值和第五哈希值密文匹配时，完成对服务器的认证。

[0129] 需要特别说明的是，前述对步骤S101-步骤S106的解释说明，也适用于步骤S211-步骤S216，本发明实施例对此不再赘述。

[0130] 从而，既实现了对终端和服务器的首次认证，又实现了终端和服务器同时存储有第一哈希值，为后续的身份认证提供了身份认证信息。

[0131] 为了避免哈希运算的次数在公开信道上直接传输，一种可能的实现方式是，终端

和服务器之间传输累计哈希次数，即从第一随机数到对应的哈希值，所经过的哈希运算的次数。

[0132] 可以理解，由于累计哈希次数和哈希值同时进行传输，一方面，可以避免第三方直接获取本次哈希运算对应的哈希次数，另一方面可以借助终端和服务器上存储的累计哈希次数的数值大小，初步判断哈希值的传输是否出现问题。

[0133] 比如说，服务器在获取第二哈希值密文和第二累计哈希次数后，需要对服务器上存储的累计哈希次数进行更新，若服务器在获取第二哈希值密文时出现问题，导致服务器获得第二累计哈希次数后，服务器上存储的累计哈希次数小于终端存储的累计哈希次数，则需要终端重新认证，服务器重新接收第二哈希值密文、第二累计哈希次数和终端的识别码。

[0134] 类似的，若终端在获取第五哈希值密文时出现问题，导致终端存储的累计哈希次数没有更新，小于服务器存储的累计哈希次数，则终端下一次认证时，需要先进行多次的哈希运算，直到终端存储的累计哈希次数大于服务器存储的累计哈希次数。

[0135] 此外，随着验证次数的增加，累计哈希次数不断增加，可能会导致累计哈希次数存储的溢出，可以将累计哈希次数置零，以及重新进行首次认证。

[0136] 相应地，本发明实施例还提出另一种在服务器上实现的双向认证方法，该方法包括：

[0137] 步骤S31，生成第一随机数，并将第一随机数发送给终端。

[0138] 步骤S32，接收第一随机数密文。

[0139] 其中，第一随机数密文由第一随机数经过白盒加密后生成。

[0140] 步骤S33，对第一随机数密文进行白盒解密，以生成第二随机数。

[0141] 步骤S34，在第一随机数和第二随机数相等时，完成对终端的首次认证。

[0142] 步骤S35，将第一哈希值密文发送给终端，以便终端对服务器进行首次认证。

[0143] 其中，第一哈希值密文由第一哈希值经过白盒加密后生成，第一哈希值由第一随机数经过第一哈希次数的哈希运算后生成。

[0144] 步骤S36，接收第一认证信息。

[0145] 其中，第一认证信息包括第二哈希值密文，第二哈希值密文由第二哈希值经过白盒加密后生成，第二哈希值由第一哈希值经过第一哈希次数的哈希运算后生成。

[0146] 步骤S37，对第二哈希值密文进行白盒解密，以生成第三哈希值。

[0147] 步骤S38，在第一哈希值和第三哈希值匹配时，完成对终端的认证。

[0148] 步骤S39，将第二认证信息发送给终端，以便终端对服务器进行认证。

[0149] 其中，第二认证信息包括第五哈希值密文，第五哈希值密文由第五哈希值经过白盒加密后生成，第五哈希值由第三哈希值经过第三哈希次数的哈希运算后生成。

[0150] 需要特别说明的是，前述对在服务器和终端上实现的另一种双向认证方法实施例的解释说明，也适用于该实施例在服务器上实现的另一种双向认证方法，本发明实施例对此不再赘述。

[0151] 相应地，本发明实施例还提出另一种在终端上实现的双向认证方法，该方法包括：

[0152] 步骤S41，将终端的识别码发送给服务器。

[0153] 步骤S42，接收第一随机数。

[0154] 步骤S43，使用终端白盒库，对第一随机数进行白盒加密，以生成第一随机数密文。

[0155] 步骤S44，将第一随机数密文发送给服务器，以便服务器进行对终端的首次认证。

[0156] 步骤S45，接收第一哈希值密文和第一哈希次数。

[0157] 其中，第一哈希值密文由第一哈希值经过白盒加密后生成，第一哈希值由第一随机数经过第一哈希次数的哈希运算后生成。

[0158] 步骤S46，使用终端白盒库，对第一哈希值密文进行白盒解密，以生成第八哈希值。

[0159] 步骤S47，对第一随机数进行第一哈希次数的哈希运算，以生成第九哈希值。

[0160] 步骤S48，在第八哈希值和第九哈希值相等的情况下，完成对服务器的首次认证。

[0161] 步骤S49，获取第一哈希值。

[0162] 其中，第一哈希值存储在终端和服务器上。

[0163] 步骤S410，将第一认证信息发送给服务器，以便服务器对终端进行认证。

[0164] 其中，第一认证信息包括第二哈希值密文，第二哈希值密文由第二哈希值经过白盒加密后生成，第二哈希值由第一哈希值经过第一哈希次数的哈希运算后生成。

[0165] 步骤S411，接收第二认证信息。

[0166] 其中，第二认证信息包括第五哈希值密文，第五哈希值密文由第五哈希值经过白盒加密后生成，第五哈希值由第三哈希值经过第三哈希次数的哈希运算后生成。

[0167] 步骤S412，在第二哈希值和第五哈希值密文匹配时，完成对服务器的认证。

[0168] 需要特别说明的是，前述对在服务器和终端上实现的另一种双向认证方法实施例的解释说明，也适用于该实施例在终端上实现的另一种双向认证方法，本发明实施例对此不再赘述。

[0169] 此外，在本发明实施例所提供的双向认证方法中，终端上需要使用终端白盒库进行加密和解密，为了在终端上生成终端白盒库，本发明实施例还提出了又一种双向认证方法。图3为本发明实施例所提供的又一种双向认证方法的流程示意图，如图3所示，基于图2所示的方法流程，在步骤S201，终端将终端的识别码发送给服务器之前，该方法还包括：

[0170] 步骤S301，服务器生成多个密钥和通用白盒库，并将多个密钥和通用白盒库分别发送给对应的终端。

[0171] 可以理解，在系统初始化时，需要在服务器和终端上同步密钥和通用白盒库，具体由服务器生成多个密钥和通用白盒库，并进行分发，使得不同终端收到相同的通用白盒库和不同的密钥。

[0172] 步骤S302，终端从服务器获取终端对应的密钥和通用白盒库，并根据终端对应的密钥和通用白盒库，生成终端白盒库。

[0173] 基于前述的说明，可以知道，本发明实施例中的终端处于容易被第三方进行白盒攻击的状态，为了避免终端对应的密钥直接存储在终端上，被第三方获取，终端在收到密钥和通用白盒库后，生成终端白盒库。第三方即便获取了终端白盒库，也无法得到密钥，提高了系统的安全性。

[0174] 需要说明的是，本发明实施例所提供的终端白盒库为动态白盒库，即白盒库能够动态更新。

[0175] 对于动态白盒库来说，有两种实现方式，一种是密钥保持不变，动态更新通用白盒库，另一种是通用白盒库不变，动态更新密钥组。更新通用白盒库较为复杂，但是安全性较

高，而更新密钥组较为简便，但是安全性较低。实际使用中，可根据需求选择合适的实现方式，本发明实施例对此不做限定。

[0176] 从而，实现了在终端上使用终端白盒库进行加密和解密。

[0177] 相应地，本发明实施例还提出又一种在服务器上实现的双向认证方法，该方法在步骤S31，生成第一随机数之前，还包括：生成多个密钥和通用白盒库，并将多个密钥和通用白盒库分别发送给对应的终端。

[0178] 需要特别说明的是，前述对在服务器和终端上实现的又一种双向认证方法实施例的解释说明，也适用于该实施例在服务器上实现的又一种双向认证方法，本发明实施例对此不再赘述。

[0179] 相应地，本发明实施例还提出又一种在终端上实现的双向认证方法，该方法在步骤S41，将终端的识别码发送给服务器之前，还包括：接收终端对应的密钥和通用白盒库，并根据终端对应的密钥和通用白盒库，生成终端白盒库。

[0180] 需要特别说明的是，前述对在服务器和终端上实现的又一种双向认证方法实施例的解释说明，也适用于该实施例在终端上实现的又一种双向认证方法，本发明实施例对此不再赘述。

[0181] 为了更加清楚地说明本发明实施所提供的双向认证方法，下面进行距离说明，图4为本发明实施例所提供的双向认证方法的一个示例的流程图，如图4所示。

[0182] 在系统初始化时，服务器上生成多个密钥和通用白盒库，并且将不同密钥和通用白盒库发送给不同的终端，终端获取对应的密钥和通用白盒库后，生成终端白盒库。

[0183] 在首次身份认证时，终端发送终端的识别码给服务器，告知服务器有新的终端需要加入网络中，需要进行首次身份认证。服务器生成第一随机数，并将第一随机数发送给终端，终端获取第一随机数后，使用终端白盒库对第一随机数进行白盒加密，生成第一随机数密文，并将第一随机数密文发送给服务器。

[0184] 服务器根据之前获取的终端的识别码，确定终端对应的密钥，使用终端对应的密钥对第一随机数密文进行白盒解密，得到第二随机数，将本地存储的第一随机数和解密获得的第二随机数进行比较，若相等，则服务器完成对终端的首次身份认证。

[0185] 服务器对第一随机数进行第一哈希次数的哈希运算，生成第一哈希值，并将第一哈希次数作为第一累计哈希次数，存储在服务器上。使用终端对应的密钥对第一哈希值进行白盒加密，得到第一哈希值密文，并将第一哈希值密文和第一累计哈希次数发送给终端。

[0186] 终端获取第一哈希值密文后，进行白盒解密，得到第八哈希值。终端获取第一累计哈希次数后，进而可以确定第一哈希次数，对本地存储的第一随机数进行第一哈希次数的哈希运算，生成第九哈希值。比较第八哈希值和第九哈希值的数值大小，若相等，则终端完成对服务器的首次身份认证，并且将第九哈希值作为第一哈希值在本地进行存储。

[0187] 在后续的身份认证过程中，终端对本地存储的第一哈希值进行第二哈希次数的哈希运算，生成第二哈希值，使用终端白盒库对第二哈希值进行白盒加密，生成第二哈希值密文。并将第一累计哈希次数和第二哈希次数相加，得到第二累计哈希次数。将第二哈希值密文、第二累计哈希次数和终端的识别码发送给服务器。

[0188] 服务器根据终端的识别码，确定终端对应的密钥，使用终端对应的密钥对第二哈希值密文进行白盒解密，以生成第三哈希值。服务器根据第二累计哈希次数和第一累计哈

希次数，得到第二哈希次数，对本地存储的第一哈希值进行第二哈希次数的哈希运算，以生成第四哈希值，比较第三哈希值和第四哈希值的大小，若相等，则服务器完成对终端的身份认证。

[0189] 服务器对第三哈希值进行第三哈希次数的哈希运算，得到第五哈希值，并使用终端对应的密钥对第五哈希值进行白盒加密，得到第五哈希值密文。并将第二累计哈希次数和第三哈希次数相加，得到第三累计哈希次数。将第五哈希值密文和第三累计哈希次数发送给终端。

[0190] 终端从服务器获取第五哈希值密文和第三累计哈希次数后，进而确定第三哈希次数的大小。终端使用终端白盒库对第五哈希值密文进行白盒解密，以生成第六哈希值。终端对本地存储的第二哈希值进行第三哈希次数的哈希运算，以生成第七哈希值。比较第六哈希值和第七哈希值的大小，若相等，则终端完成对服务器的身份认证。

[0191] 需要说明的是，本发明实施例所提供的双向认证方法中，终端和服务器对应的方法步骤可以互换，即前述在终端实现的步骤可以在服务器上实现，在服务器上实现的步骤也可以在终端上实现，本发明实施例对此不做限定。

[0192] 为了实现上述实施例，本发明实施例还提出了一种服务器，该服务器用于接收第一认证信息。其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关，第一校验信息存储在终端和服务器上。对第二校验信息密文进行白盒解密，以生成第三校验信息。在第一校验信息和第三校验信息匹配时，完成对终端的认证。将第二认证信息发送给终端，以便终端对服务器进行认证；其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第三校验信息相关，且第二认证信息与第一认证信息不同。

[0193] 具体地，图5为本发明实施例所提供的一种服务器的结构示意图，如图5所示，该服务器包括：

[0194] 接收模块110，用于接收第一认证信息。其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关，第一校验信息存储在终端和服务器上。

[0195] 解密模块120，用于对接收模块110接收的第二校验信息密文进行白盒解密，以生成第三校验信息。

[0196] 认证模块130，用于在第一校验信息和第三校验信息匹配时，完成对终端的认证。

[0197] 发送模块140，用于将第二认证信息发送给终端，以便终端对服务器进行认证。其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第三校验信息相关，且第二认证信息与第一认证信息不同。

[0198] 需要特别说明的是，前述对在服务器上实现的双向认证方法实施例的解释说明，也适用于本发明实施例所提出的服务器，此处不再赘述。

[0199] 为了实现上述实施例，本发明实施例还提出了一种终端，该终端用于获取第一校验信息。其中，第一校验信息存储在终端和服务器上。将第一认证信息发送给服务器，以便服务器对终端进行认证。其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关。接收第二认证信

息。其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第二校验信息相关，且第二认证信息与第一认证信息不同。在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。

[0200] 具体地，图6为本发明实施例所提供的一种终端的结构示意图，如图6所示，该终端包括：

[0201] 获取模块210，获取第一校验信息。其中，第一校验信息存储在终端和服务器上。

[0202] 发送模块220，将第一认证信息发送给服务器，以便服务器对终端进行认证。其中，第一认证信息包括第二校验信息密文，第二校验信息密文由第二校验信息经过白盒加密后生成，第二校验信息与第一校验信息相关。

[0203] 接收模块230，用于接收第二认证信息。其中，第二认证信息包括第五校验信息密文，第五校验信息密文由第五校验信息经过白盒加密后生成，第五校验信息与第二校验信息相关，且第二认证信息与第一认证信息不同。

[0204] 认证模块240，用于在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证。

[0205] 需要特别说明的是，前述对在终端上实现的双向认证方法实施例的解释说明，也适用于本发明实施例所提出的终端，此处不再赘述。

[0206] 为了实现上述实施例，本发明实施例还提出了一种双向认证系统，该系统包括前述实施例所提出的服务器和终端。

[0207] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0208] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0209] 作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0210] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0211] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机装置(可以是个人计算机，服务器，或者网络装置等)或处理器(Processor)执行本发明各个实施例方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0212] 以上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。

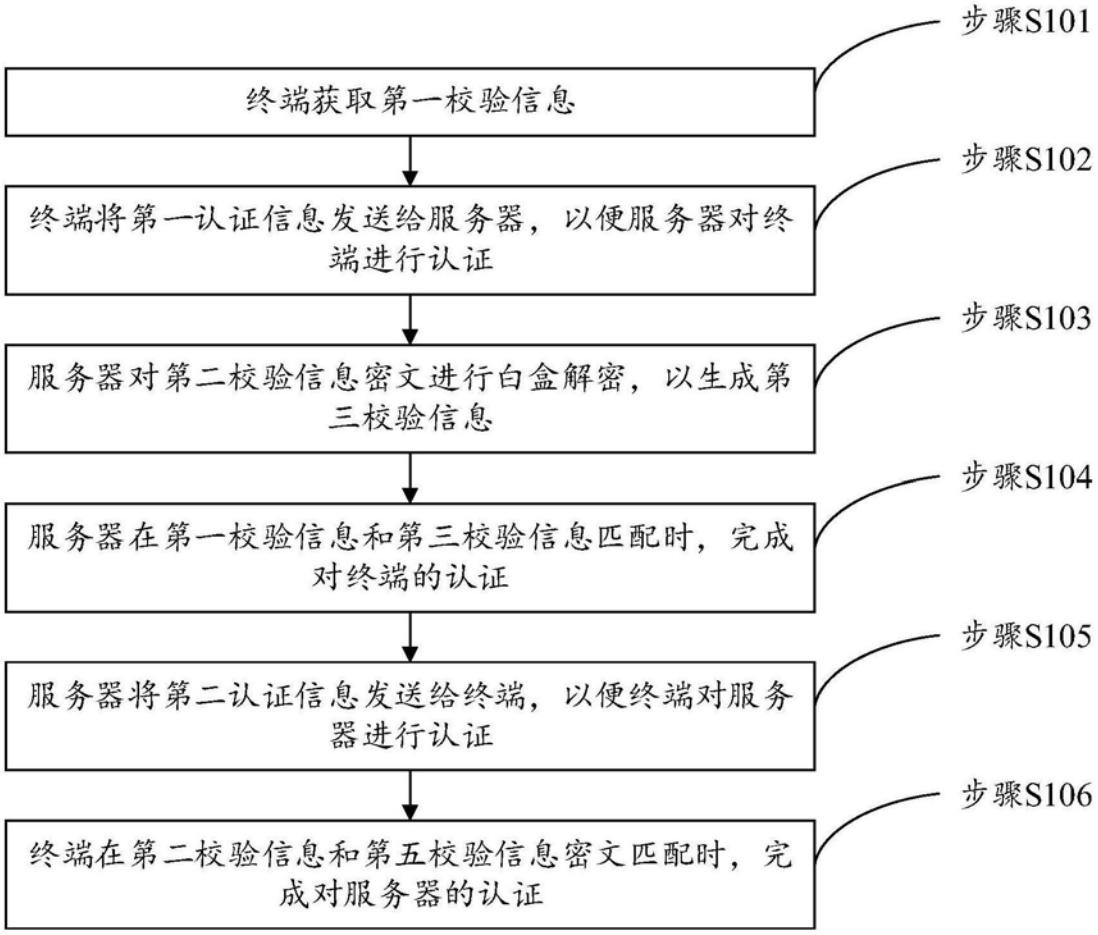

步骤S101
终端获取第一校验信息
步骤S102
终端将第一认证信息发送给服务器，以便服务器对终端进行认证
步骤S103
服务器对第二校验信息密文进行白盒解密，以生成第三校验信息
步骤S104
服务器在第一校验信息和第三校验信息匹配时，完成对终端的认证
步骤S105
服务器将第二认证信息发送给终端，以便终端对服务器进行认证
步骤S106
终端在第二校验信息和第五校验信息密文匹配时，完成对服务器的认证

图1

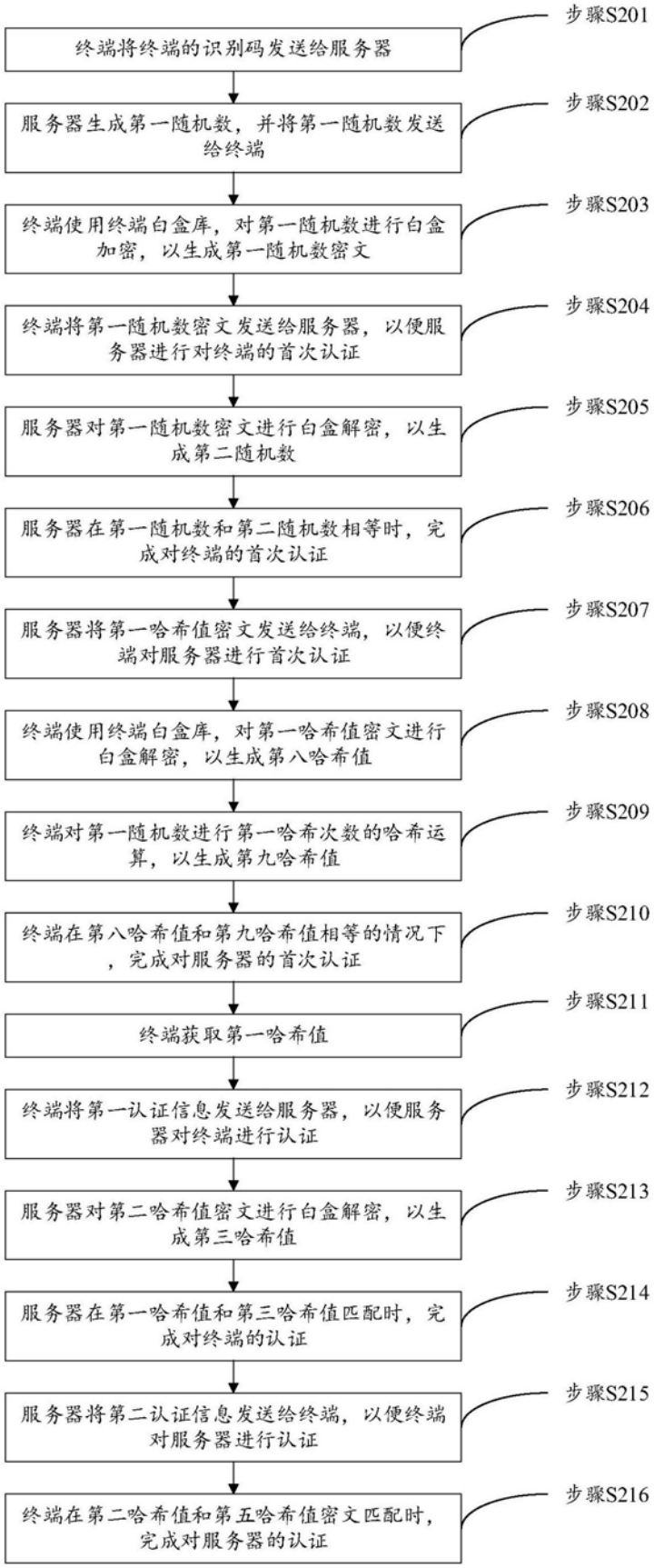

步骤S201
终端将终端的识别码发送给服务器
步骤S202
服务器生成第一随机数，并将第一随机数发送给终端
步骤S203
终端使用终端白盒库，对第一随机数进行白盒加密，以生成第一随机数密文
步骤S204
终端将第一随机数密文发送给服务器，以便服务器进行对终端的首次认证
步骤S205
服务器对第一随机数密文进行白盒解密，以生成第二随机数
步骤S206
服务器在第一随机数和第二随机数相等时，完成对终端的首次认证
步骤S207
服务器将第一哈希值密文发送给终端，以便终端对服务器进行首次认证
步骤S208
终端使用终端白盒库，对第一哈希值密文进行白盒解密，以生成第八哈希值
步骤S209
终端对第一随机数进行第一哈希次数的哈希运算，以生成第九哈希值
步骤S210
终端在第八哈希值和第九哈希值相等的情况下，完成对服务器的首次认证
步骤S211
终端获取第一哈希值
步骤S212
终端将第一认证信息发送给服务器，以便服务器对终端进行认证
步骤S213
服务器对第二哈希值密文进行白盒解密，以生成第三哈希值
步骤S214
服务器在第一哈希值和第三哈希值匹配时，完成对终端的认证
步骤S215
服务器将第二认证信息发送给终端，以便终端对服务器进行认证
步骤S216
终端在第二哈希值和第五哈希值密文匹配时，完成对服务器的认证

图2

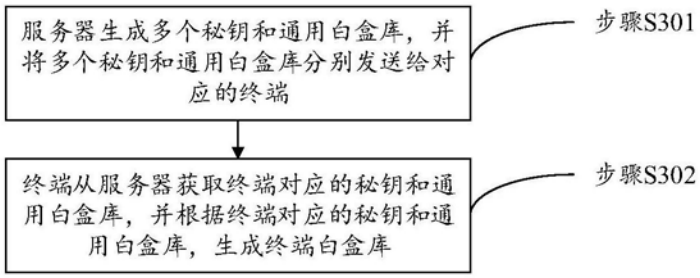

服务器生成多个秘钥和通用白盒库，并将多个秘钥和通用白盒库分别发送给对应的终端
步骤S301
终端从服务器获取终端对应的秘钥和通用白盒库，并根据终端对应的秘钥和通用白盒库，生成终端白盒库
步骤S302

图3

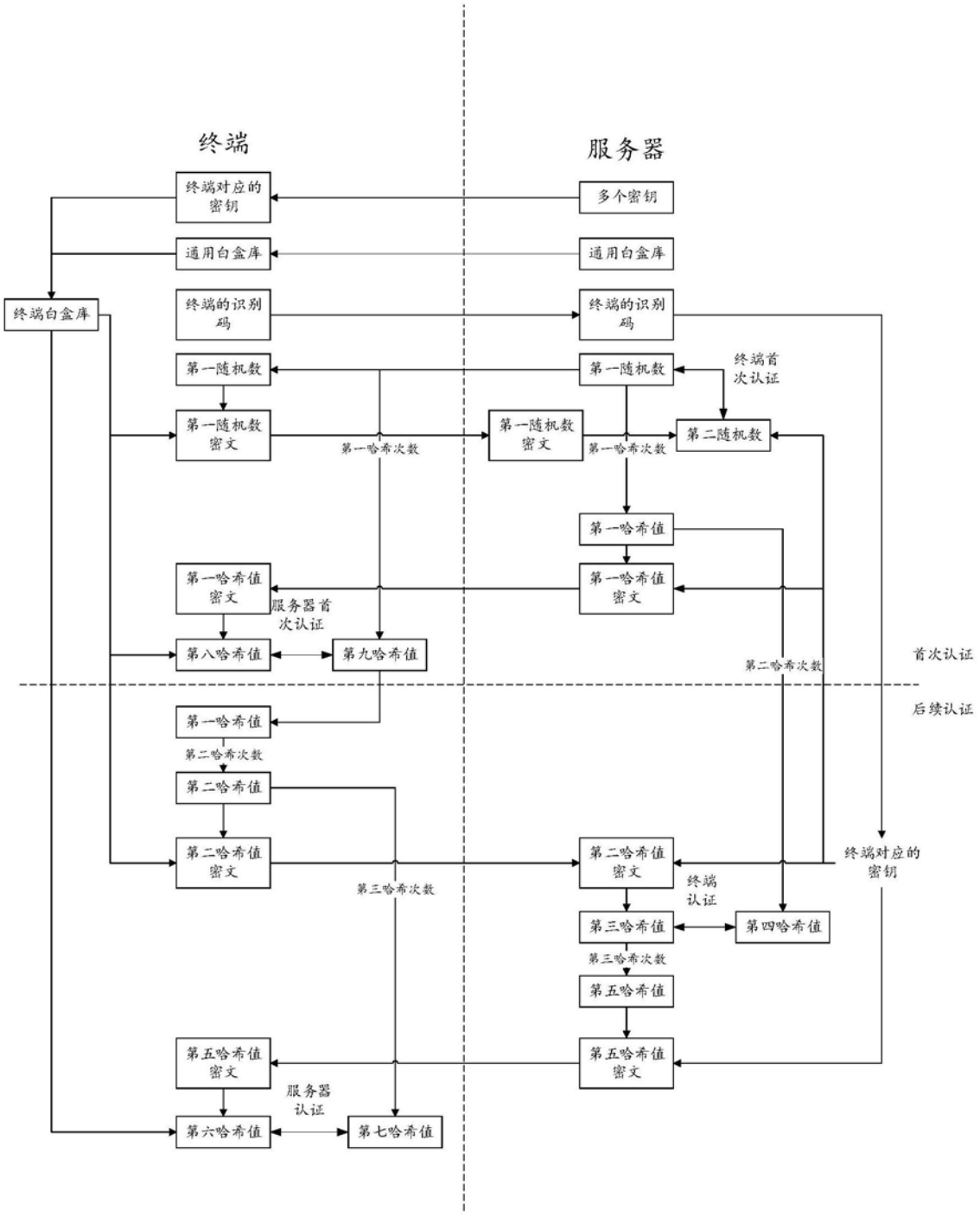

终端
服务器
终端对应的密钥
多个密钥
通用白盒库
通用白盒库
终端白盒库
终端的识别码
终端的识别码
第一随机数
第一随机数
终端首次认证
第一随机数密文
第一哈希次数
第一随机数密文
第一哈希次数
第二随机数
第一哈希值
第一哈希值密文
第一哈希值密文
服务器首次认证
第八哈希值
第九哈希值
第二哈希次数
首次认证
后续认证
第一哈希值
第二哈希次数
第二哈希值
第二哈希值密文
第二哈希值密文
终端对应的密钥
第三哈希次数
终端认证
第三哈希值
第四哈希值
第三哈希次数
第五哈希值
第五哈希值密文
第五哈希值密文
服务器认证
第六哈希值
第七哈希值

图4

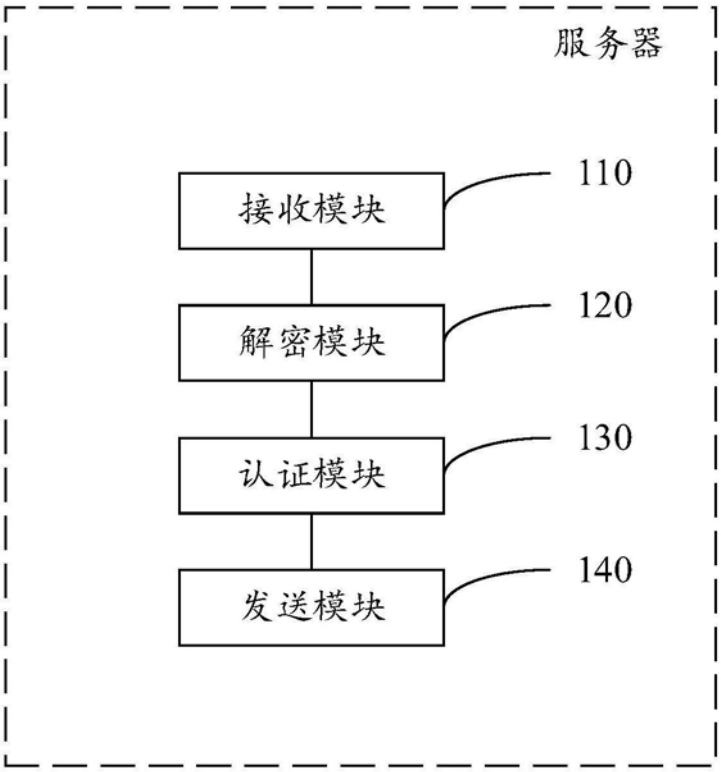

服务器
接收模块
110
解密模块
120
认证模块
130
发送模块
140

图5

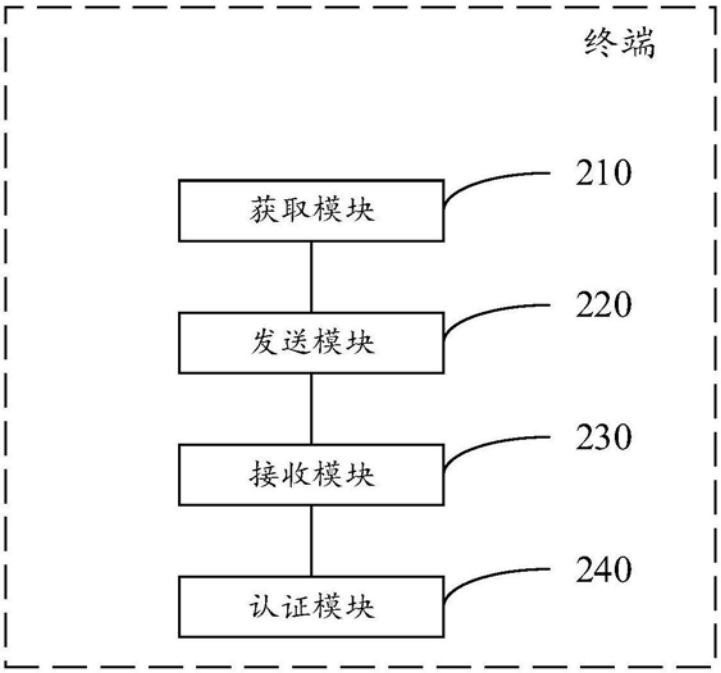

终端
获取模块
210
发送模块
220
接收模块
230
认证模块
240

图6