(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 114172664 A
(43)申请公布日 2022.03.11

(21)申请号 202111483204.1

(22)申请日 2021.12.07

(71)申请人 北京天融信网络安全技术有限公司
地址 100000 北京市海淀区上地东路1号院3号楼四层
申请人 北京天融信科技有限公司
北京天融信软件有限公司

(72)发明人 邓芳

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 李飞

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/1095(2022.01)

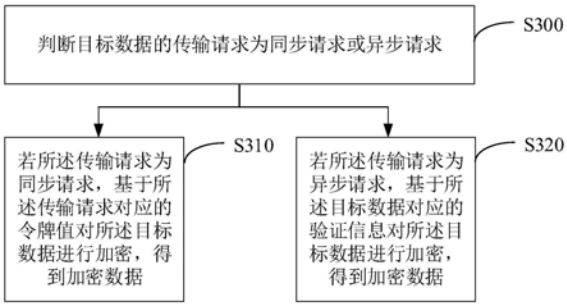
权利要求书2页 说明书13页 附图5页

(54)发明名称

数据加密、数据解密方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种数据加密、数据解密方法、装置、电子设备及存储介质，涉及网络数据安全技术领域。加密方法应用于加密终端，包括：判断目标数据的传输请求为同步请求或异步请求；若传输请求为同步请求，基于传输请求对应的令牌值对目标数据进行加密，得到加密数据；若传输请求为异步请求，基于目标数据对应的验证信息对目标数据进行加密，得到加密数据。解密方法应用于解密终端，包括：获取加密数据，以及对应的传输请求；判断传输请求为同步请求或异步请求；若传输请求为同步请求，基于传输请求对应的令牌值对加密数据进行解密，得到目标数据；若传输请求为异步请求，基于所加密数据对应的验证信息对加密数据进行解密，得到目标数据。



CN 114172664 A

1.一种数据加密方法,其特征在于,应用于加密终端,包括:

判断目标数据的传输请求为同步请求或异步请求;

若所述传输请求为同步请求,基于所述传输请求对应的令牌值对所述目标数据进行加密,得到加密数据;

若所述传输请求为异步请求,基于所述目标数据对应的验证信息对所述目标数据进行加密,得到加密数据。

2.根据权利要求1所述的方法,其特征在于,所述判断目标数据的传输请求为同步请求或异步请求之前,所述方法还包括:

获取用户登录所述加密终端时的用户信息;

获取所述用户信息对应的需要进行加密的目标数据;

基于所述用户信息确定对应的验证信息。

3.根据权利要求2所述的方法,其特征在于,所述基于所述目标数据对应的验证信息对所述目标数据进行加密,得到加密数据,包括:

基于预设的提取规则,从所述验证信息中提取第一密钥;

基于所述第一密钥对所述目标数据进行加密,得到加密数据。

4.根据权利要求1所述的方法,其特征在于,所述基于所述传输请求对应的令牌值对所述目标数据进行加密,得到加密数据,包括:

获取所述传输请求对应的令牌值;

以所述令牌值作为第二密钥对所述目标数据进行加密,得到加密数据。

5.根据权利要求1所述的方法,其特征在于,所述判断目标数据的传输请求为同步请求或异步请求,包括:

确定所述目标数据对应的传输请求;

获取所述传输请求中的请求参数;

基于所述请求参数,判断所述传输请求为同步请求或异步请求。

6.一种数据解密方法,其特征在于,应用于解密终端,包括:

获取加密数据,以及所述加密数据对应的传输请求;

判断所述传输请求为同步请求或异步请求;

若所述传输请求为同步请求,基于所述传输请求对应的令牌值对所述加密数据进行解密,得到目标数据;

若所述传输请求为异步请求,基于所述加密数据对应的验证信息对所述加密数据进行解密,得到目标数据。

7.根据权利要求6所述的方法,其特征在于,所述基于所述加密数据对应的验证信息对所述加密数据进行解密,得到目标数据,包括:

获取存储在标识区域中与所述加密数据对应的验证信息;

以所述验证信息作为第一密钥对所述加密数据进行解密,得到目标数据。

8.根据权利要求6所述的方法,其特征在于,所述基于所述传输请求对应的令牌值对所述加密数据进行解密,得到目标数据,包括:

获取所述解密终端基于所述传输请求生成的对应的令牌值;

以所述令牌值作为第二密钥对所述加密数据进行解密,得到目标数据。

9.根据权利要求6所述的方法，其特征在于，所述方法还包括：

在对所述加密数据进行解密，未得到所述目标数据时，则解密失败，向加密终端发送错误信息。

10.一种数据加密装置，其特征在于，包括：

第一判断模块，用于判断目标数据的传输请求为同步请求或异步请求；

第一同步模块，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据；

第一异步模块，用于若所述传输请求异步，则所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据。

11.一种数据解密装置，其特征在于，包括：

接收模块，用于获取加密数据，以及所述加密数据对应的传输请求；

第二判断模块，用于判断所述传输请求为同步请求或异步请求；

第二同步模块，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据；

第二异步模块，用于若所述传输请求异步，则所述传输请求为异步请求，基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据。

12.一种电子设备，其特征在于，所述电子设备包括存储器和处理器，所述存储器中存储有程序指令，所述处理器运行所述程序指令时，执行权利要求1-9中任一项所述方法中的步骤。

13.一种计算机可读取存储介质，其特征在于，所述可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器运行时，执行权利要求1-9任一项所述方法中的步骤。

数据加密、数据解密方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及网络数据安全技术领域，具体而言，涉及一种数据加密、数据解密方法、装置、电子设备及存储介质。

背景技术

[0002] 在数据传输中，为了防止请求参数被篡改，通常会对参数进行加密处理。加密的过程中最重要的是保证密钥不被窃取，如果密钥是动态变化的话，将会大大提高窃取和破解的难度。现有的做法是利用动态的token(令牌)作为密钥，对传输过程中一些关键的数据做加密，以此来保证相同数据加密后的不同结果。

[0003] 目前的加密方式中，通常是当客户端发起请求时，将最近一次请求生成的token作为对数据进行加密的密钥。服务端用最后一次生成的token为密钥进行解密。解密成功，代表数据未被篡改，解密失败，则代表数据被篡改。然而，由于客户端发起的请求中存在同步请求和异步请求的情况，当前请求若为异步时，会导致此次请求携带的token非最近一次请求返回的token，此时服务端用新生成的token进行解密时，会因密钥不同而解密失败。影响用户对数据进行正常地解密，导致数据加密或解密的效率和有效性较低，对数据进行加密传输的传输效率和安全性较低。

发明内容

[0004] 有鉴于此，本申请实施例的目的在于提供一种数据加密、数据解密方法、装置、电子设备及存储介质，以改善现有技术中存在的数据加密传输的传输效率较低的问题。

[0005] 为了解决上述问题，第一方面，本申请实施例提供了一种数据加密方法，应用于加密终端，包括：

[0006] 判断目标数据的传输请求为同步请求或异步请求；

[0007] 若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据；

[0008] 若所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据。

[0009] 在上述实现方式中，由于目标数据的传输请求中存在同步和异步情况，因此通过对传输请求为同步请求或是异步请求进行判断，能够针对不同的请求，采用不同的方式对目标数据进行加密，得到相应的加密数据。能够针对同步请求或异步请求，结合请求的令牌值或验证码对目标数据进行动态地加密，使数据加密不受请求方式的影响，可以应用在多种加密的请求或接口中，对目标数据进行更加全面地加密，提高对每个目标数据进行加密的随机性，增加了数据加密传输时的攻击难度，提高了数据在传输时的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

[0010] 可选地，所述判断目标数据的传输请求为同步请求或异步请求之前，所述方法还包括：

[0011] 获取用户登录所述加密终端时的用户信息；

[0012] 获取所述用户信息对应的需要进行加密的目标数据；

[0013] 基于所述用户信息确定对应的验证信息。

[0014] 在上述实现方式中，在对目标数据的传输请求的请求类型进行判断之前，还可以通过对用户登录加密终端时的用户信息进行获取，能够在用户信息的基础上获取对应的验证信息，以及该用户对应的需要进行加密的目标数据，以在加密工作中结合动态的验证信息对数据进行加密。能够对多个用户的验证信息以及需要进行加密的目标数据进行针对性地获取，提高了数据加密的准确性和效率。

[0015] 可选地，所述基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据，包括：

[0016] 基于预设的提取规则，从所述验证信息中提取第一密钥；

[0017] 基于所述第一密钥对所述目标数据进行加密，得到加密数据。

[0018] 在上述实现方式中，在传输请求为异步请求时，为了提高数据加密和对应的数据解密的成功率，通过对存储的验证信息进行获取，能够根据预设的提取规则在验证信息中进行提取，得到对应的第一密钥，提高了数据密钥的实时性和有效性。通过动态的验证信息生成的第一密钥对目标数据进行加密，提高了异步请求的数据加密的有效性。

[0019] 可选地，所述基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据，包括：

[0020] 获取所述传输请求对应的令牌值；

[0021] 以所述令牌值作为第二密钥对所述目标数据进行加密，得到加密数据。

[0022] 在上述实现方式中，在传输请求为同步请求时，可以由加密终端获取的解密终端基于传输请求最后一次发送的令牌值，将该令牌值作为加密的第二密钥，对目标数据进行加动态性地加密。以在加密时，能够同时对不同的目标数据进行加密且互相不受影响。

[0023] 可选地，所述判断目标数据的传输请求为同步请求或异步请求，包括：

[0024] 确定所述目标数据对应的传输请求；

[0025] 获取所述传输请求中的请求参数；

[0026] 基于所述请求参数，判断所述传输请求为同步请求或异步请求。

[0027] 在上述实现方式中，由于目标数据的传输请求中存在同步请求或异步请求两种不同情况的请求类型，通过对目标数据对应的传输请求中的请求参数进行获取，能够基于请求参数对传输请求的请求类型进行快速、准确地判断，得到同步请求或异步请求的判断结果。

[0028] 第二方面，本申请实施例还提供了一种数据解密方法，应用于解密终端，包括：

[0029] 获取加密数据，以及所述加密数据对应的传输请求；

[0030] 判断所述传输请求为同步请求或异步请求；

[0031] 若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据；

[0032] 若所述传输请求为异步请求，基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据。

[0033] 在上述实现方式中，在数据的加密传输过程中，在加密终端对数据进行加密并传

输到解密终端后，在解密终端中能够对加密数据进行解密，已完成数据的加密传输流程。在对数据进行解密时，也需要对传输请求为同步请求或是异步请求进行判断，针对不同的请求，采用不同的方式对加密数据进行解密，得到相应的目标数据。针对同步请求或异步请求，结合请求的令牌值或验证码对目标数据进行解密，使数据解密不受请求方式的影响，提高解密的成功率，能够适用于多种解密场景，快速地提取加密数据中传输的目标数据，增加了数据加密传输时的攻击难度，提高了数据在传输时的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

[0034] 可选地，所述基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据，包括：

[0035] 获取存储在标识区域中与所述加密数据对应的验证信息；

[0036] 以所述验证信息作为第一密钥对所述加密数据进行解密，得到目标数据。

[0037] 在上述实现方式中，在传输请求为异步请求时，考虑到异步请求的延时性，为了提高对异步请求的加密数据的解密成功率，通过解密终端与加密终端之间的通信连接，获取解密终端中存储在标识区域的与加密数据对应的验证信息，以在解密工作中结合动态的验证信息，生成对应的第一密钥，对数据进行解密，提高了数据密钥的实时性和有效性。通过动态的验证信息生成的第一密钥对加密数据进行解密，提高了异步请求的数据解密的有效性。能够对多个用户的验证信息以及需要进行解密的目标数据进行针对性地获取，提高了数据解密的准确性和效率。

[0038] 可选地，所述基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据，包括：

[0039] 获取所述解密终端基于所述传输请求生成的对应的令牌值；

[0040] 以所述令牌值作为第二密钥对所述加密数据进行解密，得到目标数据。

[0041] 在上述实现方式中，在传输请求为同步请求时，可以获取解密终端中基于传输请求最后一次生成的令牌值，存储在解密终端中的多个令牌值之间互不影响，将获取的令牌值作为加密的第二密钥，对加密数据进行加解密，以在解密时，能够同时对不同的加密数据进行解密且互相不受影响。

[0042] 可选地，所述方法还包括：

[0043] 在对所述加密数据进行解密，未得到所述目标数据时，则解密失败，向加密终端发送错误信息。

[0044] 在上述实现方式中，在解密终端对加密数据解密失败时，则数据的加密传输过程失败，由解密终端向加密终端发送错误信息，对错误的情况进行反馈和记录。

[0045] 第三方面，本申请实施例还提供了一种数据加密装置，包括：

[0046] 第一判断模块，用于判断目标数据的传输请求为同步请求或异步请求；

[0047] 第一同步模块，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据；

[0048] 第一异步模块，用于若所述传输请求异步，则所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据。

[0049] 第四方面，本申请实施例还提供了一种数据解密装置，包括：

[0050] 接收模块，用于获取加密数据，以及所述加密数据对应的传输请求；

[0051] 第二判断模块，用于判断所述传输请求为同步请求或异步请求；

[0052] 第二同步模块，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据；

[0053] 第二异步模块，用于若所述传输请求异步，则所述传输请求为异步请求，基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据。

[0054] 第五方面，本申请实施例还提供了一种电子设备，所述电子设备包括存储器和处理器，所述存储器中存储有程序指令，所述处理器读取并运行所述程序指令时，执行上述数据加密方法或数据解密方法中任一实现方式中的步骤。

[0055] 第六方面，本申请实施例还提供了一种计算机可读取存储介质，所述可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器读取并运行时，执行上述数据加密方法或数据解密方法中任一实现方式中的步骤。

[0056] 综上所述，本申请提供了一种数据加密、数据解密方法、装置、电子设备及存储介质，能够对数据加密传输过程中的传输请求的请求类型进行判断，并根据不同的请求类型，配合生成的令牌值和验证信息对数据进行不同方式地加密或解密，使数据的加密传输过程不受同步或异步的请求方式的影响，适用于多种加密请求和接口，增加了数据加密的全面性和随机性，提高了数据在传输时加密效率和解密效率，从而提高了加密数据的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

附图说明

[0057] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0058] 图1为本申请实施例提供的一种数据传输的交互示意图；

[0059] 图2为本申请实施例提供的一种数据加密方法的流程示意图；

[0060] 图3为本申请实施例提供的另一种数据加密方法的流程实体图；

[0061] 图4为本申请实施例提供的一种步骤S320的详细流程示意图；

[0062] 图5为本申请实施例提供的一种步骤S310的详细流程示意图；

[0063] 图6为本申请实施例提供的一种步骤S300的详细流程示意图；

[0064] 图7为本申请实施例提供的一种数据解密方法的流程示意图；

[0065] 图8为本申请实施例提供的一种步骤S430的详细流程示意图；

[0066] 图9为本申请实施例提供的一种步骤S420的详细流程示意图；

[0067] 图10为本申请实施例提供的一种数据加密装置的结构示意图；

[0068] 图11为本申请实施例提供的一种数据解密装置的结构示意图。

[0069] 图标：100-加密终端；200-解密终端；500-数据加密装置；510-第一判断模块；520-第一同步模块；530-第一异步模块；600-数据解密装置；610-接收模块；620-第二判断模块；630-第二同步模块；640-第二异步模块。

具体实施方式

[0070] 下面将结合本申请实施例中附图，对本申请实施例中的技术方案进行清楚、完整地描述。显然，所描述的实施例仅仅是本申请实施例的一部分实施例，而不是全部的实施例。基于本申请实施例的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请实施例保护的范围。

[0071] 在多种终端的数据传输过程中，如果传输的数据泄露或者被篡改，可能造成隐私泄露或数据丢失等严重的后果。因此需要对数据进行加密传输，现有的对数据的加密方式分为对称加密和非对称加密。在对称加密算法中，使用的密钥只有一个，数据的发送和接收双方都使用这个密钥对数据进行加密和解密。这就要求加密终端(即客户端)和解密终端(即服务端)中都具有加密的密钥。但是若任意一方的密钥被窃取，就意味着所有的数据相当于明文传输，数据传输的安全性较低，数据易被窃取或篡改。

[0072] 现有技术中，为了提高数据的安全性，会对数据进行动态性地加密。动态性地加密方式能够提高数据被窃取和破解的难度，目前常见的动态加密方式为利用动态的token(令牌值)作为密钥，对数据进行加密，例如，在防御CSRF攻击时，可以使用添加token的方式，当加密终端中请求携带的token跟解密终端中存储的token一致时，请求被放行。为了使token不被猜到，会保证每条请求所携带的token彼此不一致，即每次请求携带的都是重新生成的token，该过程可以包括：加密终端发起请求1，并携带token1到解密终端进行认证，认证成功时，解密终端生成token2，随响应信息一同返回加密终端；加密终端收到token2，携带token2发起请求2到解密终端认证，认证成功时，解密终端生成token3，随响应信息一同返回加密终端；加密终端收到token3，携带token3发起请求3到解密终端认证，认证成功时，解密终端生成token4，随响应信息一同返回加密终端等。

[0073] 在上述的数据加密传输流程中，在加密终端发出请求时，则将解密终端中生成的token作为加密算法的密钥，由加密终端对数据进行加密，由解密终端在接收到加密的数据后，根据生成的token对数据进行解密，解密成功，则代表数据为被篡改，解密失败，则代表数据被篡改。

[0074] 然而，数据的传输请求中存在同步和异步的情况，若当前请求为异步时，会导致此次请求携带的token非最近一次请求返回的token，解密终端用token进行解密时，可能存在密钥不同而解密失败的情况，例如，请求为异步时，在请求1发出的同时，请求2、3、4也在发出，而解密终端只会拿最后一次生成的token作为解密密钥。若请求1使用的是token1进行加密，由于加密终端一直在发请求，此时解密终端最后一次生成的token是token4，解密终端会采用token4进行解密，导致两个密钥不同，造成解密失败的情况。影响用户对数据进行正常地解密，导致数据加密或解密的效率和有效性较低，对数据进行加密传输的传输效率和安全性较低。

[0075] 因此，为了解决上述问题，本申请实施例提供了一种数据加密方法和数据解密方法，应用于各种终端设备，终端设备可以为服务器、个人电脑(Personal Computer，PC)、平板电脑、智能手机、个人数字助理(Personal Digital Assistant，PDA)等具有逻辑计算功能的电子设备，能够对数据进行加密、传输和解密。

[0076] 可选地，电子设备中可以包括存储器、存储控制器、处理器、外设接口、输入输出单元等。电子设备的组件和结构可以根据实际情况进行设置。

[0077] 上述的存储器、存储控制器、处理器、外设接口、输入输出单元各元件相互之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。上述的处理器用于执行存储器中存储的可执行模块。

[0078] 其中，存储器可以是，但不限于，随机存取存储器(Random Access Memory，简称RAM)，只读存储器(Read Only Memory，简称ROM)，可编程只读存储器(Programmable Read-Only Memory，简称PROM)，可擦除只读存储器(Erasable Programmable Read-Only Memory，简称EPROM)，电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory，简称EEPROM)等。其中，存储器用于存储程序，处理器在接收到执行指令后，执行所述程序，本申请实施例任一实施例揭示的过程定义的电子设备所执行的方法可以应用于处理器中，或者由处理器实现。

[0079] 上述的处理器可能是一种集成电路芯片，具有信号的处理能力。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，简称CPU)、网络处理器(Network Processor，简称NP)等；还可以是数字信号处理器(digital signal processor，简称DSP)、专用集成电路(Application Specific Integrated Circuit，简称ASIC)、现场可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0080] 上述的外设接口将各种输入/输出装置耦合至处理器以及存储器。在一些实施例中，外设接口，处理器以及存储控制器可以在单个芯片中实现。在其他一些实例中，他们可以分别由独立的芯片实现。

[0081] 本实施例中的电子设备可以用于执行本申请实施例提供的各个数据加密或数据解密方法中的各个步骤。下面通过几个实施例详细描述数据加密和数据解密方法的实现过程。

[0082] 请参阅图1，图1为本申请实施例提供的一种数据传输的交互示意图，包括以下交互设备：加密终端100和解密终端200。一个或多个(图中仅示出一个)加密终端100通过有线网络或者无线网络与一个或多个(图中仅示出一个)解密终端200进行通信连接，以进行数据通信和交互。

[0083] 其中，加密终端100可以为服务器、个人电脑、平板电脑、智能手机、个人数字助理等具有逻辑计算功能的电子设备，用于根据传输请求的同步或异步类型，对需要进行加密的数据进行对应地加密，得到加密数据，并将加密数据与传输请求发送给解密终端200。

[0084] 解密终端200可以为服务器、个人电脑、平板电脑、智能手机、个人数字助理等具有逻辑计算功能的电子设备，用于接收加密终端100中发送的加密数据和传输请求，并根据传输请求的同步或异步类型，对加密数据进行对应地解密，得到目标数据。由加密终端100和解密终端200实现对数据的加密传输，提高了数据传输的效率和安全性。

[0085] 可选地，加密终端100和解密终端200也可以设置在同一个电子设备中，以加密终端100作为前端，解密终端200作为后端。

[0086] 请参阅图2，图2为本申请实施例提供的一种数据加密方法的流程示意图，该方法可以包括以下步骤：

[0087] 步骤S300，判断目标数据的传输请求为同步请求或异步请求。

[0088] 其中，目标数据中可以包括需要加密的关键信息，例如用户名、密码等敏感信息，由于目标数据的传输请求中存在同步和异步的情况，同步请求为顺序处理的请求，如向服务器发出一个请求时，在服务器没返回结果给客户端之前，需要一直处于等待状态直至服务器将结果返回到客户端，才能执行下一步操作的请求，而异步请求为并行处理的请求，如向服务器发出一个请求时，在服务器没返回结果之前，还是可以执行其他操作的请求。

[0089] 步骤S310，若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据。

[0090] 其中，在传输请求为顺序处理的同步请求时，可以获取传输请求对应的令牌值，即token值，以令牌值作为加密密钥对需要进行加密传输的目标数据进行加密，得到对应的加密数据。

[0091] 步骤S320，若所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据。

[0092] 其中，在传输请求为并行处理的异步请求时，可以获取目标数据对应的验证信息，以验证信息作为加密密钥对需要进行加密传输的目标数据进行加密，得到对应的加密数据。

[0093] 在图2所示的实施例中，能够针对同步请求或异步请求，结合请求的令牌值或验证码对目标数据进行动态地加密，使数据加密不受请求方式的影响，可以应用在多种加密的请求或接口中，对目标数据进行更加全面地加密，提高对每个目标数据进行加密的随机性，增加了数据加密传输时的攻击难度，提高了数据在传输时的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

[0094] 可选地，请参阅图3，图3为本申请实施例提供的另一种数据加密方法的流程实体图，在步骤S300之前，该方法还可以包括步骤Sa-Sc。

[0095] 步骤Sa，获取用户登录所述加密终端时的用户信息。

[0096] 其中，用户在登录加密终端时，例如网页中的登录界面，加密终端会采集用户输入的基本信息作为用户信息，例如用户名、密码等信息，以对用户的身份以及用户对应的目标数据进行识别。

[0097] 步骤Sb，获取所述用户信息对应的需要进行加密的目标数据。

[0098] 其中，基于获取的用户信息，在用户信息中选择需要进行加密的关键信息，例如用户名、密码、传输的数据等。

[0099] 步骤Sc，基于所述用户信息确定对应的验证信息。

[0100] 其中，验证信息可以存储在解密终端中，解密终端的数据无法被篡改，能够有效地保证验证信息的有效性，例如，在同一个浏览器中，同时打开两个tab页签，访问同一个登陆页面，每个tab中生成的验证码也是不同的。验证信息的作用是保护终端，例如网站的安全，一般网站都要通过验证信息来防止机器大规模注册，机器暴力破解数据密码等危害。验证信息通常会在这几种情况下重新生成：手动点击验证信息进行重新生成；登陆出错，自动刷新重新生成；刷新页面重新生成等。在用户进行登录时，加密终端还可以根据用户信息中，由用户基于解密终端中生成并输入加密终端的验证信息，验证信息可以包括数字、字符验证码、线性验证码、二维验证码等多种用于验证的数据。

[0101] 值得说明的是，在根据用户信息确定对应的目标数据和验证信息时，获取的验证

信息与目标数据相对应，获取目标数据与验证信息的步骤的先后顺序可以调换，步骤Sb可以在步骤Sc之前，也可以在步骤Sc之后，步骤Sb与步骤Sc还可以同时进行。

[0102] 在图3所示的实施例中，能够对多个用户的验证信息以及需要进行加密的目标数据进行针对性地获取，提高了数据加密的准确性和效率。

[0103] 可选地，请参阅图4，图4为本申请实施例提供的一种步骤S320的详细流程示意图，步骤S320还可以包括步骤S321-步骤S322。

[0104] 步骤S321，基于预设的提取规则，从所述验证信息中提取第一密钥。

[0105] 其中，在获取的验证信息的基础上，可以采用预设的提取规则对验证信息进行提取，以获取用于加密的第一密钥。预设的提取规则可以为预先设定的多种规则，可以根据用户的应用需求和验证信息的实际情况进行选择和调整，例如对验证信息按照MD5/hash等方式进行散列，在散列后的数据中，采用十六位偶数位、十六位奇数位、隔两位值取一值、隔三位值取一值等多种方式对数据位进行提取，将提取得到的数据组作为加密的第一密钥，存储在加密终端中。

[0106] 值得说明的是，由于验证信息的实时性和唯一性，因此给予验证信息确定的第一密钥为动态的密钥。示例地，第一密钥的存储格式可以为JSON、数组等格式，例如：{“secret”:“数据”}等。

[0107] 步骤S322，基于所述第一密钥对所述目标数据进行加密，得到加密数据。

[0108] 其中，在传输请求为同步请求时，加密终端能够提取存储的第一密钥，基于多种加密算法对目标数据进行加密，得到对应的加密数据。示例地，加密算法可以为AES(Advanced Encryption Standard，高级加密标准)、DES(Data Encryption Standard，数据加密标准)、3DES、IDEA(International Data Encryption Algorithm，国际数据加密算法)、DSA(Digital Signature Algorithm，数字签名算法)等多种不同的加密算法。

[0109] 在图4所示的实施例中，能够根据预设的提取规则在验证信息中进行提取，得到对应的第一密钥，提高了数据密钥的实时性和有效性。通过动态的验证信息生成的第一密钥对目标数据进行加密，提高了异步请求的数据加密的有效性。

[0110] 可选地，请参阅图5，图5为本申请实施例提供的一种步骤S310的详细流程示意图，步骤S310还可以包括步骤S311-步骤S312。

[0111] 步骤S311，获取所述传输请求对应的令牌值。

[0112] 其中，为了提高数据加密的效率，在传输请求为同步请求时，加密终端可以直接获取解密终端中动态生成的令牌值。

[0113] 值得说明的是，解密终端中基于每个请求生成的令牌值都不一致，获取的令牌值为解密终端基于传输请求中时间最近的一次请求反馈给加密终端的令牌值，以保证令牌值的实时性和有效性。

[0114] 步骤S312，以所述令牌值作为第二密钥对所述目标数据进行加密，得到加密数据。

[0115] 其中，在传输请求为同步请求时，加密终端能够直接以接收到的令牌值作为用于加密的动态的第二密钥，对需要进行加密的目标数据进行加密，得到对应的加密数据。由于令牌值的实时性和有效性，能够同时对多个目标数据进行有效加密。

[0116] 在图5所示的实施例中，能够基于令牌值对目标数据进行加动态性地加密，还能够同时对不同的目标数据进行加密且互相不受影响。

[0117] 可选地，请参阅图6，图6为本申请实施例提供的一种步骤S300的详细流程示意图，步骤S300还可以包括步骤S301-步骤S303。

[0118] 步骤S301，确定所述目标数据对应的传输请求。

[0119] 其中，进行请求类型的判断时，先基于需要进行传输的目标数据，确定出对应的传输请求。

[0120] 步骤S302，获取所述传输请求中的请求参数。

[0121] 其中，获取传输请求中包含的多种请求参数，例如请求时间、请求线程、请求要求等多种参数。

[0122] 步骤S303，基于所述请求参数，判断所述传输请求为同步请求或异步请求。

[0123] 其中，可以采用Ajax(Asynchronous Javascript And XML，异步JavaScript和XML)算法，使用async，await函数，基于请求参数对传输请求为同步请求还是异步请求进行判断，得到传输请求的请求类型。

[0124] 在图6所示的实施例中，能够基于请求参数对传输请求的请求类型进行快速、准确地判断，得到同步请求或异步请求的判断结果。

[0125] 请参阅图7，图7为本申请实施例提供的一种数据解密方法的流程示意图，该方法可以包括以下步骤：

[0126] 步骤S400，获取加密数据，以及所述加密数据对应的传输请求。

[0127] 其中，由于解密终端与加密终端在数据传输时通信连接，因此加密终端在对数据加密后，可以将加密数据和对应的传输请求发送给解密终端，由解密终端对加密数据和对应的传输请求进行接收。

[0128] 步骤S410，判断所述传输请求为同步请求或异步请求。

[0129] 其中，解密终端在解密时，也会对传输请求的请求类型进行判断，判断的方式可以与图6中所示的实施例相同，不在进行赘述。

[0130] 步骤S420，若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据。

[0131] 其中，在判断传输请求为顺序处理的同步请求时，可以获取传输请求对应的令牌值，即token值，以令牌值作为解密密钥对需要进行解密的加密数据进行解密，得到对应的目标数据。

[0132] 步骤S430，若所述传输请求为异步请求，基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据。

[0133] 其中，在判断传输请求为并行处理的异步请求时，可以获取加密数据对应的验证信息，以验证信息作为解密密钥对需要进行解密的加密数据进行解密，得到对应的目标数据。

[0134] 值得说明的是，在得到目标数据后，解密成功，释放加密数据的传输请求，完成对数据的加密传输，继续执行后续的操作。在对加密数据进行解密，未得到目标数据时，则解密失败，向加密终端发送错误信息，能够在数据的加密传输过程失败时，由解密终端向加密终端发送错误信息，对错误的情况进行反馈和记录，以供用户对错误情况进行了解和查看，并继续执行后续的加密传输工作。

[0135] 值得说明的是，在对数据进行解密时，解密终端可以获取多个加密终端发送的多

个加密数据，加密终端可以为采用本申请提供的数据加密方法对数据进行加密的终端，也可以为采用其他方式对数据进行加密的终端，能够对不同方式进行加密的加密数据同时进行解密，适用于多种应用场景，提高了解密的效率和实用性。在进行加密时，不同的加密终端可以对加密数据添加不同的标识信息，例如编号、前缀、后缀等方式，对使用不同方式进行加密的加密数据进行区分。解密终端在接收加密数据后，可以基于加密数据中的标识信息对加密数据进行分类，在加密数据为本申请提供的数据加密方法进行加密的数据时，采用步骤S410-S430的步骤对加密数据进行解密，在加密数据为其他方式进行加密的数据时，可以直接使用步骤S420中的方式对数据进行解密。解密终端在接收加密数据后，还可以优先使用步骤S420中的方式对加密数据进行解密，在解密失败时，再采用使用步骤S430中的方式对加密数据进行解密，在两种解密方式都失败时，再向加密终端反馈错误信息。

[0136] 在图7所示的实施例中，能够针对同步请求或异步请求，结合请求的令牌值或验证码对目标数据进行解密，使数据解密不受请求方式的影响，提高解密的成功率和效率，能够适用于多种解密场景，快速地提取加密数据中传输的目标数据，增加了数据加密传输时的攻击难度，提高了数据在传输时的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

[0137] 可选地，请参阅图8，图8为本申请实施例提供的一种步骤S430的详细流程示意图，步骤S430还可以包括步骤S431-步骤S432。

[0138] 步骤S431，获取存储在标识区域中与所述加密数据对应的验证信息。

[0139] 其中，由于解密终端中数据无法被篡改，能够有效地保证验证信息的有效性，因此，可以将加密信息对应的验证信息存储在标识区域中，标识区域为能够唯一标识当前会话的数组或集合，以对验证信息进行分区存储，使多个验证信息之间互不影响，提高验证信息的安全性。示例地，标识区域可以设置为session(会话控制)[‘唯一标识’][‘验证码’]等。在需要进行解密时，能够从标识区域中对加密数据对应的额验证信息进行提取。

[0140] 步骤S432，以所述验证信息作为第一密钥对所述加密数据进行解密，得到目标数据。

[0141] 其中，在进行解密时，可以基于提取的验证信息作为第一密钥对加密数据进行解密，还可以预设的提取规则在验证信息中进行提取，以提取得到的数据作为第一密钥，以第一密钥作为动态的解密密钥对加密数据进行解密，得到对应的目标数据。

[0142] 在图8所示的实施例中，通过动态的验证信息生成的第一密钥对加密数据进行解密，提高了异步请求的数据解密的有效性。能够对多个用户的验证信息以及需要进行解密的目标数据进行针对性地获取，提高了数据解密的准确性和效率。

[0143] 可选地，请参阅图9，图9为本申请实施例提供的一种步骤S420的详细流程示意图，步骤S420还可以包括步骤S421-步骤S422。

[0144] 步骤S421，获取所述解密终端基于所述传输请求生成的对应的令牌值。

[0145] 其中，解密终端中基于每个请求生成的令牌值都不一致，获取的令牌值为解密终端基于传输请求中时间最近的一次请求反馈给加密终端的令牌值，以保证令牌值的实时性和有效性。

[0146] 步骤S422，以所述令牌值作为第二密钥对所述加密数据进行解密，得到目标数据。

[0147] 其中，在传输请求为同步请求时，解密终端能够直接生成的令牌值作为用于解密

的动态的第二密钥，对需要进行解密的加密数据进行解密，得到对应的解密数据。由于令牌值的实时性和有效性，能够同时对多个加密数据进行有效解密。

[0148] 在图9所示的实施例中，将获取的令牌值作为加密的第二密钥，对加密数据进行加解密，以在解密时，能够同时对不同的加密数据进行解密且互相不受影响。

[0149] 请参阅图10，图10为本申请实施例提供的一种数据加密装置的结构示意图，数据加密装置500可以包括：

[0150] 第一判断模块510，用于判断目标数据的传输请求为同步请求或异步请求；

[0151] 第一同步模块520，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据；

[0152] 第一异步模块530，用于若所述传输请求异步，则所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据。

[0153] 在一可选的实施方式中，数据加密装置500还可以包括预处理模块，用于获取用户登录所述加密终端时的用户信息；获取所述用户信息对应的需要进行加密的目标数据；基于所述用户信息确定对应的验证信息。

[0154] 在一可选的实施方式中，第一异步模块530中还可以包括第一提取子模块和第一加密子模块；

[0155] 第一提取子模块，用于基于预设的提取规则，从所述验证信息中提取第一密钥；

[0156] 第一加密子模块，用于基于所述第一密钥对所述目标数据进行加密，得到加密数据。

[0157] 在一可选的实施方式中，第一同步模块520中还可以包括获取子模块和第二加密子模块；

[0158] 获取子模块，用于获取所述传输请求对应的令牌值；

[0159] 第二加密子模块，用于以所述令牌值作为第二密钥对所述目标数据进行加密，得到加密数据。

[0160] 在一可选的实施方式中，第一判断模块510中还可以包括确定子模块，参数子模块和判断子模块；

[0161] 确定子模块，用于确定所述目标数据对应的传输请求；

[0162] 参数子模块，用于获取所述传输请求中的请求参数；

[0163] 判断子模块，用于基于所述请求参数，判断所述传输请求为同步请求或异步请求。

[0164] 由于本申请实施例中的装置解决问题的原理与前述的数据加密方法的实施例相似，因此本实施例中的装置的实施可以参见上述数据加密方法的实施例中的描述，重复之处不再赘述。

[0165] 请参阅图11，图11为本申请实施例提供的一种数据解密装置的结构示意图，数据解密装置600中可以包括：

[0166] 接收模块610，用于获取加密数据，以及所述加密数据对应的传输请求；

[0167] 第二判断模块620，用于判断所述传输请求为同步请求或异步请求；

[0168] 第二同步模块630，用于若所述传输请求同步，则所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据；

[0169] 第二异步模块640，用于若所述传输请求异步，则所述传输请求为异步请求，基于

所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据。

[0170] 在一可选的实施方式中，第二异步模块640中还可以包括第二提取子模块和第一解密子模块；

[0171] 第二提取子模块，用于获取存储在标识区域中与所述加密数据对应的验证信息；

[0172] 第一解密子模块，用于以所述验证信息作为第一密钥对所述加密数据进行解密，得到目标数据。

[0173] 在一可选的实施方式中，第二同步模块630中还可以包括生成子模块和第二解密子模块；

[0174] 生成子模块，用于获取所述解密终端基于所述传输请求生成的对应的令牌值；

[0175] 第二解密子模块，用于以所述令牌值作为第二密钥对所述加密数据进行解密，得到目标数据。

[0176] 在一可选的实施方式中，数据解密装置600中还可以包括反馈模块，用于在对所述加密数据进行解密，未得到所述目标数据时，则解密失败，向加密终端发送错误信息。

[0177] 由于本申请实施例中的装置解决问题的原理与前述的数据解密方法的实施例相似，因此本实施例中的装置的实施可以参见上述数据解密方法的实施例中的描述，重复之处不再赘述。

[0178] 本申请实施例还提供了一种电子设备，该电子设备包括存储器和处理器，所述存储器中存储有程序指令，所述处理器读取并运行所述程序指令时，执行本实施例提供的数据加密方法或数据解密方法中任一项所述方法中的步骤。

[0179] 本申请实施例还提供了一种计算机可读取存储介质，所述可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器读取并运行时，执行本实施例提供的数据加密方法或数据解密方法中任一项所述方法中的步骤。

[0180] 综上所述，本申请实施例提供了一种数据加密、数据解密方法、装置、电子设备及存储介质，能够对数据加密传输过程中的传输请求的请求类型进行判断，并根据不同的请求类型，配合生成的令牌值和验证信息对数据进行不同方式地加密或解密，使数据的加密传输过程不受同步或异步的请求方式的影响，适用于多种加密请求和接口，增加了数据加密的全面性和随机性，提高了数据在传输时加密效率和解密效率，从而提高了加密数据的传输效率和安全性，减少信息的被泄露或篡改的不利情况。

[0181] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的框图显示了根据本申请的多个实施例的设备的可能实现的体系架构、功能和操作。在这点上，框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现方式中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图中的每个方框、以及框图的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0182] 另外，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0183] 所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。因此本实施例还提供了一种可读取存储介质中存储有计算机程序指令，所述计算机程序指令被一处理器读取并运行时，执行区块数据存储方法中任一项所述方法中的步骤。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品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设备(可以是个人计算机，服务器，或者网络设备等)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，RanDom Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0184] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0185] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。

[0186] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

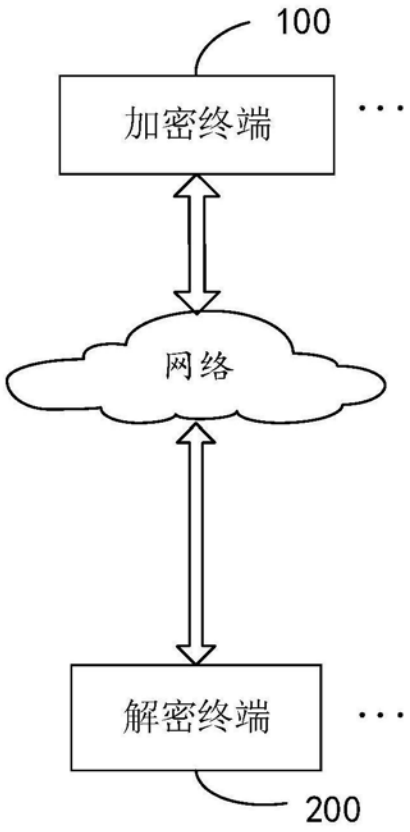

100
加密终端
网络
解密终端
200

图1

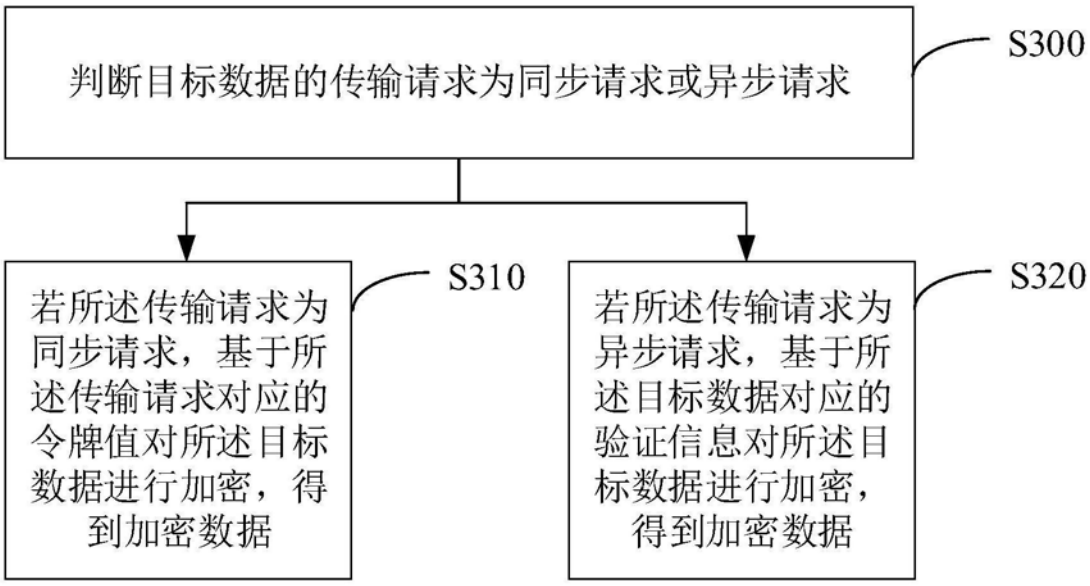

判断目标数据的传输请求为同步请求或异步请求
S300
若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述目标数据进行加密，得到加密数据
S310
若所述传输请求为异步请求，基于所述目标数据对应的验证信息对所述目标数据进行加密，得到加密数据
S320

图2

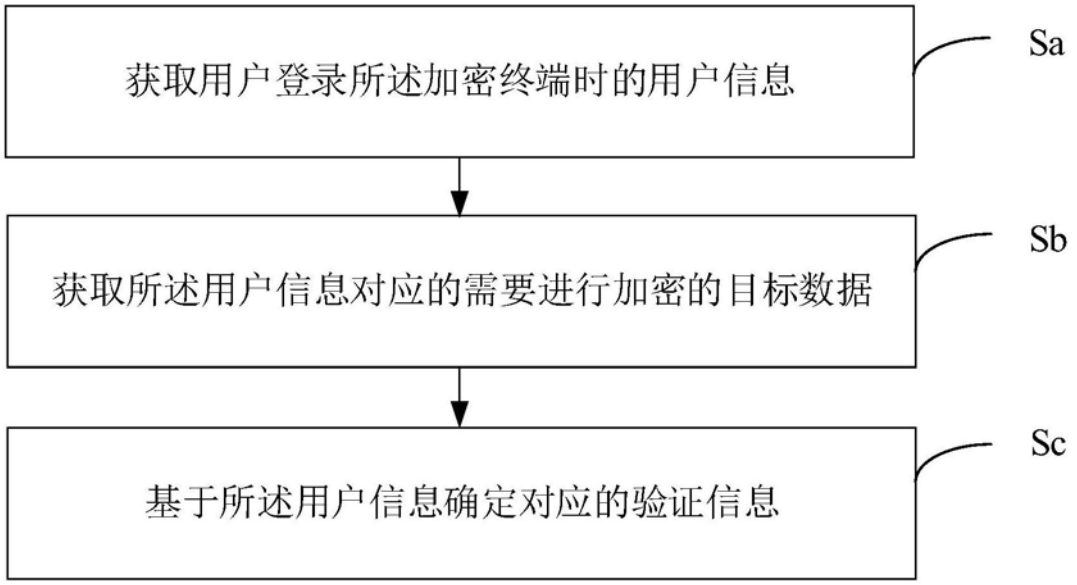

获取用户登录所述加密终端时的用户信息
Sa
获取所述用户信息对应的需要进行加密的目标数据
Sb
基于所述用户信息确定对应的验证信息
Sc

图3

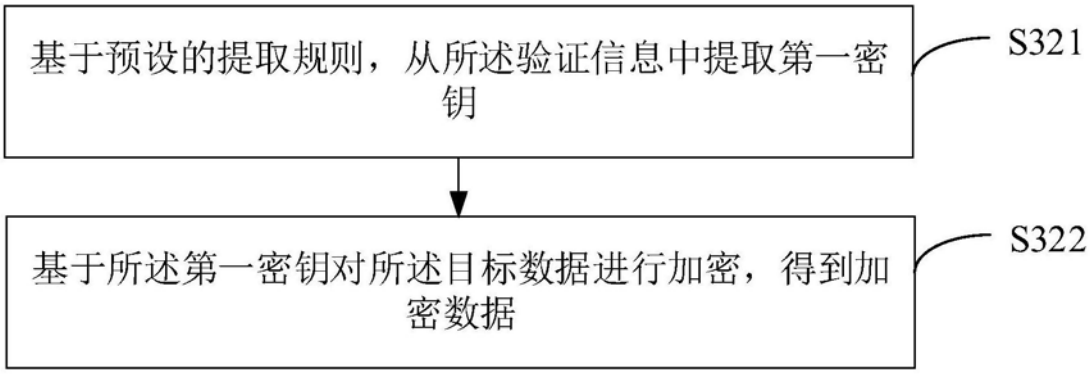

基于预设的提取规则，从所述验证信息中提取第一密钥
S321
基于所述第一密钥对所述目标数据进行加密，得到加密数据
S322

图4

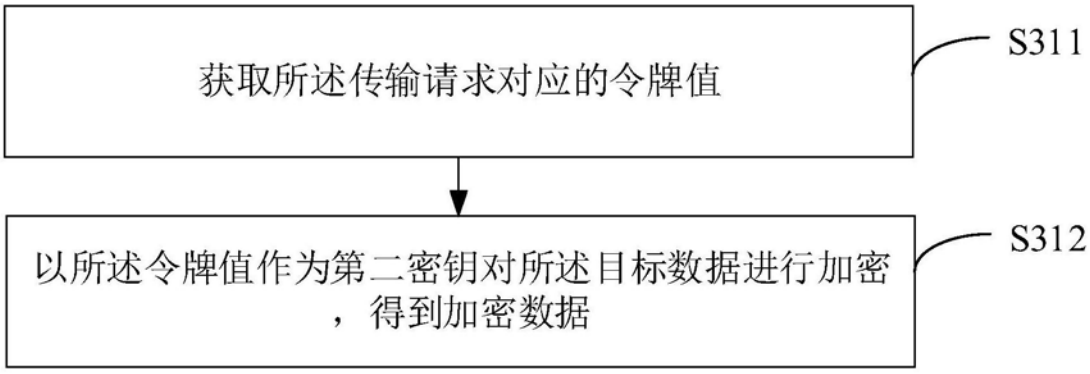

获取所述传输请求对应的令牌值
S311
以所述令牌值作为第二密钥对所述目标数据进行加密，得到加密数据
S312

图5

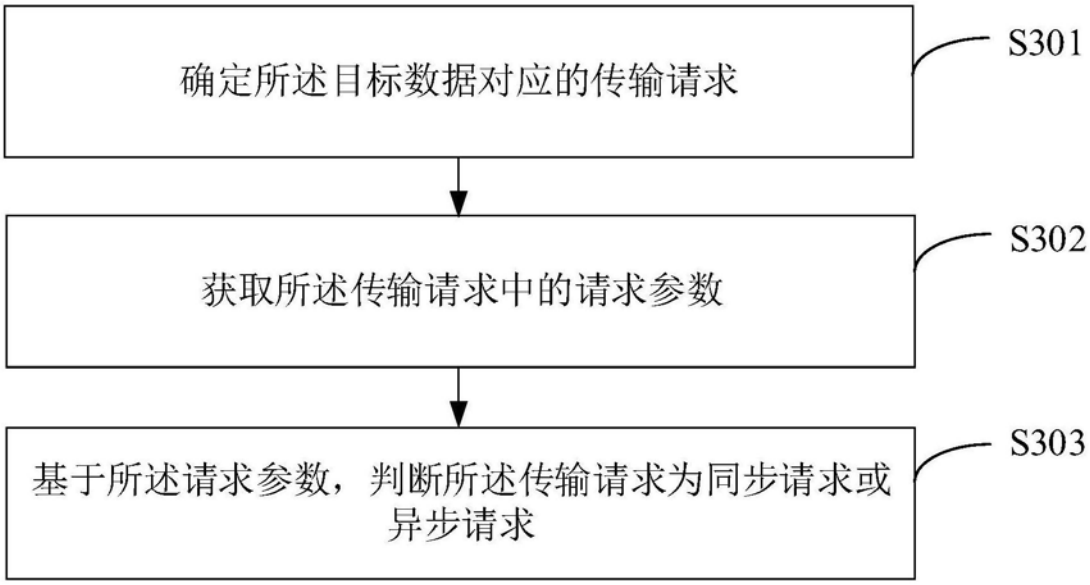

确定所述目标数据对应的传输请求
S301
获取所述传输请求中的请求参数
S302
基于所述请求参数，判断所述传输请求为同步请求或异步请求
S303

图6

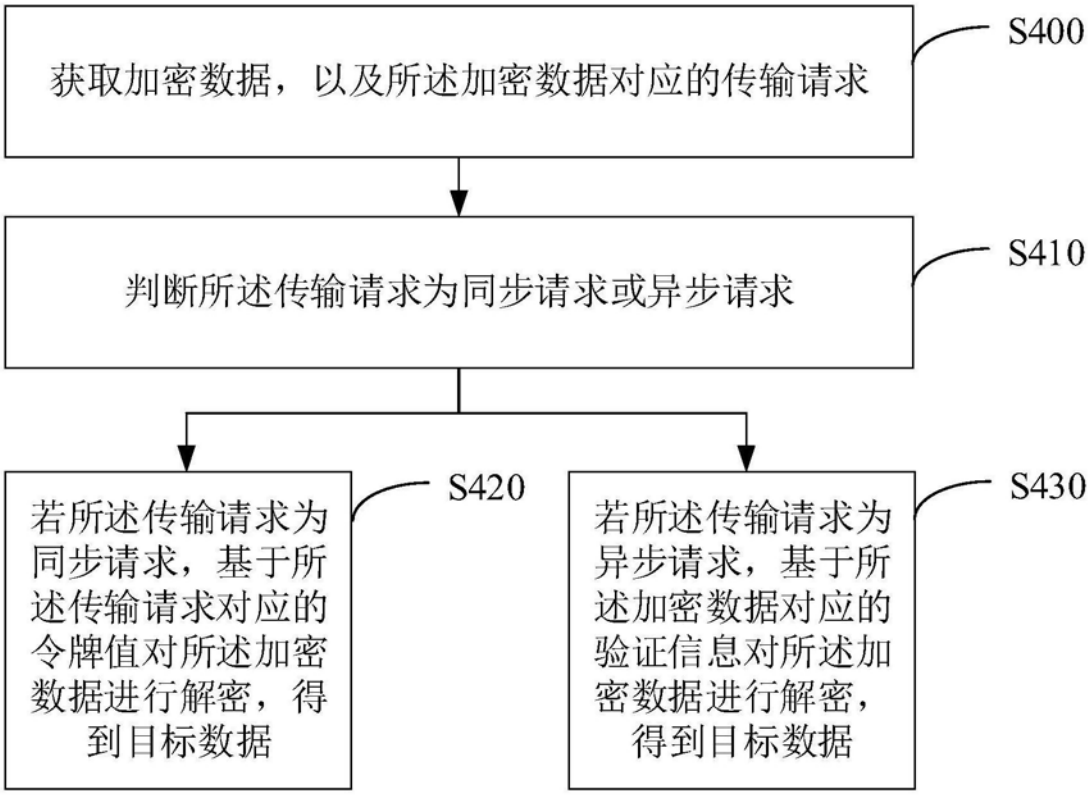

获取加密数据，以及所述加密数据对应的传输请求
S400
判断所述传输请求为同步请求或异步请求
S410
若所述传输请求为同步请求，基于所述传输请求对应的令牌值对所述加密数据进行解密，得到目标数据
S420
若所述传输请求为异步请求，基于所述加密数据对应的验证信息对所述加密数据进行解密，得到目标数据
S430

图7

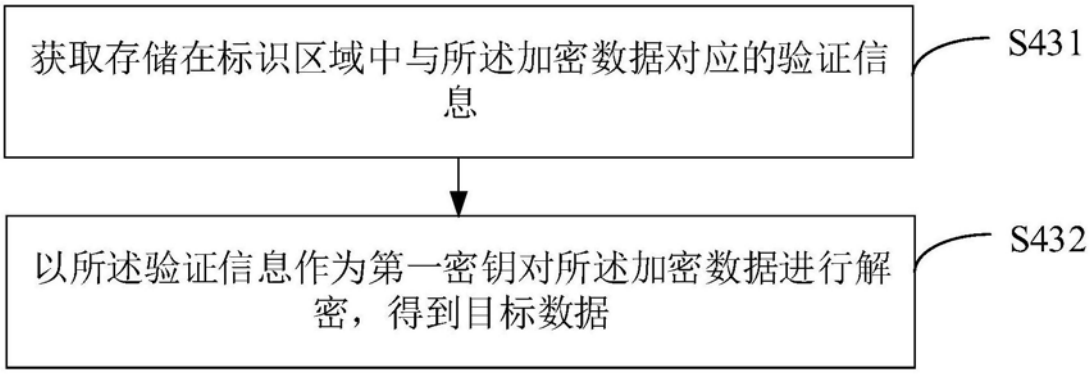

获取存储在标识区域中与所述加密数据对应的验证信息
S431
以所述验证信息作为第一密钥对所述加密数据进行解密，得到目标数据
S432

图8

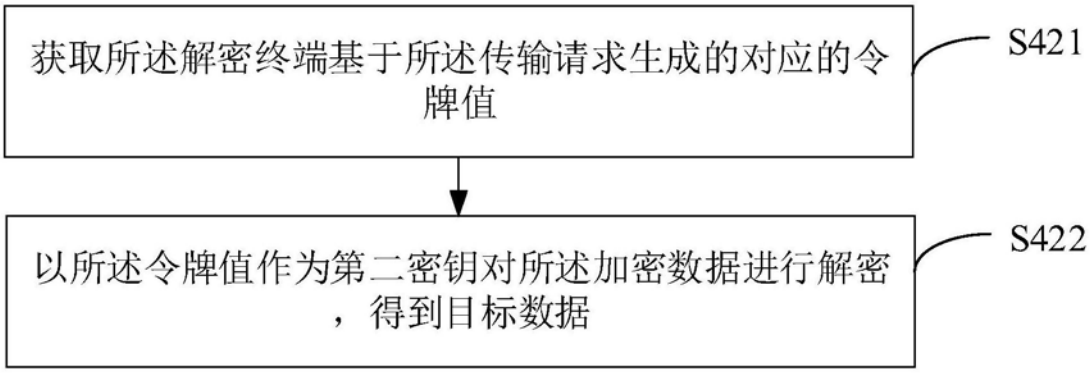

获取所述解密终端基于所述传输请求生成的对应的令牌值
S421
以所述令牌值作为第二密钥对所述加密数据进行解密，得到目标数据
S422

图9

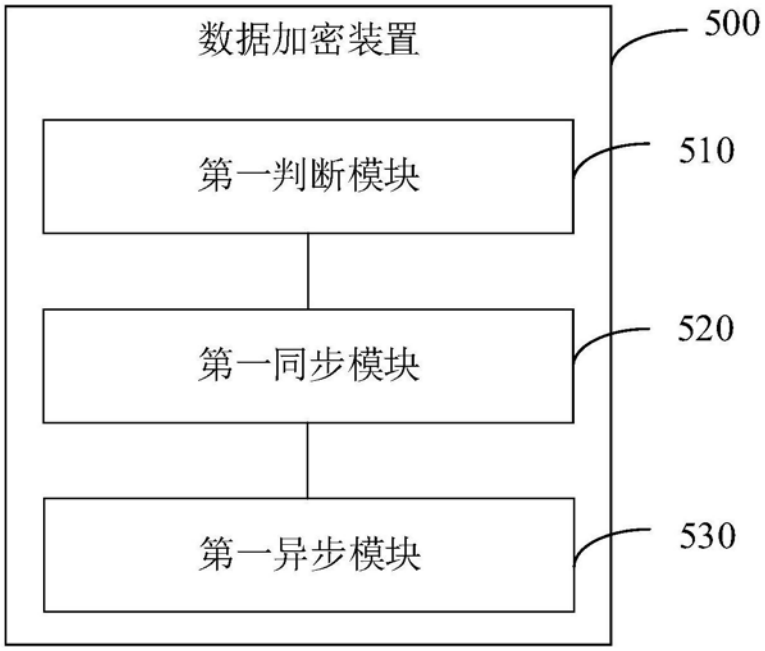

数据加密装置
500
第一判断模块
510
第一同步模块
520
第一异步模块
530

图10

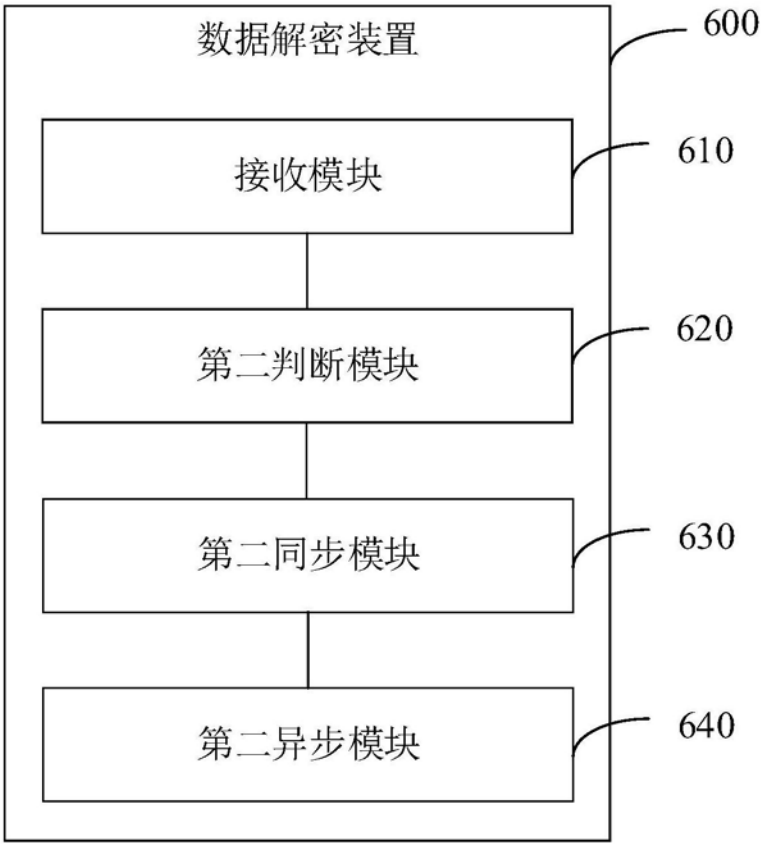


图11