

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2019 年 9 月 26 日 (26.09.2019)



(10) 国际公布号
WO 2019/178942 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) **H04L 29/08** (2006.01)

(21) 国际申请号: PCT/CN2018/088676

(22) 国际申请日: 2018 年 5 月 28 日 (28.05.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810247194.3 2018年3月23日 (23.03.2018) CN

(71) 申请人: 网宿科技股份有限公司 (WANGSU SCIENCE & TECHNOLOGY CO., LTD.) [CN/CN];
中国上海市徐汇区斜土路2899号甲光启文化
广场A幢5楼, Shanghai 200030 (CN)。

(72) 发明人: 林金棚(LIN, Jinpeng); 中国上海市徐汇区斜土路2899号甲光启文化广场A幢5楼, Shanghai 200030 (CN)。 王文灿(WANG, Wencan); 中国上海市徐汇区斜土路2899号甲光启文化广场A幢5楼, Shanghai 200030 (CN)。 董曙佳(DONG, Shujia); 中国上海市徐汇区斜土路2899号甲光启文化广场A幢5楼, Shanghai 200030 (CN)。

(74) 代理人: 上海晨皓知识产权代理事务所(普通合伙) (SHANGHAI CHENHAO INTELLECTUAL PROPERTY LAW FIRM GENERAL PARTNERSHIP); 中国上海市黄浦区制造局路787号二幢202B室, Shanghai 200011 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: METHOD AND SYSTEM FOR PERFORMING SSL HANDSHAKE

(54) 发明名称: 一种进行SSL握手的方法和系统

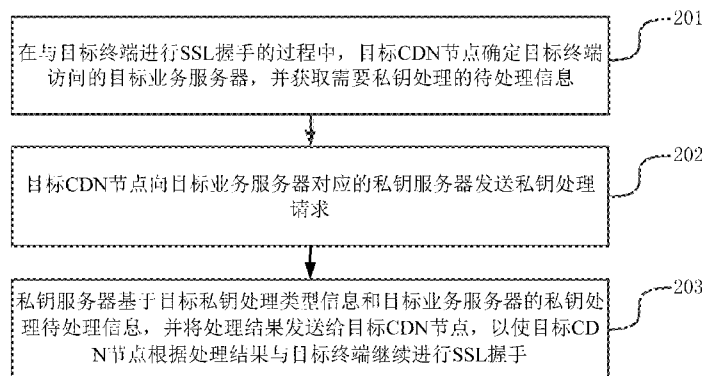


图 2

- 201 During an SSL handshake with a target terminal, a target CDN node determining a target service server accessed by the target terminal and obtaining information to be processed which requires a private key for processing
- 202 The target CDN node sending a private key processing request to a private key server corresponding to the target service server
- 203 The private key server processing the information to be processed on the basis of target private key processing type information and a private key of the target service server and sending a processing result to the target CDN node so that the target CDN node may continue to perform the SSL handshake with the target terminal according to the processing result

(57) Abstract: The present application belongs to the technical field of wireless communications and disclosed thereby are a method and system for performing an SSL Handshake. Said method comprises: during an SSL handshake with a target terminal, a target CDN node determining a target service server accessed by the target terminal and obtaining information to be processed which requires a private key for processing; the target CDN node sending a private key processing request to a private key server corresponding to the target service server, the private key processing request carrying the information to be processed and target private key processing type

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

information; the private key server processing the information to be processed on the basis of the target private key processing type information and a private key of the target service server and sending a processing result to the target CDN node so that the target CDN node may continue to perform the SSL handshake with the target terminal according to the processing result. By employing the present application, the security of the private key and the service quality of business service and CDN service may be guaranteed.

(57) 摘要: 本申请公开了一种进行SSL握手的方法和系统, 属于无线通信技术领域。所述方法包括: 在与目标终端进行SSL握手的过程中, 目标CDN节点确定所述目标终端访问的目标业务服务器, 并获取需要私钥处理的待处理信息; 所述目标CDN节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求, 所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息; 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息, 并将处理结果发送给所述目标CDN节点, 以使所述目标CDN节点根据所述处理结果与所述目标终端继续进行SSL握手。采用本申请, 可以保证私钥的安全性, 以及业务服务和CDN服务的服务质量。

一种进行 SSL 握手的方法和系统

技术领域

- 5 [0001] 本申请涉及无线通信技术领域，特别涉及一种进行 SSL 握手的方法和系统。

背景技术

- [0002] 随着互联网的快速发展，人们对于网络传输安全性的要求也越来越高，
10 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，基于安全套接层的超文本传输协议）协议因此出现，HTTPS 协议可以认为是 HTTP（Hyper Text Transfer Protocol，超文本传输协议）协议和 SSL/TLS（Secure Sockets Layer/Transport Layer Security，安全套接层/传输层安全）协议的组合。其中，SSL/TLS 协议作用在 HTTP 协议之下，用于对传输的数据进行加密处理，以保证数据在网络上传输的过程中不会被截取或窃听。
15

- [0003] 每个业务服务器上可以预先配置有 SSL 证书，SSL 证书是由受信任的数字证书颁发机构 CA（Certification Authority，电子认证机构），在验证业务服务器的身份后颁发给业务服务器的，具有服务器身份验证和数据加密功能，每个 SSL 证书都包括一个公钥和一个私钥。当终端通过 HTTPS 协议访问业务服务器
20 时，需要先与业务服务器进行 SSL 握手，而在 SSL 握手过程中，终端和业务服务器需要协商使用的加密算法，如果加密算法是 RSA 算法，则业务服务器需要使用 SSL 证书的私钥对加密后的预主密码进行解密，如果加密算法是 DH 算法，则业务服务器需要使用 SSL 证书的私钥对 DH 参数进行签名。

[0004] 在实现本申请的过程中，发明人发现现有技术至少存在以下问题：

- 25 [0005] 在 CDN（Content Delivery Network，内容分发网络）服务架构下，终端往往从 CDN 节点获取数据，故而终端需要和 CDN 节点进行 SSL 握手。然而，

一方面，由于保密需要，一些业务服务器无法将私钥提供给外界，这些业务服务器则无法使用 CDN 服务，另一方面，SSL 握手中的私钥处理需要消耗较大的 CPU 处理资源，尤其在 SSL 握手的并发量较大的情况下，CDN 节点提供的 CDN 服务可能会受到较大影响。

5

发明内容

[0006] 为了解决现有技术的问题，本申请实施例提供了一种进行 SSL 握手的方法和系统。所述技术方案如下：

[0007] 第一方面，提供了一种进行 SSL 握手的方法，所述方法包括：

10 [0008] 在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息；

[0009] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息；

15 [0010] 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手。

[0011] 可选的，所述在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，包括：

20 [0012] 在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中，目标 CDN 节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取所述目标终端发送的客户端密钥交换消息中携带的加密后的所述目标终端生成的预主密钥；

[0013] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型，包括：

25 [0014] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处

理请求，所述私钥处理请求携带有加密后的预主密钥和与所述目标终端协商的目标解密算法的算法标识；

[0015] 所述私钥服务器基于所述目标私钥处理类型和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手，包括：

[0016] 所述私钥服务器按照所述目标解密算法，使用所述目标业务服务器的私钥对所述加密后的预主密钥进行解密，并将解密得到的预主密钥发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述解密得到的预主密钥与所述目标终端继续进行 SSL 握手。

[0017] 可选的，所述在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，包括：

[0018] 在与目标终端进行 TLS1.2 协议下的 DH 握手的过程中，目标 CDN 节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的 DH 参数；

[0019] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息，包括：

[0020] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述 DH 参数和与所述目标终端协商的第一签名算法的算法标识；

[0021] 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手，包括：

[0022] 所述私钥服务器按照所述第一签名算法，使用所述目标业务服务器的私钥对所述 DH 参数进行签名，并将签名后的 DH 参数发送给所述目标 CDN 节点，

以使所述目标 CDN 节点根据所述签名后的 DH 参数与所述目标终端继续进行 SSL 握手。

[0023] 可选的,所述在与目标终端进行 SSL 握手的过程中,目标 CDN 节点确定所述目标终端访问的目标业务服务器,并获取需要私钥处理的待处理信息,包括:

[0024] 在与目标终端进行 TLS1.3 协议下的 DH 握手的过程中,目标 CDN 节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器,并获取本地生成的哈希参数,所述哈希参数基于和所述目标终端交互的握手数据包和所述目标业务服务器的 SSL 证书生成;

[0025] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求,所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息,包括:

[0026] 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求,所述私钥处理请求携带有所述哈希参数和与所述目标终端协商的第二签名算法的算法标识;

[0027] 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息,并将处理结果发送给所述目标 CDN 节点,以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手,包括:

[0028] 所述私钥服务器按照所述第二签名算法,使用所述目标业务服务器的私钥对所述哈希参数进行签名,并将签名后的哈希参数发送给所述目标 CDN 节点,以使所述目标 CDN 节点根据所述签名后的哈希参数与所述目标终端继续进行 SSL 握手。

[0029] 可选的,所述私钥处理请求中还携带有所述目标业务服务器的 SSL 证书标识;

[0030] 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息之前,还包括:

[0031] 所述私钥服务器在本地存储的私钥列表中查找所述目标业务服务器的SSL证书标识对应的所述目标业务服务器的私钥。

[0032] 可选的, 所述私钥处理请求为 http1.0 或 http2.0 请求。

[0033] 可选的, 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求, 包括:

[0034] 所述目标 CDN 节点确定指向所述目标业务服务器对应私钥服务器的下一跳 CDN 节点;

[0035] 所述目标 CDN 节点与所述下一跳 CDN 节点建立 SSL 双向认证通道, 通过所述 SSL 双向认证通道向所述下一跳 CDN 节点发送私钥处理请求, 以使所述下一跳 CDN 节点向所述私钥服务器发送私钥处理请求。

[0036] 可选的, 所述私钥服务器部署在 CDN 服务集群中或所述目标业务服务器侧。

[0037] 第二方面, 提供了一种进行 SSL 握手的系统, 所述系统包括 CDN 节点和私钥服务器, 其中:

[0038] 目标 CDN 节点, 用于在与目标终端进行 SSL 握手的过程中, 确定所述目标终端访问的目标业务服务器, 并获取需要私钥处理的待处理信息, 向所述目标业务服务器对应的私钥服务器发送私钥处理请求, 所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息;

[0039] 所述私钥服务器, 用于基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息, 并将处理结果发送给所述目标 CDN 节点, 以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手。

[0040] 可选的, 所述目标 CDN 节点, 具体用于:

[0041] 在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中, 根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器, 并获取所述目标终端发送的客户端密钥交换消息中携带的加密后的所述目标终端生成的预主密钥, 向所述目标业务服务器对应的私钥服务器发

送私钥处理请求，所述私钥处理请求携带有加密后的预主密钥和与所述目标终端协商的目标解密算法的算法标识；

[0042] 所述私钥服务器，具体用于：

[0043] 按照所述目标解密算法，使用所述目标业务服务器的私钥对所述加密后的预主密钥进行解密，并将解密得到的预主密钥发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述解密得到的预主密钥与所述目标终端继续进行 SSL 握手。

[0044] 可选的，所述目标 CDN 节点，具体用于：

[0045] 在与目标终端进行 TLS1.2 协议下的 DH 握手的过程中，根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的 DH 参数，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述 DH 参数和与所述目标终端协商的第一签名算法的算法标识；

[0046] 所述私钥服务器，具体用于：

[0047] 按照所述第一签名算法，使用所述目标业务服务器的私钥对所述 DH 参数进行签名，并将签名后的 DH 参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的 DH 参数与所述目标终端继续进行 SSL 握手。

[0048] 可选的，所述目标 CDN 节点，具体用于：

[0049] 在与目标终端进行 TLS1.3 协议下的 DH 握手的过程中，根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的哈希参数，所述哈希参数基于和所述目标终端交互的握手数据包和所述目标业务服务器的 SSL 证书生成；向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述哈希参数和与所述目标终端协商的第二签名算法的算法标识；

[0050] 所述私钥服务器，具体用于：

[0051] 按照所述第二签名算法，使用所述目标业务服务器的私钥对所述哈希参

数进行签名，并将签名后的哈希参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的哈希参数与所述目标终端继续进行 SSL 握手。

[0052] 可选的，所述私钥处理请求中还携带有所述目标业务服务器的 SSL 证书标识；

5 [0053] 所述私钥服务器，还用于：

[0054] 在本地存储的私钥列表中查找所述目标业务服务器的 SSL 证书标识对应的所述目标业务服务器的私钥。

[0055] 可选的，所述私钥处理请求为 http1.0 或 http2.0 请求。

[0056] 可选的，所述目标 CDN 节点，具体用于：

10 [0057] 确定指向所述目标业务服务器对应私钥服务器的下一跳 CDN 节点，与所述下一跳 CDN 节点建立 SSL 双向认证通道，通过所述 SSL 双向认证通道向所述下一跳 CDN 节点发送私钥处理请求，以使所述下一跳 CDN 节点向所述私钥服务器发送私钥处理请求。

15 [0058] 可选的，所述私钥服务器部署在 CDN 服务集群中或所述目标业务服务器侧。

[0059] 本申请实施例提供的技术方案带来的有益效果是：

[0060] 本申请实施例中，在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息；目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求，私钥处理
20 请求携带有待处理信息和目标私钥处理类型信息；私钥服务器基于目标私钥处理类型信息和目标业务服务器的私钥处理待处理信息，并将处理结果发送给目标 CDN 节点，以使目标 CDN 节点根据处理结果与目标终端继续进行 SSL 握手。
这样，通过架设私钥服务器，业务服务器无需将私钥提供给外界，保证了私钥的安全性，同时，将私钥处理交由私钥服务器完成，节省了 CDN 节点和业务
25 服务器的 CPU 处理资源，保证了 CDN 服务和业务服务的服务质量。

附图说明

[0061] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

- 5 [0062] 图 1 是本申请实施例提供的一种进行 SSL 握手的网络框架示意图；
[0063] 图 2 是本申请实施例提供的一种进行 SSL 握手的方法流程图；
[0064] 图 3 是本申请实施例提供的一种 TLS1.2 协议下的 RSA 握手的方法流程图；
[0065] 图 4 是本申请实施例提供的一种 TLS1.2 RSA 握手信令图；
10 [0066] 图 5 是本申请实施例提供的一种 TLS1.2 协议下的 DH 握手的方法流程图；
[0067] 图 6 是本申请实施例提供的一种 TLS1.2 DH 握手信令图；
[0068] 图 7 是本申请实施例提供的一种 TLS1.3 协议下的 DH 握手的方法流程图；
[0069] 图 8 是本申请实施例提供的一种 TLS1.3 DH 握手信令图；
[0070] 图 9 是本申请实施例提供的一种进行 SSL 握手的网络框架示意图；
15 [0071] 图 10 是本申请实施例提供的一种进行 SSL 握手的网络框架示意图。

具体实施例

[0072] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施例作进一步地详细描述。

- 20 [0073] 本申请实施例提供了一种进行 SSL 握手的方法，该方法可以由 CDN 节点服务器（以下简称为 CDN 节点）和私钥服务器共同实现，其中，CDN 节点可以是 CDN 服务集群中用于接收用户终端的数据请求的任意节点服务器，CDN 节点中可以存储有业务服务器提供的业务数据（如网页数据、资源文件等），同时还可以保存有业务服务器的 SSL 证书及相应的公钥。私钥服务器可以是部署
25 在业务服务器侧的，用于存储业务服务器的私钥，并提供私钥处理功能的服务器，上述场景的网络框架可以如图 1 所示。上述 CDN 节点和私钥服务器中均可

以包括处理器、存储器、收发器，处理器可以用于进行下述流程中的进行 SSL 握手的处理，存储器可以用于存储下述处理过程中需要的数据以及产生的数据，收发器可以用于接收和发送下述处理过程中的相关数据。

[0074] 下面将结合具体实施例，对图 2 所示的处理流程进行详细的说明，内容可以如下：

[0075] 步骤 201，在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息。

[0076] 在实施中，当用户想要通过终端访问某个网站或者获取某个数据资源时，用户可以通过终端发送相应的业务服务器（下面以目标业务服务器为例进行说明）的访问请求。CDN 服务集群可以接收到该访问请求，然后选择一个 CDN 节点（如目标 CDN 节点）为终端提供业务服务，进而，CDN 服务集群可以向终端反馈目标 CDN 节点的 IP（Internet Protocol，网络协议）地址。之后，终端可以基于目标 CDN 节点的 IP 地址，先与目标 CDN 节点建立 TCP（Transmission Control Protocol，传输控制协议）连接，再基于 TCP 连接与目标 CDN 节点进行 SSL 握手。

[0077] 目标 CDN 节点在与目标终端进行 SSL 握手的过程中，可以通过目标终端发送的客户端问候 Client Hello 消息中携带的服务器标识确定目标终端想要访问的目标业务服务器，该服务器标识可以是服务器的域名信息或者 IP 地址。同时，目标 CDN 节点可以获取需要私钥处理的待处理信息。

[0078] 步骤 202，目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求。

[0079] 其中，私钥处理请求携带有待处理信息和目标私钥处理类型信息。

[0080] 在实施中，目标 CDN 节点在获取到需要私钥处理的待处理信息后，可以先确定目标业务服务器对应的私钥服务器的 IP 地址，然后基于 IP 地址以私钥处理请求的形式向私钥服务器发送上述待处理信息，并指示相应的私钥处理类型（即同时携带目标私钥处理类型信息）。

[0081] 可选的，私钥处理请求可以采用 http1.0 或 http2.0 请求。

[0082] 在实施中，目标 CDN 节点在获取到待处理信息后，可以构造为 http1.0 或 http2.0 请求，在该 http1.0 或 http2.0 请求中添加待处理信息和目标私钥处理类型信息，之后则可以向私钥服务器发送 http1.0 或 http2.0 请求。需要说明的是，
5 如果私钥处理请求采用了 http2.0 请求，则可以利用 http2.0 请求的多路复用特性，减少在传输过程中目标 CDN 节点和其它网络设备间的连接数，同时也可以通过 http2.0 请求的头部压缩功能来减少数据传输量。

[0083] 可选的，私钥处理请求可以通过 CDN 网络来传输，使用 CDN 节点的智能路由选择功能来加速私钥处理请求的传输，相应的，步骤 202 的处理可以如
10 下：目标 CDN 节点确定指向目标业务服务器对应私钥服务器的下一跳 CDN 节点；目标 CDN 节点与下一跳 CDN 节点建立 SSL 双向认证通道，通过 SSL 双向认证通道向下一跳 CDN 节点发送私钥处理请求，以使下一跳 CDN 节点向私钥服务器发送私钥处理请求。

[0084] 在实施中，目标 CDN 节点在向私钥服务器发送私钥处理请求时，可以先
15 根据 CDN 服务集群中节点间的网络状况，进行智能路由选择，确定出指向私钥服务器的下一跳 CDN 节点。之后，目标 CDN 节点可以与选择出的下一跳 CDN 节点建立 SSL 双向认证通道，并通过该 SSL 双向认证通道向下一跳 CDN 节点发送私钥处理请求。进而，后续 CDN 节点（包括上述下一跳 CDN 节点）可以参照上述处理，各自通过智能路由选择出的下一跳 CDN 节点发送私钥处理请求，
20 直至私钥处理请求到达私钥服务器。这样，一方面，可以通过 CDN 服务集群加速私钥处理请求的传输，另一方面，通过 SSL 双向认证通道，可以防止私钥服务器提供的服务被不可信的网络设备调用，或者私钥服务器被不可信的网络设备冒充。

[0085] 步骤 203，私钥服务器基于目标私钥处理类型信息和目标业务服务器的私
25 钥处理待处理信息，并将处理结果发送给目标 CDN 节点，以使目标 CDN 节点根据处理结果与目标终端继续进行 SSL 握手。

[0086] 在实施中，私钥服务器可以接收到目标 CDN 节点发送的私钥处理请求，提取其中携带的待处理信息和目标私钥处理类型信息。之后，私钥服务器可以读取本地存储的目标业务服务器的私钥，然后基于目标私钥处理类型信息使用私钥对待处理信息进行处理。进而，私钥服务器可以将处理结果反馈给目标 CDN 节点。这样，目标 CDN 节点可以在接收到上述处理结果后，根据该处理结果继续与目标终端进行 SSL 握手。需要说明的是，基于上述 CDN 服务集群以及 SSL 双向认证通道传输私钥处理请求的处理，本步骤中私钥服务器可以通过智能路由选择出的路径，基于已建立好的 SSL 双向认证通道，将处理结果返回至目标 CDN 节点。

[0087] 可选的，私钥服务器中可以存储有多台业务服务器的私钥，故而，私钥处理请求中还可以携带有目标业务服务器的 SSL 证书标识，相应的，步骤 203 之前还可以有如下处理：私钥服务器在本地存储的私钥列表中查找目标业务服务器的 SSL 证书标识对应的目标业务服务器的私钥。

[0088] 在实施中，私钥服务器可以提供给多台业务服务器进行私钥处理，故而，私钥服务器中可以维护有私钥列表，该私钥列表中记录了多条业务服务器的 SSL 证书标识和业务服务器的私钥的对应关系。这样，私钥服务器在接收到目标 CDN 节点发送的私钥处理请求后，可以获取其中携带的目标业务服务器的 SSL 证书标识。进一步的，私钥服务器可以在本地存储的私钥列表中查找目标业务服务器的 SSL 证书标识对应的目标业务服务器的私钥。

[0089] 下面将结合不同版本的握手流程，对上述步骤 201 至步骤 203 的处理进行具体说明：

[0090] 一、TLS1.2 协议下的 RSA 握手，如图 3 所示：

[0091] 步骤 301，在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中，目标 CDN 节点根据目标终端发送的客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器，并获取目标终端发送的客户端密钥交换 Client Key Exchange 消息中携带的加密后的目标终端生成的预主密钥。

[0092] 步骤 302, 目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求。

[0093] 其中, 私钥处理请求携带有加密后的预主密钥和与目标终端协商的目标解密算法的算法标识。

- 5 [0094] 步骤 303, 私钥服务器按照目标解密算法, 使用目标业务服务器的私钥对加密后的预主密钥进行解密, 并将解密得到的预主密钥发送给目标 CDN 节点, 以使目标 CDN 节点根据解密得到的预主密钥与目标终端继续进行 SSL 握手。

[0095] 在实施中, 图 4 为 TLS1.2 RSA 握手信令图, 详细内容可以如下:

- [0096] 1、目标终端发送客户端问候 Client Hello 消息给目标 CDN 节点, 客户端
10 问候 Client Hello 消息中携带有终端支持的 SSL 协议版本、算法套件列表、SSL 扩展数据 (包含有目标业务服务器的服务器标识) 以及客户端 Client 随机数;
- [0097] 2、目标 CDN 节点收到客户端问候 Client Hello 消息后, 确定根据客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器;
- [0098] 3、目标 CDN 节点向目标终端返回服务器问候 Server Hello 消息, 服务器
15 问候 Server Hello 消息携带有选择的 SSL 协议版本 (此处为 TLS1.2), 选择的算法套件 (包含目标解密算法和会话密钥的生成算法), Server 随机数;
- [0099] 4、目标 CDN 节点向目标终端发送证书 Certificate 消息, 证书 Certificate 消息携带有目标业务服务器的 SSL 证书以及相应的证书链 (用于验证 SSL 证书的身份), SSL 证书里包含有公钥;
- 20 [00100] 5、目标 CDN 节点向目标终端发送服务器问候完成 Server Hello Done 消息, 指示本端处理结束等待对端响应;
- [00101] 6、目标终端生成预主密钥, 使用公钥对预主密钥进行加密;
- [00102] 7、目标终端向目标 CDN 节点发送客户端密钥交换 Client Key Exchange 消息, 客户端密钥交换 Client Key Exchange 消息携带有加密后的预主密钥;
- 25 [00103] 8、目标终端基于选择的会话密钥的生成算法将预主密钥与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥;

[00104] 9、目标终端向目标 CDN 节点发送更换密码规范 Change Cipher Spec 消息，再发送结束 Finished 消息。

[00105] 10、目标 CDN 节点收到客户端密钥交换 Client Key Exchange 消息后，获取客户端密钥交换 Client Key Exchange 消息中携带的加密后的预主密钥；

5 [00106] 11、目标 CDN 节点通过 CDN 网络向目标业务服务器对应的私钥服务器发送私钥处理请求，私钥处理请求携带有加密后的预主密钥和目标解密算法的算法标识；

[00107] 12、私钥服务器按照目标解密算法，使用目标业务服务器的私钥对加密后的预主密钥进行解密；

10 [00108] 13、私钥服务器将解密得到的预主密钥发送给目标 CDN 节点；

[00109] 14、目标 CDN 节点获取预主密钥，基于选择的会话密钥的生成算法将预主密钥与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥；

[00110] 15、目标 CDN 节点向目标终端发送更换密码规范 Change Cipher Spec，表明密钥协商完毕，后面的消息将使用会话密钥进行加密；

15 [00111] 16、目标 CDN 节点向目标终端发送结束 Finished 消息，完成与目标终端的 SSL 握手。

[00112] 需要说明的是，上述处理同样适用于包括 SSL3、TLS1.0 和 TLS1.1 协议下的 RSA 握手流程。

20 [00113] 二、TLS1.2 协议下的 DH 握手，如图 5 所示：

[00114] 步骤 501，在与目标终端进行 TLS1.2 协议下的 DH 握手的过程中，目标 CDN 节点根据目标终端发送的客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器，并获取本地生成的 DH 参数。

[00115] 步骤 502，目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥
25 处理请求。

[00116] 其中，私钥处理请求携带有 DH 参数和与目标终端协商的第一签名算法

的算法标识。

[00117] 步骤 503, 私钥服务器按照第一签名算法, 使用目标业务服务器的私钥对 DH 参数进行签名, 并将签名后的 DH 参数发送给目标 CDN 节点, 以使目标 CDN 节点根据签名后的 DH 参数与目标终端继续进行 SSL 握手。

5 [00118] 在实施中, 图 6 为 TLS1.2 DH 握手信令图, 详细内容可以如下:

[00119] 1、目标终端发送客户端问候 Client Hello 消息给目标 CDN 节点, 客户端问候 Client Hello 消息中携带有终端支持的 SSL 协议版本、算法套件列表、SSL 扩展数据 (包含有目标业务服务器的服务器标识) 以及客户端 Client 随机数;

10 [00120] 2、目标 CDN 节点收到客户端问候 Client Hello 消息后, 确定根据客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器;

[00121] 3、目标 CDN 节点向目标终端返回服务器问候 Server Hello 消息, 服务器问候 Server Hello 消息携带有选择的 SSL 协议版本 (此处为 TLS1.2), 选择的算法套件 (包含第一签名算法和会话密钥的生成算法), Server 随机数;

15 [00122] 4、目标 CDN 节点向目标终端发送证书 Certificate 消息, 证书 Certificate 消息携带有目标业务服务器的 SSL 证书以及相应的证书链 (用于验证 SSL 证书的身份), SSL 证书里包含有公钥;

[00123] 5、目标 CDN 节点生成 DH 参数;

20 [00124] 6、目标 CDN 节点通过 CDN 网络向目标业务服务器对应的私钥服务器发送私钥处理请求, 私钥处理请求携带有 DH 参数和第一签名算法的算法标识;

[00125] 7、私钥服务器按照第一签名算法, 使用目标业务服务器的私钥对 DH 参数进行签名;

[00126] 8、私钥服务器将签名后的 DH 参数发送给目标 CDN 节点;

25 [00127] 9、目标 CDN 节点获取签名后的 DH 参数, 向目标终端发送服务器密钥交换 Server Key Exchange 消息, 服务器密钥交换 Server Key Exchange 消息携带有签名后的 DH 参数;

[00128] 10、目标 CDN 节点向目标终端发送服务器问候完成 Server Hello Done 消息，指示本端处理结束等待对端响应；

[00129] 11、目标终端收到服务器密钥交换 Server Key Exchange 消息后，获取服务器密钥交换 Server Key Exchange 消息携带的签名后的 DH 参数；

5 [00130] 12、目标终端使用公钥对签名后的 DH 参数进行验签，生成客户端 Client DH 参数；

[00131] 13、目标终端向目标 CDN 节点发送客户端密钥交换 Client Key Exchange 消息，客户端密钥交换 Client Key Exchange 消息携带有客户端 Client DH 参数；

10 [00132] 14、目标终端基于选择的会话密钥的生成算法将客户端 Client DH 参数与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥；

[00133] 15、目标终端向目标 CDN 节点发送更换密码规范 Change Cipher Spec 消息，再发送结束 Finished 消息。

[00134] 16、目标 CDN 节点收到客户端密钥交换 Client Key Exchange 消息后，获取客户端密钥交换 Client Key Exchange 消息中携带的客户端 Client DH 参数；

15 [00135] 17、目标 CDN 节点基于选择的会话密钥的生成算法将客户端 Client DH 参数与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥；

[00136] 18、目标 CDN 节点向目标终端发送更换密码规范 Change Cipher Spec，表明密钥协商完毕，后面的消息将使用会话密钥进行加密；

20 [00137] 19、目标 CDN 节点向目标终端发送结束 Finished 消息，完成与目标终端的 SSL 握手。

[00138] 需要说明的是，上述处理同样适用于包括 SSL3、TLS1.0 和 TLS1.1 协议下的 DH 握手流程。

[00139] 三、TLS1.3 协议下的 DH 握手，如图 7 所示：

25 [00140] 步骤 701，在与目标终端进行 TLS1.3 协议下的 DH 握手的过程中，目标 CDN 节点根据目标终端发送的客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器，并获取本地生成的哈希 hash 参数。

[00141] 其中, 哈希 hash 参数基于和目标终端交互的握手数据包和目标业务服务器的 SSL 证书生成。

[00142] 步骤 702, 目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求。

- 5 [00143] 其中, 私钥处理请求携带有哈希 hash 参数和与目标终端协商的第二签名算法的算法标识。

[00144] 步骤 703, 私钥服务器按照第二签名算法, 使用目标业务服务器的私钥对哈希 hash 参数进行签名, 并将签名后的哈希 hash 参数发送给目标 CDN 节点, 以使目标 CDN 节点根据签名后的哈希 hash 参数与目标终端继续进行 SSL 握手。

- 10 [00145] 在实施中, 图 8 为 TLS1.3 DH 握手信令图, 详细内容可以如下:

[00146] 1、目标终端发送客户端问候 Client Hello 消息给目标 CDN 节点, 客户端问候 Client Hello 消息中携带有终端支持的 SSL 协议版本、算法套件列表、SSL 扩展数据 (包含有目标业务服务器的服务器标识)、key_share 扩展数据 (包含有终端支持的 DH 类别和 DH 参数) 以及客户端 Client 随机数;

- 15 [00147] 2、目标 CDN 节点收到客户端问候 Client Hello 消息后, 确定根据客户端问候 Client Hello 消息中携带的服务器标识确定目标终端访问的目标业务服务器;

[00148] 3、目标 CDN 节点向目标终端返回服务器问候 Server Hello 消息, 服务器问候 Server Hello 消息携带有选择的 SSL 协议版本 (此处为 TLS1.3), 选择的
20 算法套件 (包含第二签名算法和会话密钥的生成算法), key_share 扩展数据 (包含有选择的 DH 类别和 DH 参数) 以及服务器 Server 随机数;

[00149] 4、目标 CDN 节点向目标终端发送证书 Certificate 消息, 证书 Certificate 消息携带有目标业务服务器的 SSL 证书以及相应的证书链 (用于验证 SSL 证书的身份), SSL 证书里包含有公钥;

- 25 [00150] 5、目标 CDN 节点基于和目标终端交互的握手数据包和目标业务服务器的 SSL 证书生成哈希 hash 参数;

- [00151] 6、目标 CDN 节点通过 CDN 网络向目标业务服务器对应的私钥服务器发送私钥处理请求，私钥处理请求携带有哈希 hash 参数和第二签名算法的算法标识；
- [00152] 7、私钥服务器按照第二签名算法，使用目标业务服务器的私钥对哈希 hash 参数进行签名；
- [00153] 8、私钥服务器将签名后的哈希 hash 参数发送给目标 CDN 节点；
- [00154] 9、目标 CDN 节点获取签名后的哈希 hash 参数，向目标终端发送 Certificate Verify 消息，证书签名 Certificate Verify 消息携带有签名后的哈希 hash 参数；
- 10 [00155] 10、目标 CDN 节点基于选择的会话密钥的生成算法将选择的 DH 类别和 DH 参数与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥；
- [00156] 11、目标 CDN 节点向目标终端发送 Finished 消息；
- [00157] 12、目标终端收到证书签名 Certificate Verify 消息后，获取证书签名 Certificate Verify 消息携带的签名后的哈希 hash 参数；
- 15 [00158] 13、目标终端使用公钥对签名后的哈希 hash 参数进行验签；
- [00159] 14、目标终端基于选择的会话密钥的生成算法将选择的 DH 类别和 DH 参数与服务器 server 随机数、客户端 client 随机数共同作用生成会话密钥；
- [00160] 15、目标终端向目标 CDN 节点发送结束 Finished 消息，完成与目标终端的 SSL 握手。
- 20 [00161] 本申请实施例中，在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息；目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求，私钥处理请求携带有待处理信息和目标私钥处理类型信息；私钥服务器基于目标私钥处理类型信息和目标业务服务器的私钥处理待处理信息，并将处理结果发送给
- 25 目标 CDN 节点，以使目标 CDN 节点根据处理结果与目标终端继续进行 SSL 握手。这样，通过架设私钥服务器，业务服务器无需将私钥提供给外界，保证

了私钥的安全性，同时，将私钥处理交由私钥服务器完成，节省了 CDN 节点和业务服务器的 CPU 处理资源，保证了 CDN 服务和业务服务的服务质量。

[00162] 在另一实施例下，私钥服务器可以是部署在 CDN 服务集群中的，用于存储业务服务器的私钥，并提供私钥处理功能的服务器，具体的网络框架可以如图 9 所示。由于 SSL 握手中的私钥处理需要消耗较大的 CPU 处理资源，尤其在 SSL 握手的并发量较大的情况下，CDN 节点提供的 CDN 服务可能会受到较大影响，CDN 服务集群中可以搭建有私钥处理集群，该私钥处理集群包含有大量私钥服务器，私钥服务器中可以存储有多个业务服务器的私钥。这样，在与目标终端进行 SSL 握手的过程中，目标 CDN 节点可以先确定目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，然后可以在私钥处理集群中确定存储有目标业务服务器的私钥的目标私钥服务器，再向目标私钥服务器发送私钥处理请求，私钥处理请求可以携带有待处理信息和目标私钥处理类型信息，进而目标私钥服务器可以基于目标私钥处理类型信息和目标业务服务器的私钥处理待处理信息，并将处理结果发送给目标 CDN 节点，以使目标 CDN 节点根据处理结果与目标终端继续进行 SSL 握手。

[00163] 在又一实施例下，除了设置私钥服务器之外，CDN 节点中可以同样存储有业务服务器的私钥，具体的网络框架可以如图 10 所示。在与终端进行 SSL 握手的过程中，CDN 节点通过 CDN 网络向私钥服务器发送私钥处理请求后，如果在预设时间内未接收到私钥服务器反馈的处理结果，CDN 节点则可以使用本地存储的私钥进行私钥处理。进一步的，如果连续多次向私钥服务器发送私钥处理请求后均未得到回应，CDN 节点则可以在后续预设时长内的 SSL 握手过程中，直接使用本地存储的私钥进行私钥处理。另外，在向私钥服务器发送私钥处理请求之前，CDN 节点还可以检测本地的当前负载，如果当前负载大于预设阈值，则向私钥服务器发送私钥处理请求，如果当前负载小于预设阈值，则可以使用本地存储的私钥进行私钥处理。

[00164] 上述私钥服务器中均可以采用 SSL 加速卡来执行相关私钥处理，SSL 加

速卡提供接口，私钥服务器调用该接口时，可以将私钥和待处理信息作为接口参数传递给 SSL 加速卡。

[00165] 基于相同的技术构思，本申请实施例还提供了一种进行 SSL 握手的系统，所述系统包括 CDN 节点和私钥服务器，其中：

- 5 [00166] 目标 CDN 节点，用于在与目标终端进行 SSL 握手的过程中，确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息；

[00167] 所述私钥服务器，用于基于所述目标私钥处理类型信息和所述目标业务
10 服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手。

[00168] 可选的，所述目标 CDN 节点，具体用于：

[00169] 在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中，根据所述目标
15 终端发送的 Client Hello 消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取所述目标终端发送的 Client Key Exchange 消息中携带的加密后的所述目标终端生成的预主密钥，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有加密后的预主密钥和与所述目标终端协商的目标解密算法的算法标识；

[00170] 所述私钥服务器，具体用于：

20 [00171] 按照所述目标解密算法，使用所述目标业务服务器的私钥对所述加密后的预主密钥进行解密，并将解密得到的预主密钥发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述解密得到的预主密钥与所述目标终端继续进行 SSL 握手。

[00172] 可选的，所述目标 CDN 节点，具体用于：

25 [00173] 在与目标终端进行 TLS1.2 协议下的 DH 握手的过程中，根据所述目标终端发送的 Client Hello 消息中携带的服务器标识确定所述目标终端访问的目标业

务服务器，并获取本地生成的 DH 参数，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述 DH 参数和与所述目标终端协商的第一签名算法的算法标识；

[00174] 所述私钥服务器，具体用于：

- 5 [00175] 按照所述第一签名算法，使用所述目标业务服务器的私钥对所述 DH 参数进行签名，并将签名后的 DH 参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的 DH 参数与所述目标终端继续进行 SSL 握手。

[00176] 可选的，所述目标 CDN 节点，具体用于：

- 10 [00177] 在与目标终端进行 TLS1.3 协议下的 DH 握手的过程中，根据所述目标终端发送的 Client Hello 消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的哈希 hash 参数，所述哈希 hash 参数基于和所述目标终端交互的握手数据包和所述目标业务服务器的 SSL 证书生成；向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述哈希 hash 参数和与所述目标终端协商的第二签名算法的算法标识；

- 15 [00178] 所述私钥服务器，具体用于：

[00179] 按照所述第二签名算法，使用所述目标业务服务器的私钥对所述哈希 hash 参数进行签名，并将签名后的哈希 hash 参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的哈希 hash 参数与所述目标终端继续进行 SSL 握手。

- 20 [00180] 可选的，所述私钥处理请求中还携带有所述目标业务服务器的 SSL 证书标识；

[00181] 所述私钥服务器，还用于：

[00182] 在本地存储的私钥列表中查找所述目标业务服务器的 SSL 证书标识对应的所述目标业务服务器的私钥。

- 25 [00183] 可选的，所述私钥处理请求为 http1.0 或 http2.0 请求。

[00184] 可选的，所述目标 CDN 节点，具体用于：

[00185] 确定指向所述目标业务服务器对应私钥服务器的下一跳 CDN 节点，与所述下一跳 CDN 节点建立 SSL 双向认证通道，通过所述 SSL 双向认证通道向所述下一跳 CDN 节点发送私钥处理请求，以使所述下一跳 CDN 节点向所述私钥服务器发送私钥处理请求。

- 5 [00186] 可选的，所述私钥服务器部署在 CDN 服务集群中或所述目标业务服务器侧。

[00187] 本申请实施例中，在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息；目标 CDN 节点向目标业务服务器对应的私钥服务器发送私钥处理请求，私钥处理请求携带有待处理信息和目标私钥处理类型信息；私钥服务器基于目标私钥处理类型信息和目标业务服务器的私钥处理待处理信息，并将处理结果发送给目标 CDN 节点，以使目标 CDN 节点根据处理结果与目标终端继续进行 SSL 握手。这样，通过架设私钥服务器，业务服务器无需将私钥提供给外界，保证了私钥的安全性，同时，将私钥处理交由私钥服务器完成，节省了 CDN 节点和业务服务器的 CPU 处理资源，保证了 CDN 服务和业务服务的服务质量。

10
15

[00188] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

- 20 [00189] 以上所述仅为本申请的较佳实施例，并不用以限制本申请，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。

权 利 要 求 书

1、一种进行 SSL 握手的方法，其特征在于，所述方法包括：

在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息；

5 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息；

所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手。

10

2、根据权利要求 1 所述的方法，其特征在于，所述在与目标终端进行 SSL 握手的过程中，目标 CDN 节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，包括：

在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中，目标 CDN 节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取所述目标终端发送的客户端密钥交换消息中携带的加密后的所述目标终端生成的预主密钥；

15 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型，包括：

20 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有加密后的预主密钥和与所述目标终端协商的目标解密算法的算法标识；

所述私钥服务器基于所述目标私钥处理类型和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手，包括：

25 所述私钥服务器按照所述目标解密算法，使用所述目标业务服务器的私钥对所述加密后的预主密钥进行解密，并将解密得到的预主密钥发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述解密得到的预主密钥与所述目标终端继续进行 SSL 握手。

3、根据权利要求1所述的方法，其特征在于，所述在与目标终端进行SSL握手的过程中，目标CDN节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，包括：

5 在与目标终端进行TLS1.2协议下的DH握手的过程中，目标CDN节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的DH参数；

 所述目标CDN节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息，包
10 括：

 所述目标CDN节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述DH参数和与所述目标终端协商的第一签名算法的算法标识；

 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的
15 私钥处理所述待处理信息，并将处理结果发送给所述目标CDN节点，以使所述目标CDN节点根据所述处理结果与所述目标终端继续进行SSL握手，包括：

 所述私钥服务器按照所述第一签名算法，使用所述目标业务服务器的私钥对所述DH参数进行签名，并将签名后的DH参数发送给所述目标CDN节点，以使所述目标CDN节点根据所述签名后的DH参数与所述目标终端继续进行
20 SSL握手。

4、根据权利要求1所述的方法，其特征在于，所述在与目标终端进行SSL握手的过程中，目标CDN节点确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，包括：

25 在与目标终端进行TLS1.3协议下的DH握手的过程中，目标CDN节点根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的哈希参数，所述哈希参数基于和所述目标终端交互的握手数据包和所述目标业务服务器的SSL证书生成；

 所述目标CDN节点向所述目标业务服务器对应的私钥服务器发送私钥处理
30 请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息，包

括:

所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求, 所述私钥处理请求携带有所述哈希参数和与所述目标终端协商的第二签名算法的算法标识;

- 5 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息, 并将处理结果发送给所述目标 CDN 节点, 以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手, 包括:

所述私钥服务器按照所述第二签名算法, 使用所述目标业务服务器的私钥对所述哈希参数进行签名, 并将签名后的哈希参数发送给所述目标 CDN 节点,
10 以使所述目标 CDN 节点根据所述签名后的哈希参数与所述目标终端继续进行 SSL 握手。

5、根据权利要求 1 所述的方法, 其特征在于, 所述私钥处理请求中还携带有所述目标业务服务器的 SSL 证书标识;

- 15 所述私钥服务器基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息之前, 还包括:

所述私钥服务器在本地存储的私钥列表中查找所述目标业务服务器的 SSL 证书标识对应的所述目标业务服务器的私钥。

- 20 6、根据权利要求 1 所述的方法, 其特征在于, 所述私钥处理请求为 http1.0 或 http2.0 请求。

7、根据权利要求 1 所述的方法, 其特征在于, 所述目标 CDN 节点向所述目标业务服务器对应的私钥服务器发送私钥处理请求, 包括:

- 25 所述目标 CDN 节点确定指向所述目标业务服务器对应私钥服务器的下一跳 CDN 节点;

所述目标 CDN 节点与所述下一跳 CDN 节点建立 SSL 双向认证通道, 通过所述 SSL 双向认证通道向所述下一跳 CDN 节点发送私钥处理请求, 以使所述下一跳 CDN 节点向所述私钥服务器发送私钥处理请求。

30

8、根据权利要求 1-7 中任一项所述的方法，其特征在于，所述私钥服务器部署在 CDN 服务集群中或所述目标业务服务器侧。

5 9、一种进行 SSL 握手的系统，其特征在于，所述系统包括 CDN 节点和私钥服务器，其中：

目标 CDN 节点，用于在与目标终端进行 SSL 握手的过程中，确定所述目标终端访问的目标业务服务器，并获取需要私钥处理的待处理信息，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述待处理信息和目标私钥处理类型信息；

10 所述私钥服务器，用于基于所述目标私钥处理类型信息和所述目标业务服务器的私钥处理所述待处理信息，并将处理结果发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述处理结果与所述目标终端继续进行 SSL 握手。

15 10、根据权利要求 9 所述的系统，其特征在于，所述目标 CDN 节点，具体用于：

在与目标终端进行 TLS1.2 协议下的 RSA 握手的过程中，根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取所述目标终端发送的客户端密钥交换消息中携带的加密后的所述目标终端生成的预主密钥，向所述目标业务服务器对应的私钥服务器发送
20 私钥处理请求，所述私钥处理请求携带有加密后的预主密钥和与所述目标终端协商的目标解密算法的算法标识；

所述私钥服务器，具体用于：

按照所述目标解密算法，使用所述目标业务服务器的私钥对所述加密后的预主密钥进行解密，并将解密得到的预主密钥发送给所述目标 CDN 节点，以使
25 所述目标 CDN 节点根据所述解密得到的预主密钥与所述目标终端继续进行 SSL 握手。

11、根据权利要求 9 所述的系统，其特征在于，所述目标 CDN 节点，具体用于：

30 在与目标终端进行 TLS1.2 协议下的 DH 握手的过程中，根据所述目标终端

发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的 DH 参数，向所述目标业务服务器对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述 DH 参数和与所述目标终端协商的第一签名算法的算法标识；

5 所述私钥服务器，具体用于：

按照所述第一签名算法，使用所述目标业务服务器的私钥对所述 DH 参数进行签名，并将签名后的 DH 参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的 DH 参数与所述目标终端继续进行 SSL 握手。

10 12、根据权利要求 9 所述的系统，其特征在于，所述目标 CDN 节点，具体用于：

在与目标终端进行 TLS1.3 协议下的 DH 握手的过程中，根据所述目标终端发送的客户端问候消息中携带的服务器标识确定所述目标终端访问的目标业务服务器，并获取本地生成的哈希参数，所述哈希参数基于和所述目标终端交互的握手数据包和所述目标业务服务器的 SSL 证书生成；向所述目标业务服务器
15 对应的私钥服务器发送私钥处理请求，所述私钥处理请求携带有所述哈希参数和与所述目标终端协商的第二签名算法的算法标识；

所述私钥服务器，具体用于：

按照所述第二签名算法，使用所述目标业务服务器的私钥对所述哈希参数
20 进行签名，并将签名后的哈希参数发送给所述目标 CDN 节点，以使所述目标 CDN 节点根据所述签名后的哈希参数与所述目标终端继续进行 SSL 握手。

13、根据权利要求 9 所述的系统，其特征在于，所述私钥处理请求中还携带有所述目标业务服务器的 SSL 证书标识；

25 所述私钥服务器，还用于：

在本地存储的私钥列表中查找所述目标业务服务器的 SSL 证书标识对应的所述目标业务服务器的私钥。

14、根据权利要求 9 所述的系统，其特征在于，所述私钥处理请求为 http1.0
30 或 http2.0 请求。

15、根据权利要求 9 所述的系统，其特征在于，所述目标 CDN 节点，具体用于：

5 确定指向所述目标业务服务器对应私钥服务器的下一跳 CDN 节点，与所述下一跳 CDN 节点建立 SSL 双向认证通道，通过所述 SSL 双向认证通道向所述下一跳 CDN 节点发送私钥处理请求，以使所述下一跳 CDN 节点向所述私钥服务器发送私钥处理请求。

16、根据权利要求 9-15 中任一项所述的系统，其特征在于，所述私钥服务
10 器部署在 CDN 服务集群中或所述目标业务服务器侧。

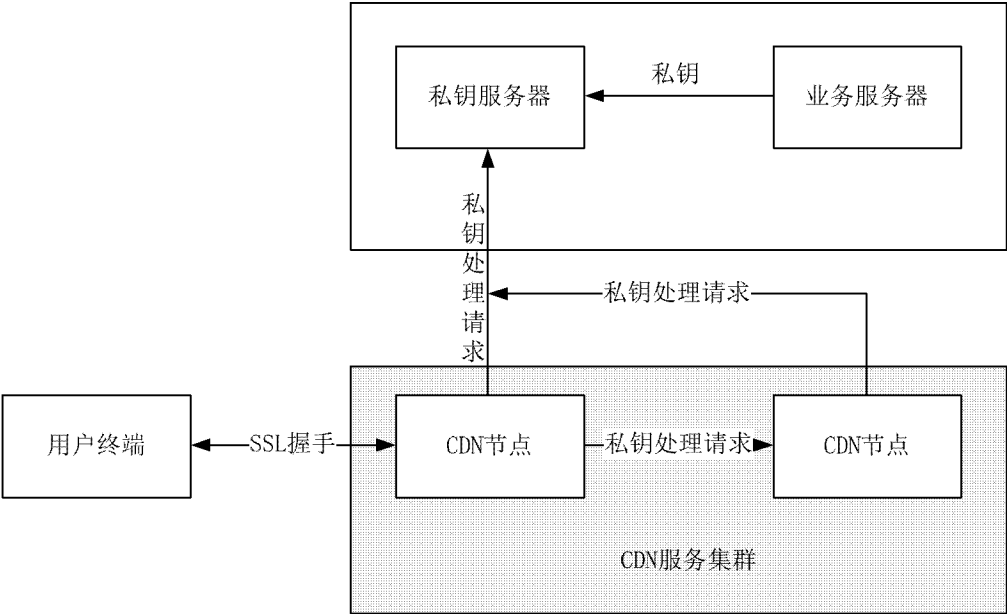


图 1

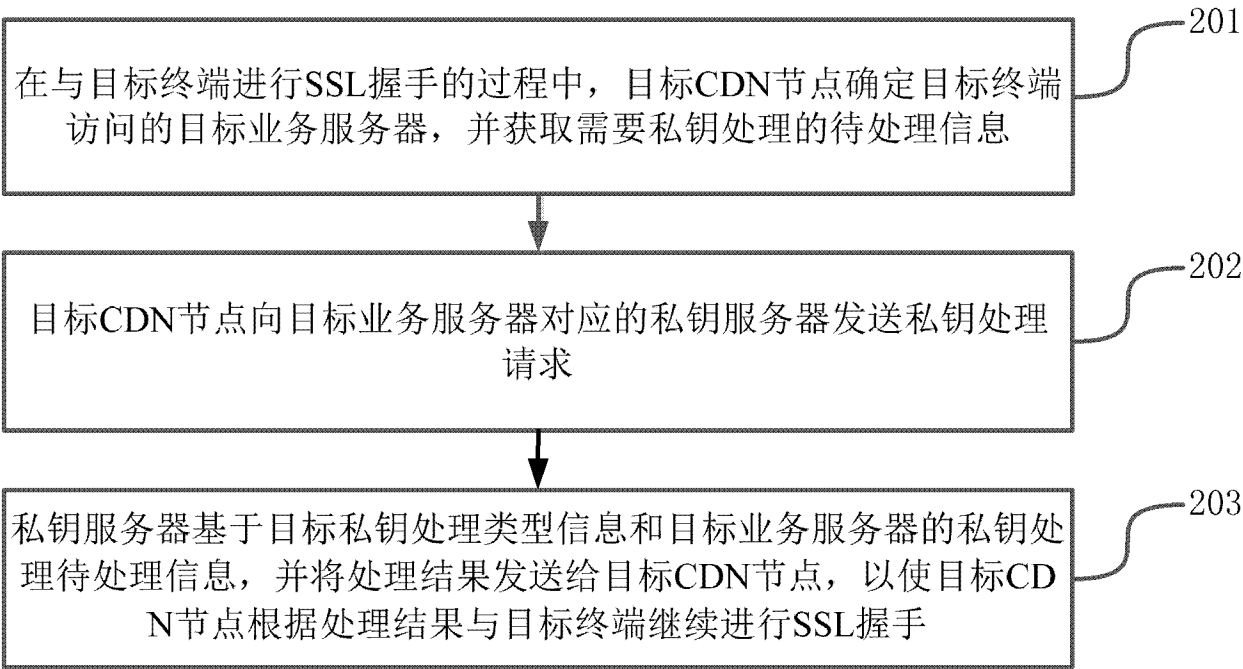


图 2

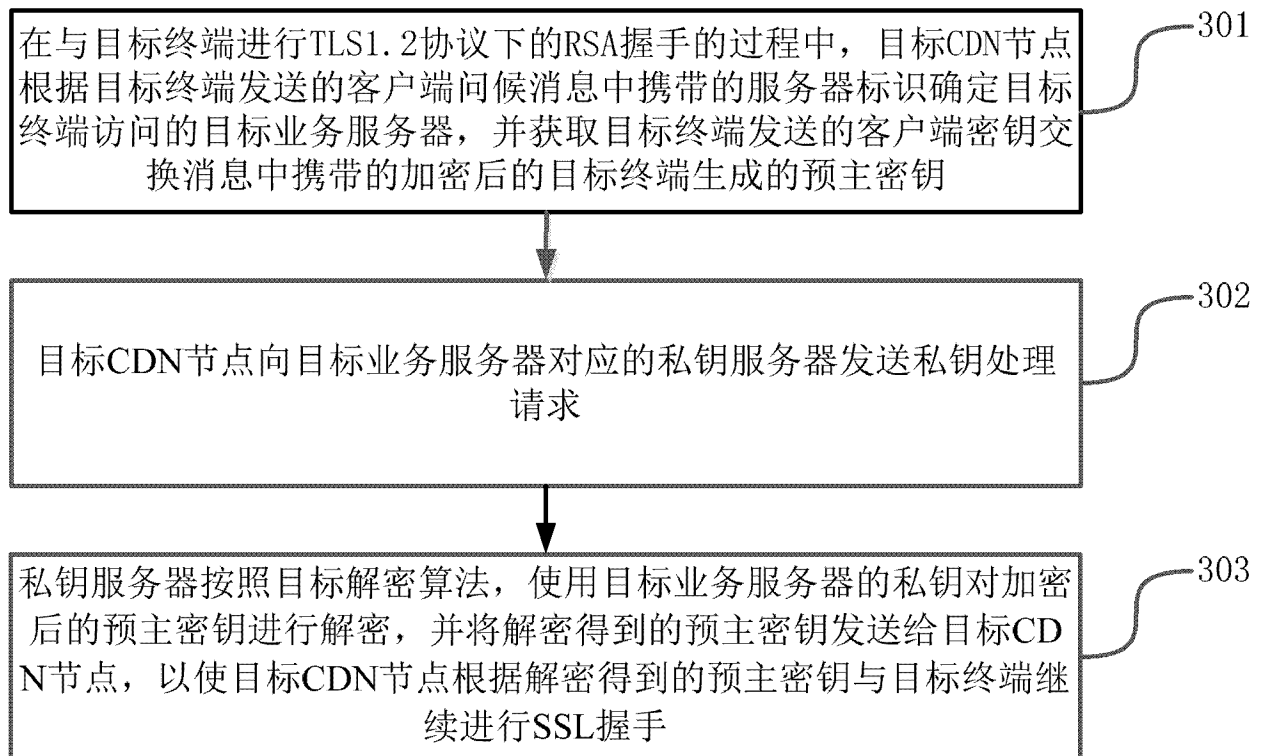


图 3

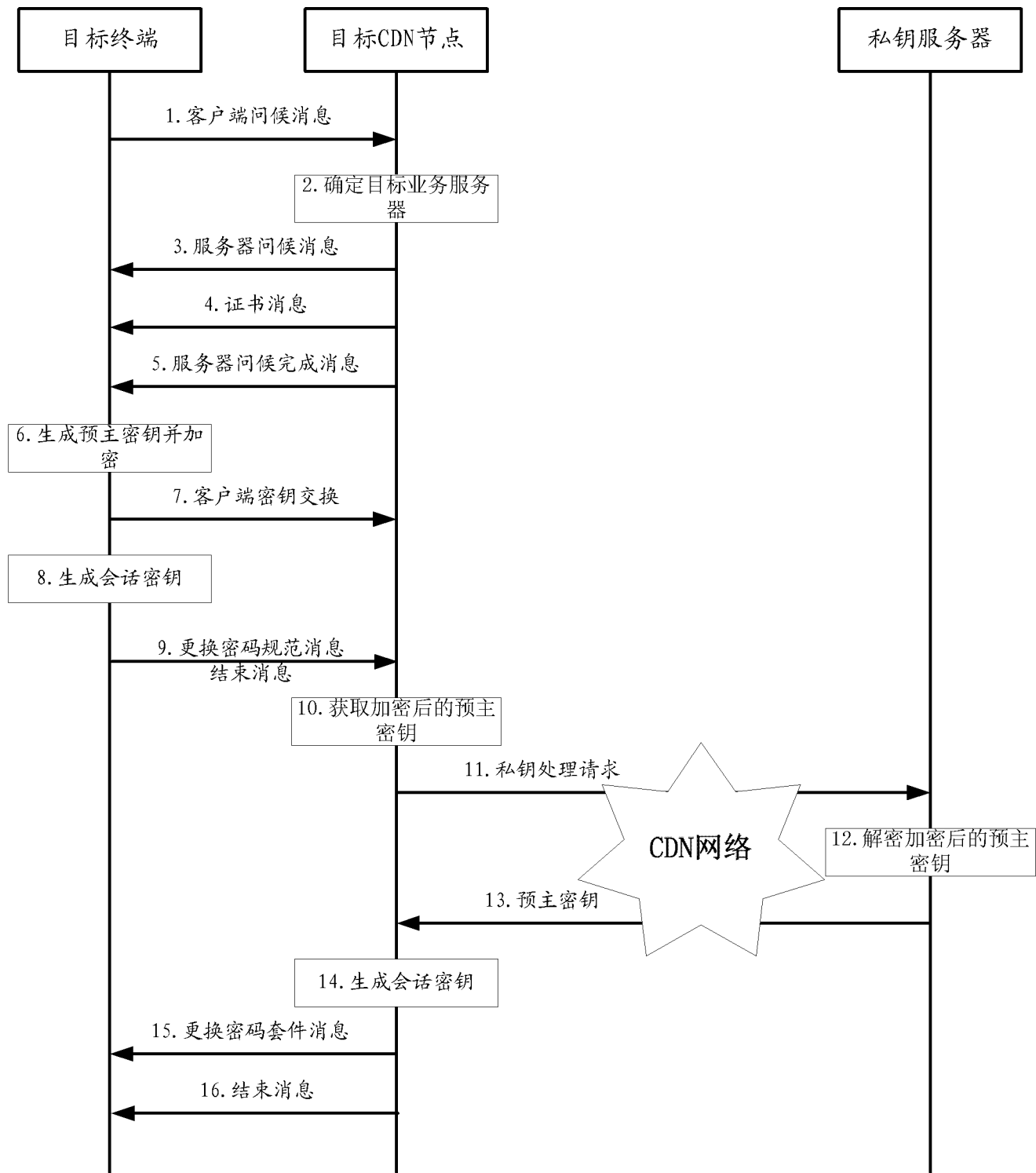


图 4

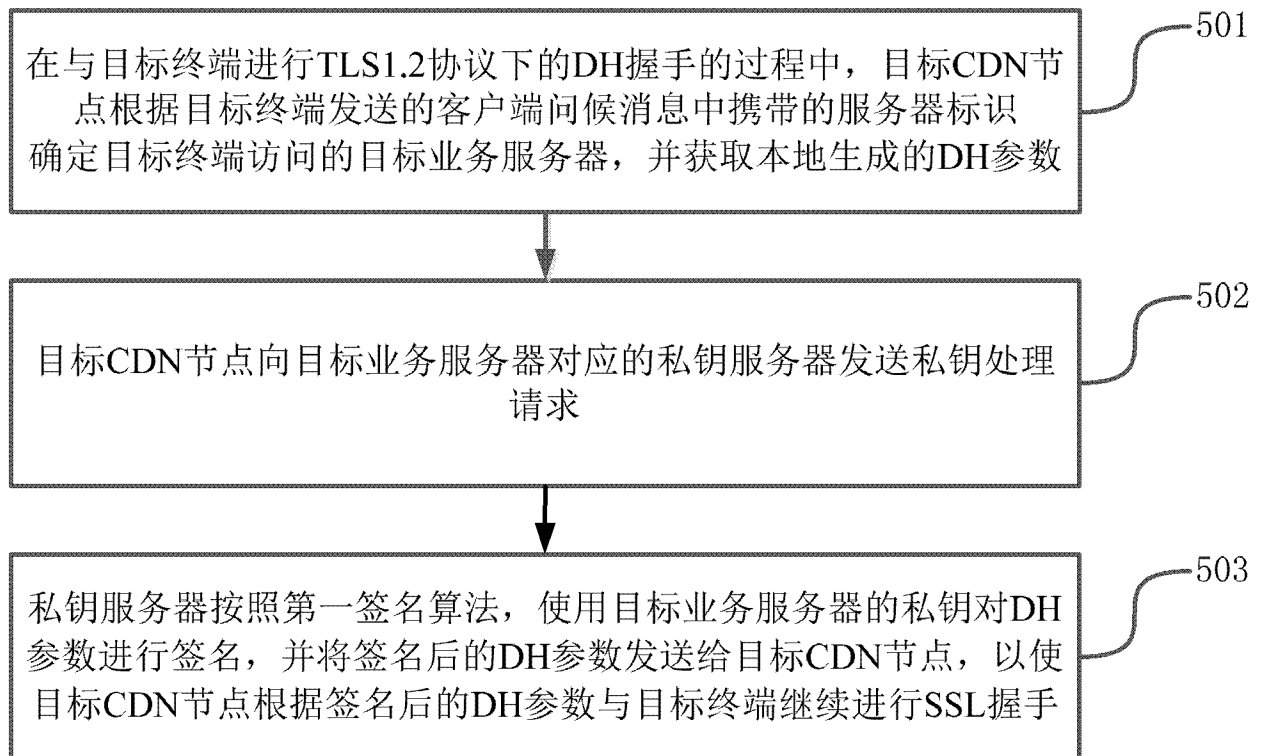


图 5

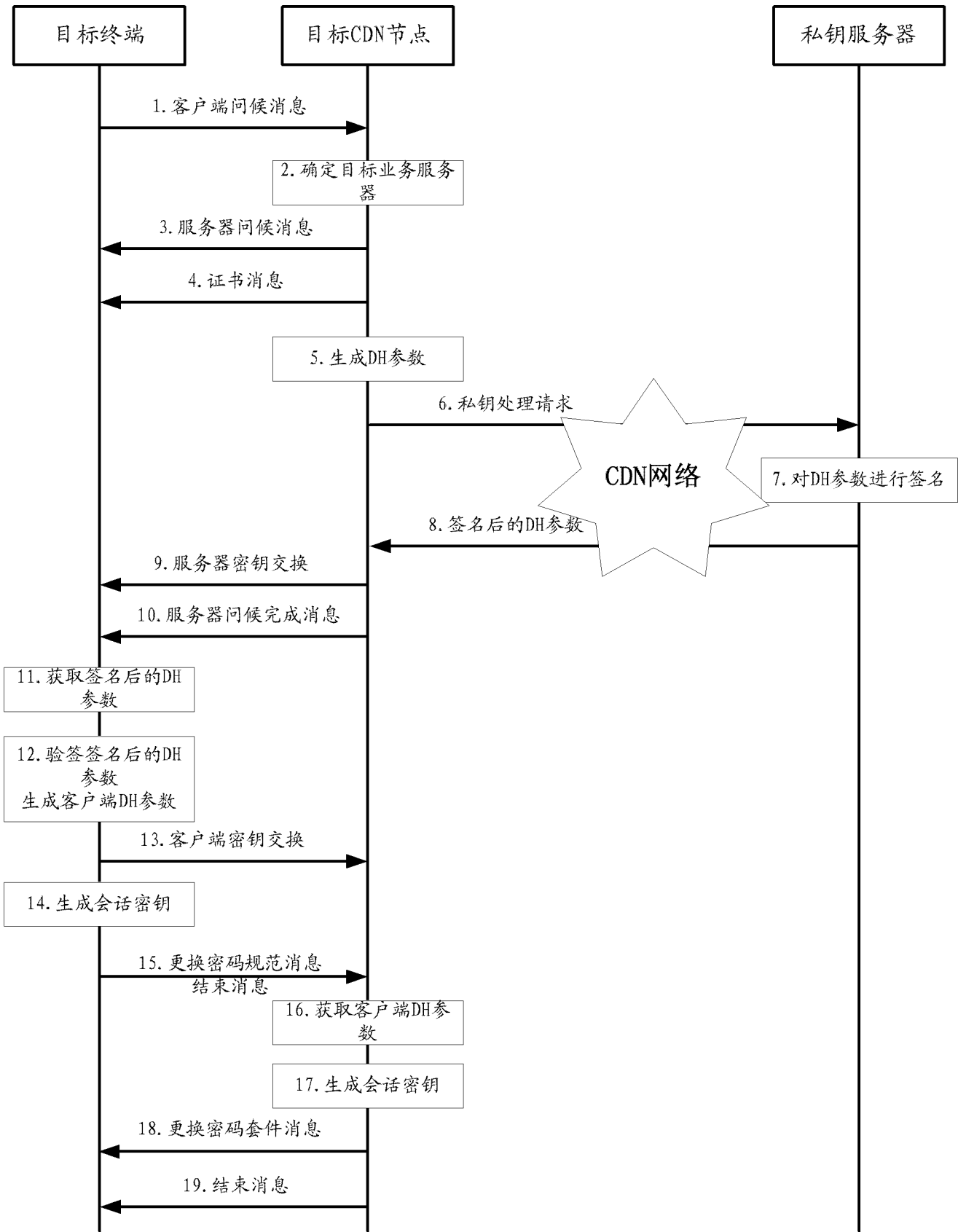


图 6

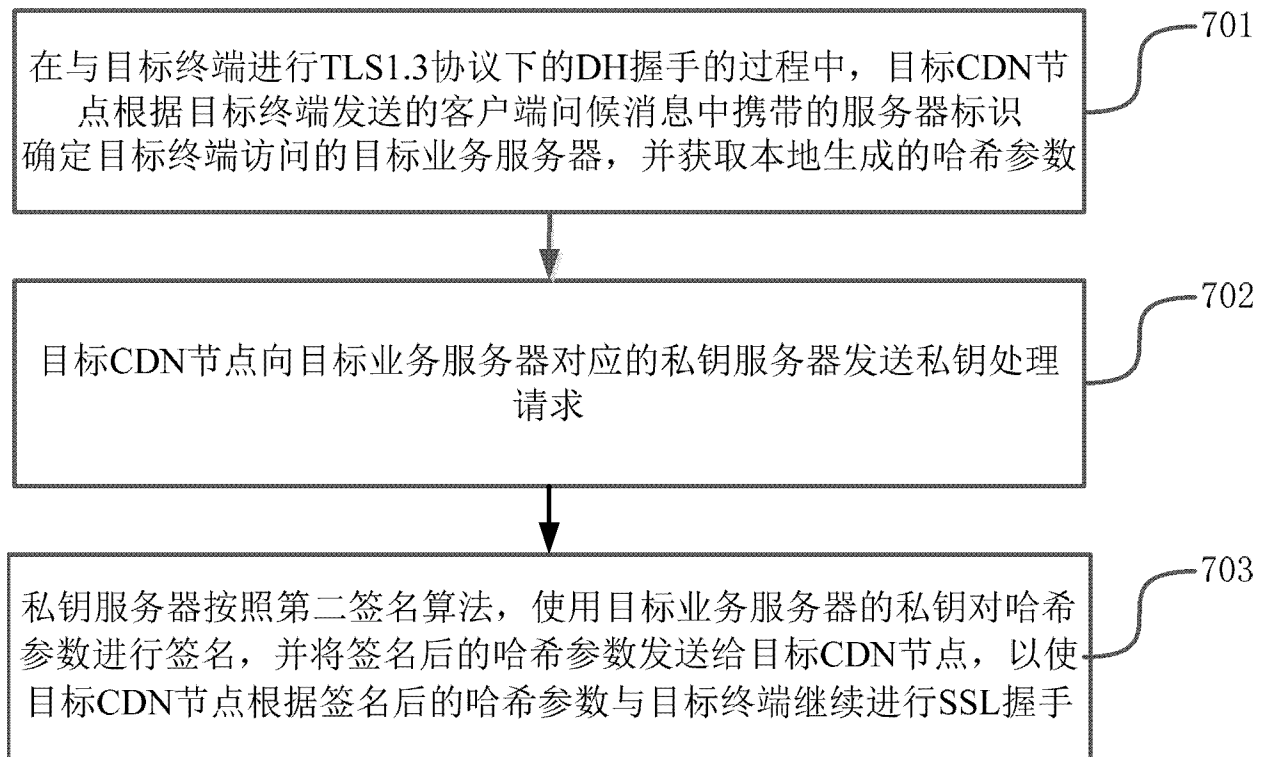


图 7

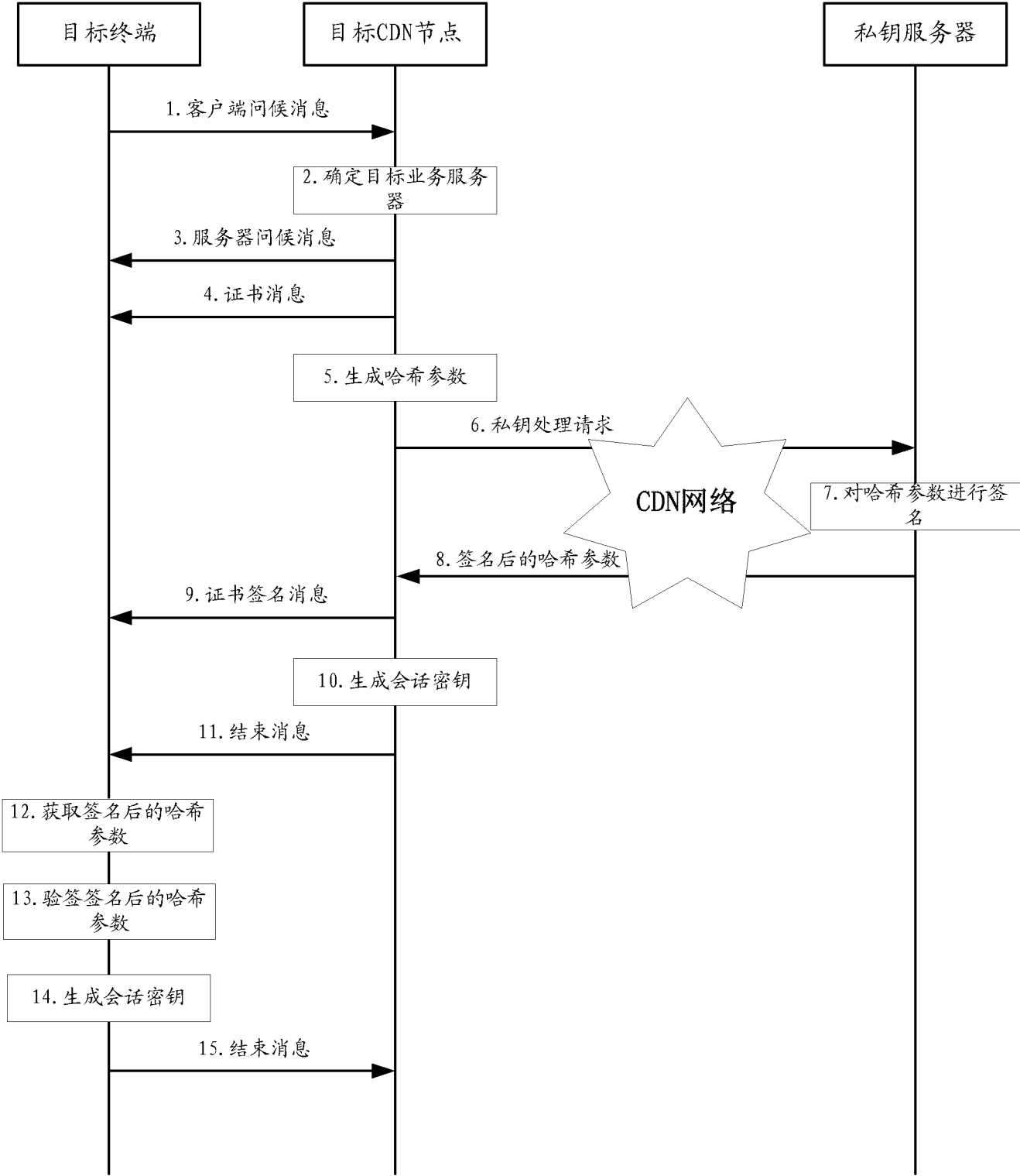


图 8

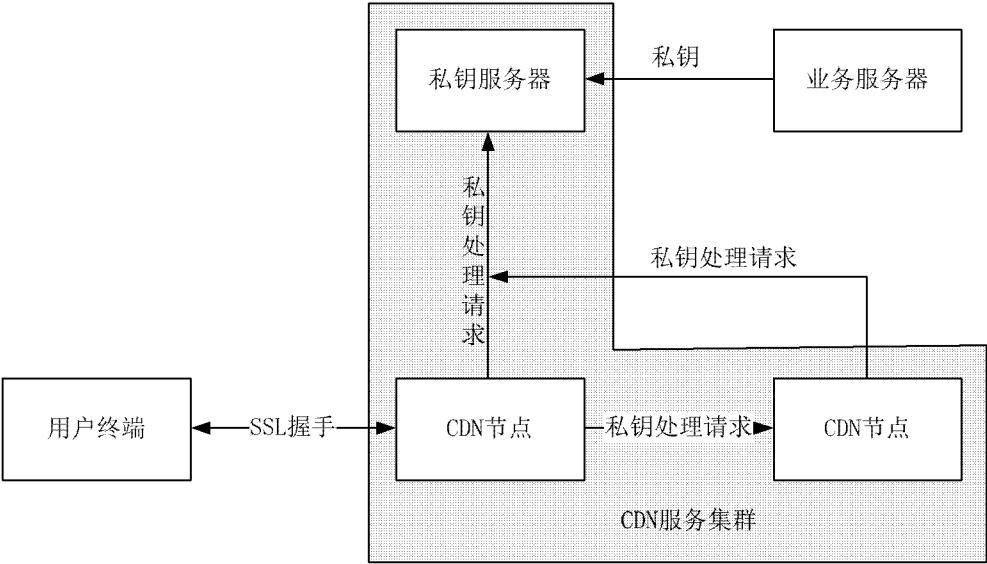


图 9

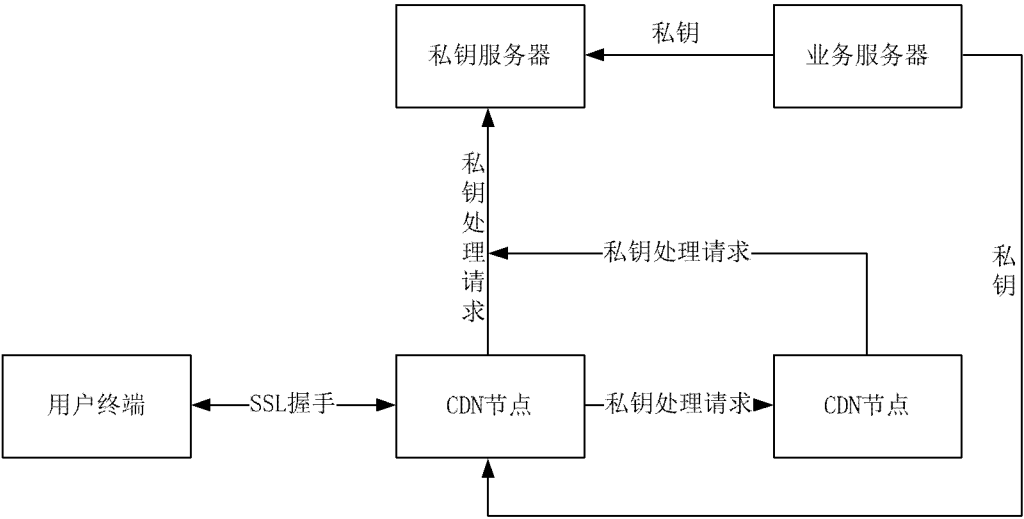


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/088676

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: SSL, 握手, 秘钥, CDN, 服务器, handshake, server, key, encrypt+, decrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106790090 A (BEIJING QIHOO TECHNOLOGY CO., LTD. ET AL.) 31 May 2017 (2017-05-31) description, paragraphs [0035]-[0063], and figures 1-3	1-16
A	CN 102801616 A (HUAWEI TECHNOLOGIES CO., LTD.) 28 November 2012 (2012-11-28) entire document	1-16
A	CN 105871797 A (LETV CLOUD COMPUTING CO., LTD.) 17 August 2016 (2016-08-17) entire document	1-16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

26 November 2018

Date of mailing of the international search report

29 December 2018

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/088676

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106790090	A	31 May 2017	None			
CN	102801616	A	28 November 2012	WO	2014019386	A1	06 February 2014
				US	2015156025	A1	04 June 2015
CN	105871797	A	17 August 2016	None			

国际检索报告

国际申请号

PCT/CN2018/088676

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNKI, CNPAT, WPI, EPODOC:SSL, 握手, 秘钥, CDN, 服务器, handshake, server, key, encrypt+, decrypt+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 106790090 A (北京奇虎科技有限公司等) 2017年 5月 31日 (2017 - 05 - 31) 说明书第[0035]-[0063]段、图1-3	1-16
A	CN 102801616 A (华为技术有限公司) 2012年 11月 28日 (2012 - 11 - 28) 全文	1-16
A	CN 105871797 A (乐视云计算有限公司) 2016年 8月 17日 (2016 - 08 - 17) 全文	1-16

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2018年 11月 26日

国际检索报告邮寄日期

2018年 12月 29日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

黄菲

电话号码 86-(10)-53961743

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/088676

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106790090	A	2017年 5月 31日	无			
CN	102801616	A	2012年 11月 28日	WO	2014019386	A1	2014年 2月 6日
				US	2015156025	A1	2015年 6月 4日
CN	105871797	A	2016年 8月 17日	无			

表 PCT/ISA/210 (同族专利附件) (2015年1月)