(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
2022 年 12 月 29 日 (29.12.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/267977 A1

(51) 国际专利分类号:
*H04L 61/45* (2022.01) *H04L 9/40* (2022.01)

(21) 国际申请号: PCT/CN2022/099220

(22) 国际申请日: 2022 年 6 月 16 日 (16.06.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110712488.0 2021年6月25日 (25.06.2021) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 尹芹 (YIN, Qin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 陶国军 (TAO, Guojun); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 缪川扬 (MIAO, Chuanyang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 童浩 (TONG, Hao); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 广州嘉权专利商标事务所有限公司 (JIAQUAN IP LAW); 中国广东省广州市天河区黄埔大道西 100 号富力盈泰广场 A 栋 910, Guangdong 510627 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA,

(54) **Title:** INFORMATION PROCESSING METHOD, INTERMEDIATE PARSER, NETWORK DEVICE AND STORAGE MEDIUM

(54) **发明名称**: 信息处理方法、中间解析器、网络设备及存储介质

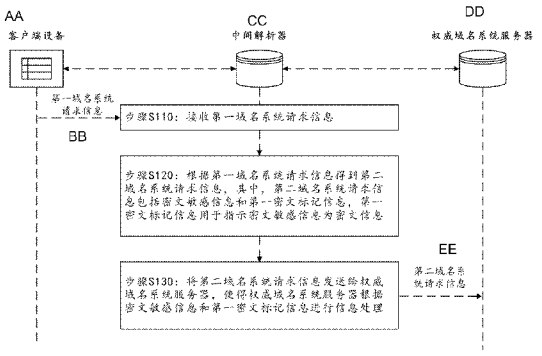


图 2

AA Client device
BB First domain name system request information
CC Intermediate parser
DD Authoritative domain name system server
EE Second domain name system request information
FF Step S110: receive the first domain name system request information
GG Step S120: obtain second domain name system request information according to the first domain name system request information, wherein the second domain name system request information comprises ciphertext sensitive information and first ciphertext marking information, and the first ciphertext marking information is used for indicating that the ciphertext sensitive information is ciphertext information
HH Step S130: send the second domain name system request information to the authoritative domain name system server, such that the authoritative domain name system server performs information processing according to the ciphertext sensitive information and the first ciphertext marking information

(57) **Abstract:** Disclosed in the present application are an information processing method, an intermediate parser, a network device and a storage medium. The information processing method comprises: receiving first domain name system request information; obtaining second domain name system request information according to the first domain name system request information, wherein the second domain name system request information comprises ciphertext sensitive information and first ciphertext marking information, and the first ciphertext marking information is used for indicating that the ciphertext sensitive information is ciphertext information; and sending the second domain name system request information to an authoritative domain name system server, such that the authoritative domain name system server performs information processing according to the ciphertext sensitive information and the first ciphertext marking information.

(57) **摘要**: 本申请公开了信息处理方法、中间解析器、网络设备及存储介质。其中，信息处理方法包括：接收第一域名系统请求信息；根据第一域名系统请求信息得到第二域名系统请求信息，其中，第二域名系统请求信息包括密文敏感信息和第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息；将第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据密文敏感信息和第一密文标记信息进行信息处理。

WO 2022/267977 A1

[见续页]

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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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)。

**根据细则4.17的声明：**

— 发明人资格(细则4.17(iv))

**本国际公布：**

— 包括国际检索报告(条约第21条(3))。

# 信息处理方法、中间解析器、网络设备及存储介质

## 相关申请的交叉引用

本申请基于申请号为202110712488.0、申请日为2021年6月25日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

## 技术领域

本申请涉及信息处理技术领域，尤其是一种信息处理方法、中间解析器、网络设备及存储介质。

## 背景技术

域名系统（Domain Name System，DNS）是在互联网上应用极其广泛的一套域名和地址映射的解析系统。用户通过对域名服务器进行域名查询能够获得目标服务器的真实网际互连协议（Internet Protocol，IP）地址，从而能够帮助用户建立和目标服务器的链接。

在相关技术中，当用户设备发起获取域名字段的IP地址的DNS请求信息时，会先将该DNS请求信息发送给中间解析器。为了提供更加精确的归属地判断，中间解析器可以在DNS请求信息中，将能够标识用户设备或者近端服务节点的位置或身份等敏感信息作为附加信息，但是，这会使得在网络中传输的DNS请求信息把这些敏感信息暴露在安全风险之下。现有的DNS安全保护为了应对该安全风险，需要对整个DNS请求信息中的每一个字段都进行加密处理，其目的是防止中间攻击者的伪造反馈消息，保持数据的完整性，但这对于敏感数据泄露则没有很好的保护作用。并且，现有的安全技术要求所有设备均具有支持对DNS请求信息的加密处理和解密处理的信任机制，从而导致了网络资源开销的增加，提高了设备的维护成本。

## 发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本申请实施例提供了一种信息处理方法、中间解析器、网络设备及存储介质，能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本。

第一方面，本申请实施例提供了一种信息处理方法，应用于中间解析器，所述方法包括：

接收第一域名系统请求信息；

根据所述第一域名系统请求信息得到第二域名系统请求信息，其中，所述第二域名系统请求信息包括密文敏感信息和第一密文标记信息，所述第一密文标记信息用于指示所述密文敏感信息为密文信息；

将所述第二域名系统请求信息发送给权威域名系统服务器，使得所述权威域名系统服务器根据所述密文敏感信息和所述第一密文标记信息进行信息处理。

第二方面，本申请实施例还提供了一种中间解析器，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如上所述

的信息处理方法。

第三方面，本申请实施例还提供了一种网络设备，包括有如上所述的中间解析器。

第四方面，本申请实施例还提供了一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于执行如上所述的信息处理方法。

本申请实施例包括：接收第一域名系统请求信息；根据所述第一域名系统请求信息得到第二域名系统请求信息，其中，所述第二域名系统请求信息包括密文敏感信息和第一密文标记信息，所述第一密文标记信息用于指示所述密文敏感信息为密文信息；将所述第二域名系统请求信息发送给权威域名系统服务器，使得所述权威域名系统服务器根据所述密文敏感信息和所述第一密文标记信息进行信息处理。

本申请实施例包括：接收第一域名系统请求信息；根据第一域名系统请求信息得到第二域名系统请求信息，其中，第二域名系统请求信息包括密文敏感信息和第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息；将第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据密文敏感信息和第一密文标记信息进行信息处理。根据本申请实施例的方案，通过将第一域名系统请求信息转换成包括有密文敏感信息和第一密文标记信息的第二域名系统请求信息，无需对整个第一域名系统请求信息进行加密处理，因此能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本。

本申请的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

## 附图说明

附图用来提供对本申请技术方案的进一步理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本申请的技术方案，并不构成对本申请技术方案的限制。

图 1 是本申请一个实施例提供的用于执行信息处理方法的系统架构的示意图；

图 2 是本申请一个实施例提供的信息处理方法的流程图；

图 3 是本申请一个实施例提供的一种消息体子结构的示意图；

图 4 是本申请一个实施例提供的另一种消息体子结构的示意图；

图 5 是图 4 中的 RDATA 元素的消息体子结构经过扩展后的示意图；

图 6 是图 2 中步骤 S120 的具体方法的流程图；

图 7 是图 6 中步骤 S124 的具体方法的流程图；

图 8 是图 6 中步骤 S124 的另一具体方法的流程图；

图 9 是图 5 中步骤 S1244 的具体方法的流程图；

图 10 是图 6 中步骤 S122 的具体方法的流程图；

图 11 是图 10 中步骤 S1222 的具体方法的流程图；

图 12 是图 2 中步骤 S120 的另一具体方法的流程图；

图 13 是图 12 中步骤 S128 的具体方法的流程图；

图 14 是图 12 中步骤 S128 的另一具体方法的流程图；

图 15 是图 14 中步骤 S1284 的具体方法的流程图；

图 16 是图 12 中步骤 S126 的具体方法的流程图；

图 17 是图 16 中步骤 S1262 的具体方法的流程图；

图 18 是本申请另一个实施例提供的信息处理方法的流程图；

图 19 是图 18 中步骤 S150 的具体方法的流程图；

图 20 是图 18 中步骤 S150 的另一具体方法的流程图；

图 21 是图 18 中步骤 S150 的另一具体方法的流程图；

图 22 是本申请一个具体示例提供的信息处理方法的流程图。

**具体实施方式**

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

需要说明的是，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于流程图中的顺序执行所示出或描述的步骤。说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

本申请提供了一种信息处理方法、中间解析器、网络设备及存储介质，当接收到第一域名系统请求信息，将第一域名系统请求信息转换成包括有密文敏感信息和第一密文标记信息的第二域名系统请求信息，接着将第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据密文敏感信息和第一密文标记信息进行信息处理，即是说，本申请实施例的方案通过将包括有密文敏感信息和第一密文标记信息的第二域名系统请求信息进行传输，无需对整个第一域名系统请求信息进行加密处理，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

下面结合附图，对本申请实施例作进一步阐述。

如图 1 所示，图 1 是本申请一个实施例提供的用于执行信息处理方法的系统架构的示意图。在图 1 的示例中，该系统架构包括客户端设备 110、中间解析器 120 和权威域名系统服务器 130。其中，中间解析器 120 分别与客户端设备 110 和权威域名系统服务器 130 通信连接。

中间解析器 120 能够接收由客户端设备 110 发送的第一域名系统请求信息，并且，在第一域名系统请求信息携带有敏感信息的情况下，中间解析器 120 能够对第一域名系统请求信息中的敏感信息进行加密，得到携带有密文敏感信息的第二域名系统请求信息；在第一域名系统请求信息不携带敏感信息的情况下，中间解析器 120 能够获取与客户端设备 110 对应的敏感信息，并对该敏感信息进行加密，接着结合第一域名系统请求信息生成携带有密文敏感信息的第二域名系统请求信息。此外，第二域名系统请求信息还携带有用于指示密文敏感信息为密文信息的第一密文标记信息。另外，中间解析器 120 还能够将第二域名系统请求信息发送至权威域名系统服务器 130，使得权威域名系统服务器 130 能够根据密文敏感信息和第一密文标记信息进行相关的信息处理。此外，中间解析器 120 还能够从权威域名系统服务器

130 获取包括有反馈类型信息和第二密文标记信息的反馈信息，中间解析器 120 能够根据反馈类型信息和第二密文标记信息将反馈信息转发至客户端设备 110，或者重新构建新的域名系统请求信息并发送给权威域名系统服务器 130，使得权威域名系统服务器 130 对新的域名系统请求信息重新进行处理。

本申请实施例描述的系统架构以及应用场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域技术人员可知，随着系统架构的演变和新应用场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本领域技术人员可以理解的是，图 1 中示出的系统架构并不构成对本申请实施例的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

基于上述系统架构，下面提出本申请的数据处理方法的各个实施例。

如图 2 所示，图 2 是本申请一个实施例提供的信息处理方法的流程图，该信息处理方法，可以应用于中间解析器，例如图 1 所示系统架构中的中间解析器 120。该信息处理方法可以包括但不限于有步骤 S110、步骤 S120 和步骤 S130。

步骤 S110：接收第一域名系统请求信息。

本步骤中，第一域名系统请求信息用于请求域名与网际协议互联地址间的映射关系。第一域名系统请求信息的发起方包括但不限于需要获取域名与网际协议互联地址间映射关系的客户端设备，第一域名系统请求信息的接收方包括但不限于互联网服务提供商设备和中间解析器。

在一实施例中，第一域名系统请求信息可以携带对应于第一域名系统请求信息的发送方的敏感信息，该敏感信息可以用于表征该发送方对应的网际协议互联地址或该发送方设备对应的硬件标识码。

具体地，在一实施例中，第一域名系统请求信息可以包括扩展域名系统客户端子网选项（EDNS Client Subnet，ECS）信息，该扩展域名系统客户端子网选项信息携带有敏感信息。在一实施例中，第一域名系统请求信息基于域名系统的扩展名机制（Extension Mechanisms for DNS，EDNS）协议，如 IETF RFC 6891 协议，以及部分扩展域名系统客户端子网协议，如 IETF RFC 7871 协议所定义的消息体结构生成。

具体地，在一实施例中，采用一种传递包大小的域名系统的扩展名机制协议所定义的数据结构生成第一域名系统请求信息。

在一实施例中，第一域名系统请求信息以用户数据报协议（User Datagram Protocol，UDP）封装后发送。

步骤 S120：根据第一域名系统请求信息得到第二域名系统请求信息。其中，第二域名系统请求信息包括密文敏感信息和第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息。

本步骤中，由于在步骤 S110 中接收到了第一域名系统请求信息，因此可以对该第一域名系统请求信息进行第一信息处理，得到包括由敏感信息经过加密后生成的密文敏感信息的第二域名系统请求信息，以便于后续步骤可以将该包括有密文敏感信息的第二域名系统请求信息信息发送给权威域名系统服务器。

需要说明的是，第一域名系统请求信息可以携带有敏感信息，也可以不携带敏感信息，

本申请实施例对此不做具体限定。

需要说明的是，对第一域名系统请求信息进行第一信息处理得到第二域名系统请求信息，可以有不同的实施方式，本实施例对此并不作具体限定。例如，在第一域名系统请求信息携带有敏感信息的情况下，可以先将第一域名系统请求信息按照其各个组成部分拆分成各个数据部分，然后在这些数据部分中识别出敏感信息，再对识别出的敏感信息进行加密处理得到密文敏感信息，接着将密文敏感信息和第一域名系统请求信息中的其他数据合并形成第二域名系统请求信息；又如，可以先在第一域名系统请求信息中识别出敏感信息，然后对识别出的敏感信息进行加密处理得到密文敏感信息，接着将第一域名系统请求信息中的敏感信息更新为密文敏感信息得到第二域名系统请求信息。其中，在第一域名系统请求信息的各个数据部分中识别出敏感信息，或者直接在第一域名系统请求信息中识别出敏感信息，可以基于预先定义的识别规则进行识别，也可以基于智能分析过程进行识别，本实施例对此并不作具体限定。例如，当基于预先定义的识别规则进行识别时，该预先定义的识别规则定义了哪些表的哪些字段属于敏感信息；当基于智能分析过程进行识别时，可以根据数据的具体内容自动判断是否属于敏感信息。再如，在第一域名系统请求信息不携带敏感信息的情况下，可以由第一域名系统请求信息的接收方，如中间解析器，生成对应于该接收方的敏感信息，然后对该敏感信息进行加密处理得到密文敏感信息，接着将密文敏感信息和第一域名系统请求信息中的其他数据合并形成第二域名系统请求信息，或者将第一域名系统请求信息中的敏感信息更新为密文敏感信息得到第二域名系统请求信息。

在一实施例中，第一域名系统请求信息是基于 RFC6891 协议中定义的基于域名系统的扩展名机制信息，第二域名系统请求信息对于 RFC6891 协议定义的消息体结构中的 TTL 元素和 RDATA 元素进行了扩展。

具体地，如图 3 所示，图 3 是本申请一个实施例提供的一种消息体子结构的示意图。参照图 3，本申请实施例对 RFC6891 协议定义的消息体结构中的 TTL 元素进行了扩展，TTL 元素的消息体子结构中包括有 OPTION-CODE 字段、OPTION-LENGTH 字段和 EXTENDED-RCODE 字段，其中，EXTENDED-RCODE 字段用于表示域名系统请求信息经过了扩展，采用了扩展返回消息类型，此字段和域名系统请求信息中头部字段中的 RCODE 字段合并可以表示除普通域名系统请求返回消息之外更多的类型。例如，EXTENDED-RCODE 字段和 RCODE 字段合并后为 0x1 则表示本域名系统请求信息采用了本申请实施例中的扩展返回消息类型。此外，当 EXTENDED-RCODE 字段为 0 则表示不使用扩展返回消息类型。因此，本申请实施例中的 EXTENDED-RCODE 字段需要在域名系统请求消息生成时赋值为非 0 值。

需要说明的是，本申请实施例仅对 TTL 元素的消息体子结构的 EXTENDED-RCODE 字段进行了扩展，并未改变由 RFC6891 协议定义的消息体结构，从而保证了兼容性。

如图 4 所示，图 4 是本申请一个实施例提供的另一种消息体子结构的示意图，参照图 4，本申请实施例对 RFC6891 协议定义的消息体结构中的 RDATA 元素的消息体子结构包括有 OPTION-DATA 字段，该字段可以容纳多个附加信息，本申请实施例对于 OPTION-DATA 字段进行了扩展。

具体地，参照图 5，图 5 是图 4 中的 RDATA 元素的消息体子结构经过扩展后的示意图，在图 5 的示例中，OPTION-DATA 字段经过扩展后包括 FAMILY 字段、ENCRYPTION TYPE

字段、ENCRYPTION FLAG 字段和 SIGNATURE 字段。本申请实施例将该种消息体子结构的类型定义为伪地址（Pseudo Address，PADR）类型，上述 FAMILY 字段、ENCRYPTION TYPE 字段、ENCRYPTION FLAG 字段和 SIGNATURE 字段的集合定义为 PADR 字段。

RDATA 元素的消息体子结构中的 OPTION-CODE 字段在本申请实施例中用于表示域名系统请求信息是否携带有加密后的密文敏感信息，也即表示域名系统请求信息是否携带有用户端设备的网际协议地址或中间解析器的网际协议地址经过加密后得到的伪地址。

OPTION-LENGTH 字段用于表示整个 OPTION-DATA 字段的长度。

FMAILY 字段用于表示域名系统请求信息中携带的密文敏感信息的类型。例如，当密文敏感信息是经过加密后的网际协议版本 4（Internet Protocol version 4，IPv4）地址，则 FMAILY 字段赋值为 1，当密文敏感信息是经过加密后的网际协议版本 6（Internet Protocol version 6，IPv6）地址，则 FMAILY 字段赋值为 2。

ECRYPTION TYPE 字段用于表示对敏感信息进行加密所使用的加密算法类型。例如，当敏感信息未经加密，则 ECRYPTION TYPE 字段赋值为 0，当采用 MD5 信息摘要算法对敏感信息进行加密，则 ECRYPTION TYPE 字段赋值为 1，当使用使用安全散列算法 1（Secure Hash Algorithm 1，SHA-1）则 ECRYPTION TYPE 字段赋值为 2。

ECRYPTION FLAG 字段是代表加密敏感信息是否通过验证。例如中间解析器能够通过权威域名系统服务器向中间解析器发送的反馈细信息中的 ECRYPTION FLAG 字段是否发生变化来判断权威域名系统服务器是否成功对密文敏感信息进行了解密。

SIGNATURE 字段用于存储对需要保护的信息进行加密后生成的字符串，例如 SIGNATURE 字段可以存储密文敏感信息，或者可以用于存储加密敏感信息所使用的密钥。

此外，RDATA 元素的消息体结构中还可以包括扩展域名系统客户端子网选项信息，该扩展域名系统客户端子网选项信息同样可以用于存储密文敏感信息。

需要说明的是，扩展域名系统客户端子网选项信息紧随在域名系统请求信息中的上一个消息体的结尾之后或者之前，伪地址字段的位置可以不固定。

具体地，在域名系统请求信息同时设置有伪地址字段和扩展域名系统客户端子网选项信息时，伪地址字段和扩展域名系统客户端子网选项信息相邻设置。

在一实施例中，当密文敏感信息存储于域名系统请求信息的 SIGNATURE 字段中，则可以不设置扩展域名系统客户端子网选项信息，或者将扩展域名系统客户端子网选项信息赋值为 0。

步骤 S130：将第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据密文敏感信息和第一密文标记信息进行信息处理。

本步骤中，由于在步骤 S120 中得到了包括密文敏感信息和第一密文标记信息的第二域名系统请求信息，因此可以将该第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器可以根据密文敏感信息和第一密文标记信息进行数据处理。由于本申请实施例并未对整个第一域名系统请求信息进行加密处理，而是能够将敏感信息单独加密得到携带有密文敏感信息的第二域名系统请求信息以实现对敏感信息的保护，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务

器对第二域名系统请求信息的处理准确性。

需要说明的是，权威域名系统服务器在根据密文敏感信息和第一密文标记信息进行信息处理后，会向中间解析器发送反馈结果，中间解析器能够根据该反馈结果判断权威域名系统服务器是否反馈了正确的域名与网际协议互联地址间的映射关系。

在一实施例中，第一域名系统请求信息包括第一扩展域名系统附加选项信息，其中，第一扩展域名系统附加选项信息包括源端敏感信息。第一扩展域名系统附加选项信息是根据扩展域名系统客户端子网协议生成的，源端敏感信息包括但不限于客户端设备的网际互连协议地址。

在一实施例中，第一密文标记信息存储于第二域名系统请求信息的 OPTION-CODE 字段，OPTION-CODE 字段在本申请实施例中用于表示域名系统请求信息是否携带有加密后的密文敏感信息，也即表示域名系统请求信息是否携带有用户端设备的网际协议地址或中间解析器的网际协议地址经过加密后得到的伪地址。

如图 6 所示，图 6 是图 2 中步骤 S120 的具体方法的流程图，图 6 对步骤 S120 进行进一步的说明，该步骤 S120 可以包括但不限于步骤 S121、步骤 S122、步骤 S123、步骤 S124 和步骤 S125。

步骤 S121：获取第一扩展域名系统附加选项信息中的源端敏感信息。

本步骤中，源端敏感信息由客户端设备生成后添加至第一域名系统请求信息中，具体地，第一域名系统请求信息包括第一扩展域名系统附加选项信息，源端敏感信息由客户端设备生成后添加至第一扩展域名系统附加选项信息中。源端敏感信息用于表征客户端设备的网际互联协议地址。

需要说明的是，第一扩展域名系统附加选项信息可以由客户端设备生成，也可以由中间解析器生成。

需要说明的是，源端敏感信息并非仅仅限定于仅由客户端设备生成，例如，连接到用户端设备一侧的第一中间解析器用于实现第一域名系统请求信息的数据穿透，第一中间解析器获取到第一域名系统请求信息后会校验第一域名系统请求信息是否携带有源端敏感信息，在第一域名系统请求信息未携带源端敏感信息的情况下，第一中间解析器会根据第一域名系统请求信息获取本地敏感信息，并向第二中间解析器发送携带有该本地敏感信息的第一域名系统请求信息，该本地敏感信息即用于替代由客户端设备生成的源端敏感信息，第二中间解析器在接收到该第一域名系统请求信息后，对第一域名系统请求信息中的本地敏感信息进行加密处理得到密文敏感信息。

在一实施例中，源端敏感信息可以存储在第一扩展域名系统附加选项信息中的 ADDRESS 字段中。

在一实施例中，源端敏感信息也可以存储在第一域名系统请求信息的 SIGNATURE 字段中。

步骤 S122：对源端敏感信息进行加密处理得到密文敏感信息。

需要说明的是，对源端敏感信息进行加密处理而采用到的加密算法，可以是对称加密算法、高级加密标准或者其他加密算法，可以根据实际的应用情况而进行适当的选择，本实施例对此并不作具体限定。其中，对称加密算法是指加密和解密使用相同密钥的加密算法，收发双方在进行安全通信之前，需要商定一个公共密钥。高级加密标准又称 Rijndael 加密法，

是一种区块加密标准，能够支持更大范围的区块和密钥长度。

需要说明的是，对敏感数据进行加密处理而采用到的加密算法或加密策略等信息，可以包含在中间解析器中，也可以是中间解析器从其他地方获取得到，例如从权威域名系统服务器中获取得到或者从第一域名系统请求信息中获取得到，本实施例对此并不作具体限定。

在一实施例中，加密后的密文敏感信息存储于第二域名系统请求信息 PADR 字段的 SIGNATURE 字段中。

在一实施例中，第二域名系统请求信息包括扩展域名系统客户端子网选项信息，加密后的密文敏感信息存储于该扩展域名系统客户端子网选项信息中。

在一实施例中，第二域名系统请求信息包括 ECRYPTION TYPE 字段，ECRYPTION TYPE 字段用于表示对敏感信息进行加密所使用的加密算法类型。例如，当敏感信息未经加密，则 ECRYPTION TYPE 字段赋值为 0，当采用 MD5 信息摘要算法对敏感信息进行加密，则 ECRYPTION TYPE 字段赋值为 1，当使用使用安全散列算法 1（Secure Hash Algorithm 1，SHA-1）则 ECRYPTION TYPE 字段赋值为 2。

步骤 S123：构建第一附加选项信息，其中，第一附加选项信息包括第一密文标记信息。

本步骤中，第一附加选项信息包括第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息，权威域名系统服务器在接收到第二域名系统请求信息后首先检测该第二域名系统请求信息是否携带有第一密文标记信息，在权威域名系统服务器检测到第一密文标记信息的情况下，权威域名系统服务器对密文敏感信息进行解密。

在一实施例中，第一附加选项信息存储于第二域名系统请求信息的 RDATA 元素的消息体子结构中。

在一实施例中，密文标记信息存储于第二域名系统请求信息 OPTION-CODE 字段中。

步骤 S124：根据密文敏感信息和第一附加选项信息得到第二域名系统请求信息。

本步骤中，将密文敏感信息和第一域名系统请求信息中的第一附加选项信息合并形成第二域名系统请求信息，由于本申请实施例并未对整个第一域名系统请求信息进行加密处理，而是能够将敏感信息单独加密得到携带有密文敏感信息的第二域名系统请求信息以实现对敏感信息的保护，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

需要说明的是，本申请实施例中的密文敏感信息与第一附加选项信息不限于是并列关系，例如，密文敏感信息和第一附加选项信息可以存储于第二域名系统请求信息中的两个不同的字段中，再如，密文敏感信息可以包含于第一附加选项信息中，使得密文敏感信息和第一附加选项信息可以存储于第二域名系统请求信息中的同一个字段中。

在一实施例中，第一附加选项信息包括第一加密签名字段。

如图 7 所示，图 7 是图 6 中步骤 S124 的具体方法的流程图，图 7 对步骤 S124 进行进一步的说明，该步骤 S124 可以包括但不限于有步骤 S1241 和步骤 S1242。

步骤 S1241：将密文敏感信息填充进第一加密签名字段。

本步骤中，密文敏感信息被填充进第一加密签名字段，第一加密签名字段被包含在第一附加选项信息中，第一附加选项信息可以是根据扩展域名系统客户端子网选项协议生成的，

也可以是根据扩展域名系统客户端子网协议生成的。权威域名系统服务器在获取到第二域名系统请求信息后对其进行解析以获得第一附加选项信息，并通过检测第一附加选项信息中的第一加密签名字段获取密文敏感信息。

在一实施例中，密文敏感信息被填充进第二域名系统请求信息的 SIGNATURE 字段中。

步骤 S1242：根据包括第一密文标记信息和密文敏感信息的第一附加选项信息，得到第二域名系统请求信息。

本步骤中，权威域名系统服务器在获取到第二域名系统请求信息后对其进行解析以获得第一附加选项信息，并通过检测第一附加选项信息中的第一加密签名字段获取密文敏感信息。在一实施例中，第一密文标记信息也可以通过第一附加选项信息得到。

如图 8 所示，图 8 是图 6 中步骤 S124 的另一具体方法的流程图，图 8 对步骤 S124 进行进一步的说明，该步骤 S124 还可以包括但不限于有步骤 S1243 和步骤 S1244。

步骤 S1243：将第一扩展域名系统附加选项信息中的源端敏感信息更新为密文敏感信息。

本步骤中，将第一扩展域名系统附加选项信息中的源端敏感信息更新为密文敏感信息，因此第二域名系统请求信息相比第一域名系统请求信息仅对于源端敏感信息进行了加密，且源端敏感信息进行加密后生成的密文敏感信息仍包含于第一扩展域名系统附加选项信息中，因此第二域名系统请求信息并未整体进行加密，相比第一域名系统请求信息，第二域名系统请求信息于第一域名系统请求信息仍具有相同的数据结构，因此，本申请实施例的方案通过将包括有密文敏感信息和第一密文标记信息的第二域名系统请求信息进行传输，无需对整个第一域名系统请求信息进行加密处理，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

在一实施例中，源端敏感信息存储在第一域名系统请求信息的 SIGNATURE 字段中，通过对源端敏感信息进行加密得到密文敏感信息，并将密文敏感信息填充进第一域名系统请求信息的 SIGNATURE 字段中以得到第二域名系统请求信息。

步骤 S1244：根据更新后的第一扩展域名系统附加选项信息和第一附加选项信息得到第二域名系统请求信息。

本步骤中，中间解析器根据更新后的第一扩展域名系统附加选项信息和第一附加选项信息得到第二域名系统请求信息，由于源端敏感信息经加密后的密文敏感信息仍包含在第一扩展域名系统附加选项信息中，因此，本申请实施例无需对整个第一域名系统请求信息进行加密处理，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

在一实施例中，第一扩展域名系统附加选项信息中存储有加密敏感信息所使用的密钥，第一附加选项信息包括存储有密文敏感信息的 SIGNATURE 字段，因此根据更新后的第一扩展域名系统附加选项信息和第一附加选项信息得到第二域名系统请求信息，其仅仅对敏感信息进行了加密，并未对整个域名系统请求信息进行加密。

如图 9 所示，图 9 是图 5 中步骤 S1244 的具体方法的流程图，图 9 对步骤 S1244 进行进一步的说明，该步骤 S1244 可以包括但不限于有步骤 S12441 和步骤 S12442。

步骤 S12441：在第一加密签名字段中填充密钥信息或者第一签名信息，其中，密钥信息用于解密密文敏感信息，第一签名信息用于验证加密后的源端敏感信息的完整性。

本步骤中，密钥信息可以是加密敏感信息所使用的公钥，权威域名系统服务器能够根据该密钥信息对密文敏感信息进行解密，此外，密钥信息还可以反应加密敏感信息时所使用的加密算法。第一签名信息可以用于对加密后的源端敏感信息进行校验，以保证加密后的源端敏感信息的完整性。

在一实施例中，第二域名系统请求信息的 SIGNATURE 字段也可以用于存储加密敏感信息所使用的公钥。

步骤 S12442：根据更新后的第一扩展域名系统附加选项信息，以及包括密钥信息或者第一签名信息的第一附加选项信息，得到第二域名系统请求信息。

本步骤中，第二域名系统请求信息相比第一域名系统请求信息更新了第一扩展域名系统附加选项信息以及包括有密钥信息或者第一签名信息的第一附加选项信息，因此，本申请实施例无需对整个第一域名系统请求信息进行加密处理，从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

在一实施例中，第一扩展域名系统附加选项信息中可以存储有密文敏感信息，也可以存储有加密敏感信息所使用的密钥，第一附加选项信息包括存储有 SIGNATURE 字段，SIGNATURE 字段可以存储密文敏感信息，也可以存储用于加密敏感信息所使用的密钥。因此根据更新后的第一扩展域名系统附加选项信息和第一附加选项信息得到第二域名系统请求信息，其仅仅对敏感信息进行了加密，并未对整个域名系统请求信息进行加密。

如图 10 所示，图 10 是图 6 中步骤 S122 的具体方法的流程图，图 10 对步骤 S122 进行进一步的说明，该步骤 S122 可以包括但不限于有步骤 S1221 和步骤 S1222。

步骤 S1221：根据源端敏感信息的信息长度确定第一加密策略信息，其中，第一加密策略信息包括第一密文长度。

本步骤中，通过源端敏感信息的信息长度确定第一加密策略信息。当源端敏感信息为网际协议版本 4 地址，中间解析器能够通过检测源端敏感信息的信息长度确定远端敏感信息类型为网际协议版本 4 地址，并将第一加密策略信息配置为对应于网际协议版本 4 地址的第一加密策略信息。当源端敏感信息为网际协议版本 6 地址，中间解析器能够通过检测源端敏感信息的信息长度确定远端敏感信息类型为网际协议版本 6 地址，并将第一加密策略信息配置为对应于网际协议版本 6 地址的第一加密策略信息。

在一实施例中，第一加密策略信息除了包括第一密文长度，还包括对于源端敏感信息的加密方法，例如，当源端敏感信息对应于网际协议版本 4 地址，根据加密方法，首先从源端敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进

制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用哈希算法获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。

又如，当源端敏感信息对应于网际协议版本 6 地址，根据加密方法，将源端敏感信息视为一个整字符串进行加密，该过程所使用的加密算法包括但不限于 MD5 信息摘要算法，由于源端敏感信息为网际协议版本 6 地址，因此需要预留 128 位的地址空间。

再如，当源端敏感信息过长，根据加密策略，对源端敏感信息进行二次加密处理以缩减加密后的密文敏感信息的位数。

在一实施例中，源端敏感信息的信息长度可以通过第一域名系统请求信息中的 SIGNATURE 确定，或者通过第一域名系统请求信息中的第一扩展域名系统附加选项信息中数据的长度确定。

步骤 S1222：根据第一加密策略信息对源端敏感信息进行加密处理得到密文敏感信息，其中，密文敏感信息的信息长度与第一密文长度相匹配。

本步骤中，根据第一加密策略信息对源端敏感信息进行加密处理得到密文敏感信息，例如，当源端敏感信息对应网际协议版本 4 地址，第一加密策略信息则配置为对应于网际协议版本 4 地址的第一加密策略信息，具体地，首先从源端敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用哈希算法获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。

此外，当源端敏感信息对应网际协议版本 6 地址，第一加密策略信息则配置为对应于网际协议版本 6 地址的第一加密策略信息，将源端敏感信息视为一个整字符串进行加密，该过程所使用的加密算法包括但不限于 MD5 信息摘要算法，由于源端敏感信息为网际协议版本 6 地址，因此需要预留 128 位的地址空间。

在一实施例中，第一域名系统请求信息基于本申请实施例的伪地址类型消息体构建，通过第一域名系统请求信息能够得知源端敏感信息的类型，例如，若源端敏感信息对应网际协议版本 4 地址，则将第二域名系统请求信息的 FAMILY 字段赋值为 1，若源端敏感信息对应网际协议版本 6 地址，则将第二域名系统请求信息的 FAMILY 字段赋值为 2。

在一实施例中，源端敏感信息的类型是通过第一域名系统请求信息的 FAMILY 字段确定的，例如，当第一域名系统请求信息的 FAMILY 字段赋值为 1，则源端敏感信息对应网际协议版本 4 地址，当第一域名系统请求信息的 FAMILY 字段赋值为 1，则源端敏感信息对应网际协议版本 6 地址。

如图 11 所示，图 11 是图 10 中步骤 S1222 的具体方法的流程图，图 11 对步骤 S1222 进行进一步的说明，当第一域名系统请求信息不包括第一扩展域名系统附加选项信息，该步骤 S1222 可以包括但不限于有步骤 S12221 和步骤 S12222。

步骤 S12221：根据第一加密策略信息对源端敏感信息进行第一加密处理得到第一密文信息。

本步骤中，根据第一加密策略信息对源端敏感信息进行第一加密处理得到第一密文信息，

第一密文信息可以是根据源端敏感信息得到的网际互连协议地址，例如，当源端敏感信息对应网际协议版本 4 地址，第一加密策略信息则配置为对应于网际协议版本 4 地址的第一加密策略信息，具体地，首先从源端敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址。又如，当源端敏感信息对应网际协议版本 6 地址，第一加密策略信息则配置为对应于网际协议版本 6 地址的第一加密策略信息，通过源端敏感信息进行第一加密处理得到 128 位的网际协议版本 6 地址。

步骤 S12222：根据第一加密策略信息对第一密文信息进行第二加密处理得到密文敏感信息，其中，密文敏感信息的信息长度小于第一密文信息的信息长度。

本步骤中，根据第一加密策略信息对第一密文信息进行第二加密处理得到密文敏感信息，例如，首先从源端敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用第二加密处理获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。由于地址位数限制，若网际协议版本 4 地址经过一次第二加密处理后仍超过 32 位，则再次进行至少一次第二加密处理，以防止加密处理后得到的密文敏感信息的信息长度大于第一密文的信息长度而导致信息丢失。

又如，当源端敏感信息对应网际协议版本 6 地址，第一加密策略信息则配置为对应于网际协议版本 6 地址的第一加密策略信息，将源端敏感信息视为一个整字符串进行加密，该过程所使用的加密算法包括但不限于，由于源端敏感信息对应网际协议版本 6 地址，因此需要预留 128 位的地址空间。若源端敏感信息经过第一加密处理后获得的网际协议版本 6 地址经过一次第二加密处理后信息长度仍超过 128 位，则再次进行至少一次第二加密处理，以防止加密处理后得到的密文敏感信息的信息长度大于第一密文的信息长度而导致信息丢失。

在一实施例中，第二加密处理采用的算法包括但不限于哈希算法或 MD5 信息摘要算法。

在一实施例中，对密文敏感信息进行加密后，根据对敏感信息进行加密所使用的加密算法类型设置 ECRYPTION TYPE 字段。例如，当敏感信息未经加密，则 ECRYPTION TYPE 字段赋值为 0，当采用 MD5 信息摘要算法对敏感信息进行加密，则 ECRYPTION TYPE 字段赋值为 1，当使用使用安全散列算法 1（Secure Hash Algorithm 1，SHA-1）则 ECRYPTION TYPE 字段赋值为 2。

如图 12 所示，图 12 是图 2 中步骤 S120 的另一具体方法的流程图，图 12 对步骤 S120 进行进一步的说明，当第一域名系统请求信息不包括第一扩展域名系统附加选项信息，该步骤 S120 可以包括但不限于有步骤 S125、步骤 S126、步骤 S127 和步骤 S128。

步骤 S125：根据第一域名系统请求信息获取本地敏感信息。

本步骤中，中间解析器首先检测获取到的第一域名系统请求信息是否携带有敏感信息，由于敏感信息携带于系统客户端子网选项信息，因此通过检测第一域名系统请求信息是否包括第一扩展域名系统附加选项信息即可确定第一域名系统请求信息是否携带有敏感信息。当

第一域名系统请求信息未携带敏感信息，则该中间解析器获取本地敏感信息。本地敏感信息包括但不限于该中间解析器的网际互联协议地址以及该中间解析器的硬件标识码。

步骤 S126：对本地敏感信息进行加密处理得到密文敏感信息。

需要说明的是，对本地敏感信息进行加密处理而采用到的加密算法，可以是对称加密算法、高级加密标准或者其他加密算法，可以根据实际的应用情况而进行适当的选择，本实施例对此并不作具体限定。其中，对称加密算法是指加密和解密使用相同密钥的加密算法，收发双方在进行安全通信之前，需要商定一个公共密钥。高级加密标准又称 Rijndael 加密法，是一种区块加密标准，能够支持更大范围的区块和密钥长度。

需要说明的是，对敏感数据进行加密处理而采用到的加密算法或加密策略等信息，可以包含在中间解析器中，也可以是中间解析器从其他地方获取得到，例如从权威域名系统服务器中获取得到或者从第一域名系统请求信息中获取得到，本实施例对此并不作具体限定。

在一实施例中，加密后的密文敏感信息存储于第二域名系统请求信息 PADR 字段的 SIGNATURE 字段中。

在一实施例中，第二域名系统请求信息包括扩展域名系统客户端子网选项信息，加密后的密文敏感信息存储于该扩展域名系统客户端子网选项信息中。

在一实施例中，第二域名系统请求信息包括 ECRYPTION TYPE 字段，ECRYPTION TYPE 字段用于表示对敏感信息进行加密所使用的加密算法类型。例如，当敏感信息未经加密，则 ECRYPTION TYPE 字段赋值为 0，当采用 MD5 信息摘要算法对敏感信息进行加密，则 ECRYPTION TYPE 字段赋值为 1，当使用使用安全散列算法 1（Secure Hash Algorithm 1，SHA-1）则 ECRYPTION TYPE 字段赋值为 2。

步骤 S127：构建第二附加选项信息，其中，第二附加选项信息包括第一密文标记信息。

本步骤中，第二附加选项信息包括第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息，权威域名系统服务器在接收到第二域名系统请求信息后首先检测该第二域名系统请求信息是否携带有第一密文标记信息，在权威域名系统服务器检测到第一密文标记信息的情况下，权威域名系统服务器对密文敏感信息进行解密。

在一实施例中，第一域名系统请求信息是根据扩展域名系统客户端子网选项协议构建的，第二附加选项信息可以包含在扩展域名系统客户端子网选项信息中。

在一实施例中，第二附加选项信息存储于第二域名系统请求信息的 RDATA 元素的消息体子结构中。

在一实施例中，第一域名系统请求信息是根据扩展域名系统客户端子网选项协议构建的，第二附加选项信息可以包含在扩展域名系统客户端子网选项信息中。

在一实施例中，第一密文标记信息存储于第二域名系统请求信息的 OPTION-CODE 字段，OPTION-CODE 字段在本申请实施例中用于表示域名系统请求信息是否携带有加密后的密文敏感信息，也即表示域名系统请求信息是否携带有用户端设备的网际协议地址或中间解析器的网际协议地址经过加密后得到的伪地址。

步骤 S128：根据密文敏感信息和第二附加选项信息得到第二域名系统请求信息。

本步骤中，将密文敏感信息和第一域名系统请求信息中的第二附加选项信息合并形成第二域名系统请求信息，由于本申请实施例的方案通过将包括有密文敏感信息和第一密文标记信息的第二域名系统请求信息进行传输，无需对整个第一域名系统请求信息进行加密处理，

从而能够在避免敏感信息暴露在安全风险之下的情况下，降低网络资源的开销，从而降低设备的维护成本；另外，由于第一密文标记信息用于指示密文敏感信息为密文信息，因此权威域名系统服务器可以根据第一密文标记信息对密文敏感信息进行适当的解密处理，从而可以提高权威域名系统服务器对第二域名系统请求信息的处理准确性。

需要说明的是，本申请实施例中的密文敏感信息与第二附加选项信息不限于是并列关系，例如，密文敏感信息和第二附加选项信息可以存储于第二域名系统请求信息中的两个不同的字段中，再如，密文敏感信息可以包含于第二附加选项信息中，使得密文敏感信息和第二附加选项信息可以存储于第二域名系统请求信息中的同一个字段中。

在一实施例中，第二附加选项信息包括第二加密签名字段。

如图 13 所示，图 13 是图 12 中步骤 S128 的具体方法的流程图，图 13 对步骤 S128 进行进一步的说明，该步骤 S128 可以包括但不限于有步骤 S1281 和步骤 S1282。

步骤 S1281：将密文敏感信息填充进第二加密签名字段。

本步骤中，密文敏感信息被填充进第二加密签名字段，第二加密签名字段被包含在第二附加选项信息中，第二附加选项信息可以是根据扩展域名系统客户端子网选项协议生成的，也可以是根据扩展域名系统客户端子网协议生成的。权威域名系统服务器在获取到第二域名系统请求信息后对其进行解析以获得第二附加选项信息，并通过检测第二附加选项信息中的第二加密签名字段获取密文敏感信息。

在一实施例中，密文敏感信息被填充进第二域名系统请求信息的 SIGNATURE 字段中。

步骤 S1282：根据包括第一密文标记信息和密文敏感信息的第二附加选项信息，得到第二域名系统请求信息。

本步骤中，权威域名系统服务器在获取到第二域名系统请求信息后对其进行解析以获得第二附加选项信息，并通过检测第二附加选项信息中的第二加密签名字段获取密文敏感信息。如图 14 所示，图 14 是图 12 中步骤 S128 的另一具体方法的流程图，图 14 对步骤 S128 进行进一步的说明，该步骤 S128 还可以包括但不限于有步骤 S1283 和步骤 S1284。

步骤 S1283：根据密文敏感信息构建第二扩展域名系统附加选项信息，其中，第二扩展域名系统附加选项信息包括密文敏感信息。

本步骤中，根据密文敏感信息构建第二扩展域名系统附加选项信息，因此第二域名系统请求信息相比第一域名系统请求信息仅对于本地敏感信息进行了加密，且本地敏感信息进行加密后生成的密文敏感信息仍包含于第二扩展域名系统附加选项信息中，因此第二域名系统请求信息并未整体进行加密，相比第一域名系统请求信息，第二域名系统请求信息于第一域名系统请求信息仍具有相同的数据结构，因此，本申请实施例并未对整个第一域名系统请求信息进行加密处理，而是能够将敏感信息单独加密得到携带有密文敏感信息的第二域名系统请求信息以实现对敏感信息的保护，使得传输路径中的设备无需支持整个域名系统请求信息的加密和解密处理，从而减少了网络资源的开销，降低了设备的维护成本。

在一实施例中，密文敏感信息填充至第二扩展域名系统附加选项信息中，此外，第二扩展域名系统附加选项信息还可用于保存加密后的密文敏感信息所使用的密钥。

在一实施例中，密文敏感信息可以存储在第二扩展域名系统附加选项信息中的 ADDRESS 字段中。

步骤 S1284：根据第二扩展域名系统附加选项信息和第二附加选项信息得到第二域名系

统请求信息。

本步骤中，中间解析器根据第二附加选项信息得到第二域名系统请求信息，由于本地敏感信息经加密后的密文敏感信息仍包含在第二附加选项信息中，因此，本申请实施例并未对整个第一域名系统请求信息进行加密处理，而是能够将敏感信息单独加密得到携带有密文敏感信息的第二域名系统请求信息以实现对敏感信息的保护，使得传输路径中的设备无需支持整个域名系统请求信息的加密和解密处理，从而减少了网络资源的开销，降低了设备的维护成本。

在一实施例中，第一扩展域名系统附加选项信息中可以存储有密文敏感信息，也可以存储有加密敏感信息所使用的密钥，第二附加选项信息包括存储有 SIGNATURE 字段，SIGNATURE 字段可以存储密文敏感信息，也可以存储用于加密敏感信息所使用的密钥。因此根据更新后的第一扩展域名系统附加选项信息和第二附加选项信息得到第二域名系统请求信息，其仅仅对敏感信息进行了加密，并未对整个域名系统请求信息进行加密。

如图 15 所示，图 15 是图 14 中步骤 S1284 的具体方法的流程图，图 15 对步骤 S1284 进行进一步的说明，该步骤 S1284 可以包括但不限于有步骤 S12841 和步骤 S12842。

步骤 S12841：在第二加密签名字段中填充密钥信息或者第二签名信息，其中，密钥信息用于解密密文敏感信息，第二签名信息用于验证加密后的本地敏感信息的完整性。

本步骤中，密钥信息可以是加密敏感信息所使用的公钥，权威域名系统服务器能够根据该密钥信息对密文敏感信息进行解密，此外，密钥信息还可以反应加密敏感信息时所使用的加密算法。第二签名信息可以用于对加密后的本地敏感信息进行校验，以保证本地敏感信息的完整性。

在一实施例中，第二域名系统请求信息的 SIGNATURE 字段也可以用于存储加密敏感信息所使用的公钥。

步骤 S12842：根据第二扩展域名系统附加选项信息，以及包括密钥信息或者第二签名信息的第二附加选项信息，得到第二域名系统请求信息。

本步骤中，第二域名系统请求信息相比第一域名系统请求信息在第二附加选项信息中携带了密文敏感信息，因此，本申请实施例并未对整个第一域名系统请求信息进行加密处理，而是能够将敏感信息单独加密得到携带有密文敏感信息的第二域名系统请求信息以实现对敏感信息的保护，使得传输路径中的设备无需支持整个域名系统请求信息的加密和解密处理，从而减少了网络资源的开销，降低了设备的维护成本。

如图 16 所示，图 16 是图 12 中步骤 S126 的具体方法的流程图，图 16 对步骤 S126 进行进一步的说明，该步骤 S126 可以包括但不限于有步骤 S1261 和步骤 S1262。

步骤 S1261：根据本地敏感信息的信息长度确定第二加密策略信息，其中，第二加密策略信息包括第二密文长度。

本步骤中，通过本地敏感信息的信息长度确定第二加密策略信息。当本地敏感信息对应网际协议版本 4（Internet Protocol version 4，IPv4）地址，中间解析器能够通过检测本地敏感信息的信息长度确定远端敏感信息类型为网际协议版本 4 地址，并将第二加密策略信息配置为对应于网际协议版本 4 地址的第二加密策略信息。当本地敏感信息对应网际协议版本 6（Internet Protocol version 6，IPv4）地址，中间解析器能够通过检测本地敏感信息的信息长度确定远端敏感信息类型为网际协议版本 6 地址，并将第二加密策略信息配置为对应于网际协

议版本 6 地址的第二加密策略信息。

在一实施例中，第二加密策略信息除了包括第一密文长度，还包括对于本地敏感信息的加密方法，例如，当本地敏感信息对应于网际协议版本 4 地址，根据加密方法，首先从本地敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用哈希算法获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。

又如，当本地敏感信息对应于网际协议版本 6 地址，根据加密方法，将本地敏感信息视为一个整字符串进行加密，该过程所使用的加密算法包括但不限于 MD5 信息摘要算法，由于本地敏感信息为网际协议版本 6 地址，因此需要预留 128 位的地址空间。

再如，当本地敏感信息过长，根据加密方法，对本地敏感信息进行二次加密处理以缩减加密后的密文敏感信息的位数。

步骤 S1262：根据第二加密策略信息对本地敏感信息进行加密处理得到密文敏感信息，其中，密文敏感信息的信息长度与第一密文长度相匹配。

本步骤中，根据第二加密策略信息对本地敏感信息进行加密处理得到密文敏感信息，例如，当本地敏感信息对应网际协议版本 4 地址，第二加密策略信息则配置为对应于网际协议版本 4 地址的第二加密策略信息，具体地，首先从本地敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用哈希算法获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。

此外，当本地敏感信息对应网际协议版本 6 地址，第二加密策略信息则配置为对应于网际协议版本 6 地址的第二加密策略信息，将本地敏感信息视为一个整字符串进行加密，该过程所加密算法包括但不限于 MD5 信息摘要算法，由于本地敏感信息为网际协议版本 6 地址，因此需要预留 128 位的地址空间。

在一实施例中，第一域名系统请求信息基于本申请实施例的伪地址类型消息体构建，通过第一域名系统请求信息能够得知本地敏感信息的类型，例如，若本地敏感信息对应网际协议版本 4 地址，则将第二域名系统请求信息的 FAMILY 字段赋值为 1，若本地敏感信息对应网际协议版本 6 地址，则将第二域名系统请求信息的 FAMILY 字段赋值为 2。

在一实施例中，本地敏感信息的类型是通过第一域名系统请求信息的 FAMILY 字段确定的，例如，当第一域名系统请求信息的 FAMILY 字段赋值为 1，则本地敏感信息对应网际协议版本 4 地址，当第一域名系统请求信息的 FAMILY 字段赋值为 1，则本地敏感信息对应网际协议版本 6 地址。

如图 17 所示，图 17 是图 16 中步骤 S1262 的具体方法的流程图，图 17 对步骤 S1262 进行进一步的说明，该步骤 S1262 可以包括但不限于有步骤 S12621 和步骤 S12622。

步骤 S12621：根据第二加密策略信息对本地敏感信息进行第一加密处理得到第二密文信

息。

本步骤中，根据第二加密策略信息对本地敏感信息进行第一加密处理得到第二密文信息，第二密文信息可以是根据本地敏感信息得到的网际互连协议地址，例如，当本地敏感信息对应网际协议版本 4 地址，第二加密策略信息则配置为对应于网际协议版本 4 地址的第二加密策略信息，具体地，首先从本地敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址。又如，当本地敏感信息对应网际协议版本 6 地址，第二加密策略信息则配置为对应于网际协议版本 6 地址的第二加密策略信息，通过本地敏感信息进行第一加密处理得到 128 位的网际协议版本 6 地址。

步骤 S12622：根据第二加密策略信息对第二密文信息进行第二加密处理得到密文敏感信息，其中，密文敏感信息的信息长度小于第二密文信息的信息长度。

本步骤中，根据第二加密策略信息对第二密文信息进行第二加密处理得到密文敏感信息，例如，首先从本地敏感信息中提取网际协议版本 4 形式的域名字段，并将其通过字符串转换函数转换成整实数，并可以通过数值限制将转换后的整数限制在 0~15 之间，由于经过加密后的伪地址也是网际协议版本 4 地址，因此需要预留 32 位的地址空间，将转换后的整实数再转换为 4 个四位的二进制数，余下地址空间补零，再从头每次取 8 位二进制数转换为十进制数，以得到网际协议版本 4 地址，再采用第二加密处理获得该网际协议版本 4 地址所对应的伪地址，以实现对于敏感信息的加密。由于地址位数限制，若网际协议版本 4 地址经过一次第二加密处理后仍超过 32 位，则再次进行至少一次第二加密处理，以防止加密处理后得到的密文敏感信息的信息长度大于第二密文的信息长度而导致信息丢失。

又如，当本地敏感信息对应网际协议版本 6 地址，第二加密策略信息则配置为对应于网际协议版本 6 地址的第二加密策略信息，将本地敏感信息视为一个整字符串进行加密，该过程所使用的加密算法包括但不限于，由于本地敏感信息对应网际协议版本 6 地址，因此需要预留 128 位的地址空间。若本地敏感信息经过第一加密处理后获得的网际协议版本 6 地址经过一次第二加密处理后信息长度仍超过 128 位，则再次进行至少一次第二加密处理，以防止加密处理后得到的密文敏感信息的信息长度大于第二密文的信息长度而导致信息丢失。

在一实施例中，第二加密处理采用的算法包括但不限于哈希算法或 MD5 信息摘要算法。

在一实施例中，对密文敏感信息进行加密后，根据对敏感信息进行加密所使用的加密算法类型设置 ECRYPTION TYPE 字段。例如，当敏感信息未经加密，则 ECRYPTION TYPE 字段赋值为 0，当采用 MD5 信息摘要算法对敏感信息进行加密，则 ECRYPTION TYPE 字段赋值为 1，当使用使用安全散列算法 1（Secure Hash Algorithm 1，SHA-1）则 ECRYPTION TYPE 字段赋值为 2。

如图 18 所示，图 18 是本申请另一个实施例提供的信息处理方法的流程图，参照图 18，该信息处理方法还可以包括但不限于有步骤 S140 和步骤 S150。

步骤 S140：接收权威域名系统服务器根据密文敏感信息和第一密文标记信息发送的反馈信息，其中，反馈信息包括反馈类型信息和第二密文标记信息。

本步骤中，权威域名系统服务器接收到第二域名系统请求信息后，根据第二域名系统请

求信息生成反馈信息，并向客户端设备发送该反馈信息，反馈信息用于使客户端设备得到所需的域名与网际互连协议地址的对应关系，此外，反馈信息还用于使得中间解析器或客户端设备获知权威域名系统服务器是否成功解密第二域系统名请求信息中的密文敏感信息。

在一实施例中，反馈信息是根据本申请实施例中的PADR消息体结合类型构建的。

在一实施例中，反馈信息也包括有扩展域名系统子网选项信息。

步骤S150：根据反馈类型信息和第二密文标记信息进行信息处理。

本步骤中，中间解析器根据反馈信息所携带的反馈类型信息和第二密文标记信息进行信息处理，使得中间解析器能够根据权威域名系统服务器的处理情况做进一步的处理。

如图19所示，图19是图18中步骤S150的具体方法的流程图，图19对步骤S150进行进一步的说明，该步骤S150可以包括但不限于有步骤S151和步骤S152。

步骤S151：当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器无法解密密文敏感信息，根据第一域名系统请求信息重构第三域名系统请求信息，其中，第三域名系统请求信息不包括密文敏感信息。

本步骤中，当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，则权威域名系统服务器亦无法对密文敏感信息进行解密，因此中间解析器根据第一域名系统请求信息重构第三域名系统请求信息，该第三域名系统请求信息不包括密文敏感信息。当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，例如对应的权威域名系统服务器不支持扩展域名系统客户端子网选项或对应的权威域名系统服务器没有预先配置相应的解密算法或该权威域名系统服务器失效，则重构第三域名系统请求信息，并将该第三域名系统请求信息发送至权威域名系统服务器，以对于该权威域名系统服务器的可用性进行检测。

在一实施例中，反馈信息使用了本申请实施例中的伪地址类型消息体结构，因此通过检验反馈信息中的ECRYPTION FLAG字段能够确定权威域名系统服务器是否能够识别第二域名系统请求信息以及是否能够对第二域名系统请求信息中的密文敏感信息进行解密。

具体的，当反馈信息的ECRYPTION FLAG字段中的FLAG标志位为0，则表示权威域名系统服务器不能识别第二域名系统请求信息，也无法对第二域名系统请求信息中的密文敏感信息进行解密。

在一实施例中，当检测到当前选择的权威域名系统服务器失效，则选择新的权威域名系统服务器。

需要说明的是，第三域名系统请求信息可以携带也可以不携带第二附加选项信息和/或第一扩展域名系统附加选项信息，本实施例对此不做具体限定。

需要说明的是，第三域名系统请求信息可以携带也可以不携带第二附加选项信息和/或第二扩展域名系统附加选项信息，本实施例对此不做具体限定。

步骤S152：将第三域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据第三域名系统请求信息进行信息处理。

本步骤中，中间解析器将第三域名系统请求信息发送至权威域名系统服务器，使得权威域名系统服务器根据第三域名系统请求信息进行信息处理。

如图20所示，图20是图18中步骤S150的另一具体方法的流程图，图20对步骤S150进行进一步的说明，该步骤S150可以包括但不限于有步骤S153和步骤S154。

步骤 S153：当反馈类型信息表示权威域名系统服务器正常识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器没有解密密文敏感信息，根据第一域名系统请求信息重构第四域名系统请求信息，其中，第四域名系统请求信息包括密文敏感信息对应的明文敏感信息。

本步骤中，当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，则权威域名系统服务器亦无法对密文敏感信息进行解密，因此中间解析器根据第一域名系统请求信息重构第四域名系统请求信息，该第四域名系统包括密文敏感信息对应的明文敏感信息。当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，例如对应的权威域名系统服务器不支持扩展域名系统客户端子网选项或对应的权威域名系统服务器没有预先配置相应的解密算法，则重构使用明文记载敏感信息的第四域名系统请求信息，并将该第四域名系统请求信息发送至权威域名系统服务器，以提高兼容性。

在一实施例中，反馈信息使用了本申请实施例中的伪地址类型消息体结构，因此通过检验反馈信息中的 ECRYPTION FLAG 字段能够确定权威域名系统服务器是否能够识别第二域名系统请求信息以及是否能够对第二域名系统请求信息中的密文敏感信息进行解密。

具体的，当反馈信息的 ECRYPTION FLAG 字段中的 FLAG 标志位为 2，则表示权威域名系统服务器能够识别第二域名系统请求信息，但无法对第二域名系统请求信息中的密文敏感信息进行解密。

需要说明的是，第四域名系统请求信息可以携带也可以不携带第二附加选项信息和/或第一扩展域名系统附加选项信息，本实施例对此不做具体限定。

需要说明的是，第四域名系统请求信息可以携带也可以不携带第二附加选项信息和/或第二扩展域名系统附加选项信息，本实施例对此不做具体限定。

步骤 S154：将第四域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据明文敏感信息进行信息处理。

本步骤中，中间解析器将第四域名系统请求信息发送至权威域名系统服务器，使得权威域名系统服务器根据第四域名系统请求信息携带的明文敏感信息进行信息处理。

在一实施例中，反馈信息还包括目标网际互连协议地址，目标网际互连协议地址是第一域名系统请求信息对应的网际互连协议地址。

如图 21 所示，图 21 是图 18 中步骤 S150 的另一具体方法的流程图，图 21 对步骤 S150 进行进一步的说明，该步骤 S150 可以包括但不限于有步骤 S155 和步骤 S156。

步骤 S155：当反馈类型信息表示权威域名系统服务器正常识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器正确解密密文敏感信息，缓存第一域名系统请求信息与目标网际互连协议地址之间的映射关系。

本步骤中，当反馈类型信息表示权威域名系统服务器正常识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器正确解密密文敏感信息，因此证明权威域名系统服务器能够正常识别第二域名系统请求信息，并对第二域名系统请求信息中的密文敏感信息进行解密，通过将第一域名系统请求信息与目标网际互连协议地址之间的映射关系缓存在中间解析器，能够提高客户端设备获取第一域名系统请求信息与目标网际互连协议地址之间的映射关系的效率，减少了系统调度的复杂性。

在一实施例中，反馈信息使用了本申请实施例中的伪地址类型消息体结构，因此通过检

验反馈信息中的ECRYPTION FLAG字段能够确定权威域名系统服务器是否能够识别第二域名系统请求信息以及是否能够对第二域名系统请求信息中的密文敏感信息进行解密。

具体的，当反馈信息的ECRYPTION FLAG字段中的FLAG标志位为1，则表示权威域名系统服务器能够识别第二域名系统请求信息，且能够对密文敏感信息进行解密。

步骤S156：将反馈信息转发回第一域名系统请求信息的发起方。

本步骤中，反馈信息包括第一域名系统请求信息对应的网际互连协议地址，通过将反馈信息转发回第一域名系统请求信息的发起方，能够使得第一第一域名系统请求信息的发起方获得第一域名系统请求信息与目标网际互连协议地址之间的映射关系。此外，反馈信息可以是经过加密的，也可以是未经加密的，本实施例对此不做具体限定。

需要说明的是，第一域名系统请求信息的发起方可以是客户端设备，也可以是中间解析器，本实施例对此不做具体限定。

为了更加清楚的说明本申请实施例提供的信息处理方法的处理流程，下面以具体的示例进行说明。

如图22所示，图22是本申请一个具体示例提供的信息处理方法的流程图。该信息处理方法应用于，该信息处理方法包括以下步骤：

步骤S101：接收第一域名系统请求信息；

步骤S102a：提取第一域名系统请求信息中的域名字段并查找本地DNS缓存是否存在对应的解析记录，当本地DNS缓存中有相应的解析记录，根据解析记录构造DNS响应信息并发送至用户端设备；

步骤S102b：当本地DNS缓存中没有对应的解析记录，获取敏感信息；

步骤S103：根据敏感信息的长短选择加密算法对敏感信息进行加密，得到密文敏感信息；

步骤S104：根据密文敏感信息以eDNS0格式重构第一域名系统请求信息得到第二域名系统请求信息；

步骤S105：将第二域名系统请求信息封装成UDP包后发送至权威域名系统服务器；

步骤S106：从权威域名系统服务器接收反馈信息，检查反馈信息中的RCODE字段，当RCODE的字段返回代码是0，检查PADR字段中的ENCRYPTION FLAG字段；

步骤S107a：当ENCRYPTION FLAG字段的字段返回代码是0，以未加密的敏感信息进行RDATA字段的填写以构造第三域名系统请求信息并发送至权威域名系统服务器；

步骤S107b：当ENCRYPTION FLAG字段的字段返回代码是1，检查反馈信息的其它字段。

步骤S108：在反馈信息的所有字段正常的情况下，将反馈信息中的域名映射关系记录到本地DNS缓存中，并将域名映射关系转发回客户端设备。

需要说明的是，步骤S103根据敏感信息的长短选择加密算法的具体方法包括：在敏感信息的目标是映射为较短的IPv4地址的情况下，预留32位的地址空间，并且每4位对应一个整数。将敏感信息以字符串转换函数转换为整实数，将转换后的整实数再转换为4个四位的二进制数，余下地址空间补零，再从头每次取8位二进制数转换为十进制数，以得到IPv4地址。在以eDNS0格式重构第二域名系统请求信息的过程中，将TTL元素中的EXTENDED-RCODE字段设置为0x1，表示该域名系统请求信息携带有密文敏感信息。RDATA字段中的OPTION-CODE字段设置为27000，OPTION-LENGTH字段设置为36，FAMILY字

段设置为 1，表示后续将使用 IPv4 地址格式；ENCRYPTION TYPE 字段设置为 2，表示使用 crc32（），bese_convert（）的加密机制；ENCRYPTION FLAG 字段设置为 0，用于 DNS 请求消息中，代表本消息存在加密的伪地址，并且默认远端的 DNS 权威服务器不能识别本消息；SIGNATURE 字段中填入加密后的密文敏感信息或加密过程中使用的密钥。另外，还可以将加密后得到的伪地址填写入扩展域名系统客户端子网选项信息的 ADDRESS 字段中。

需要说明的是，步骤 S103 根据敏感信息的长短选择加密算法的具体方法还包括：在敏感信息的目标是映射为较长的 IPv6 地址的情况下，预留 128 位的地址空间。将敏感信息以 MD5 方式转换成一个 128 位的字符串，每 4 个位对应一个字符获得 IPv6 地址。在以 eDNS0 格式重构第二域名系统请求信息的过程中，将 TTL 元素中的 EXTENDED-RCODE 字段设置为 0x1，表示该域名系统请求信息携带有密文敏感信息。RDATA 字段中的 OPTION-CODE 字段设置为 27000，OPTION-LENGTH 字段设置为 132，FAMILY 字段设置为 2，表示后续将使用 IPv6 地址格式；ENCRYPTION TYPE 字段设置为 1；ENCRYPTION FLAG 字段设置为 0，用于 DNS 请求消息中，代表本消息存在加密的伪地址，并且默认远端的 DNS 权威服务器不能识别本消息；SIGNATURE 字段中填入加密后的密文敏感信息或加密过程中使用的密钥。另外，还可以将加密后得到的伪地址填写入扩展域名系统客户端子网选项信息的 ADDRESS 字段中。

另外，本申请的一个实施例还提供了一种中间解析器，该中间解析器包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序。

处理器和存储器可以通过总线或者其他方式连接。

存储器作为一种非暂态计算机可读存储介质，可用于存储非暂态软件程序以及非暂态性计算机可执行程序。此外，存储器可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施方式中，存储器可选包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至该处理器。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

需要说明的是，本实施例中的中间解析器，可以应用至例如图 1 所示实施例中的中间解析器 120，本实施例中的中间解析器能够构成例如图 1 所示实施例中的系统架构的一部分，这些实施例均属于相同的发明构思，因此这些实施例具有相同的实现原理以及技术效果，此处不再详述。

实现上述实施例的信息处理方法所需的非暂态软件程序以及指令存储在存储器中，当被处理器执行时，执行上述实施例中的信息处理方法，例如，执行以上描述的图 2 中的方法步骤 S110 至 S130、图 6 中的方法步骤 S121 至 S124、图 7 中的方法步骤 S1241 至 S1242、图 8 中的方法步骤 S1243 至 S1244、图 9 中的方法步骤 S12441 至 S12442、图 10 中的方法步骤 S1221 至 S1222、图 11 中的方法步骤 S12221 至 S12222、图 12 中的方法步骤 S125 至 S128、图 13 中的方法步骤 S1281 至 S1282、图 14 中的方法步骤 S1283 至 S1284、图 15 中的方法步骤 S12841 至 S12842、图 16 中的方法步骤 S1261 至 S1262、图 17 中的方法步骤 S12621 至 S12622、图 18 中的方法步骤 S140 至 S150、图 19 中的方法步骤 S151 至 S152、图 20 中的方法步骤 S153 至 S154、图 21 中的方法步骤 S155 至 S156 或者如图 22 中示出的方法步骤 S101 至 S108。

另外，本申请的一个实施例还提供了一种网络设备，该网络设备包括有上述实施例的中间解析器，因此本实施例中的网络设备与上述实施例中的中间解析器属于相同的发明构思，因此这些实施例具有相同的实现原理以及技术效果，此处不再详述。

以上所描述的装置实施例或者系统实施例仅仅是示意性的，其中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，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模块来实现本实施例方案的目的。

此外，本申请的一个实施例还提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机可执行指令，该计算机可执行指令被一个处理器或控制器执行，例如，被上述装置实施例中的一个处理器执行，可使得上述处理器执行上述实施例中的信息处理方法，例如，执行以上描述的图 2 中的方法步骤 S110 至 S130、图 6 中的方法步骤 S121 至 S124、图 7 中的方法步骤 S1241 至 S1242、图 8 中的方法步骤 S1243 至 S1244、图 9 中的方法步骤 S12441 至 S12442、图 10 中的方法步骤 S1221 至 S1222、图 11 中的方法步骤 S12221 至 S12222、图 12 中的方法步骤 S125 至 S128、图 13 中的方法步骤 S1281 至 S1282、图 14 中的方法步骤 S1283 至 S1284、图 15 中的方法步骤 S12841 至 S12842、图 16 中的方法步骤 S1261 至 S1262、图 17 中的方法步骤 S12621 至 S12622、图 18 中的方法步骤 S140 至 S150、图 19 中的方法步骤 S151 至 S152、图 20 中的方法步骤 S153 至 S154、图 21 中的方法步骤 S155 至 S156 或者如图 22 中示出的方法步骤 S101 至 S108。

本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统可以被实施为软件、固件、硬件及其适当的组合。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质（或非暂时性介质）和通信介质（或暂时性介质）。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

以上是对本申请的较佳实施进行了具体说明，但本申请并不局限于上述实施方式，熟悉本领域的技术人员在不违背本申请本质的前提下还可作出种种的等同变形或替换，这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

# 权 利 要 求 书

1. 一种信息处理方法，应用于中间解析器，所述方法包括：

接收第一域名系统请求信息；

根据所述第一域名系统请求信息得到第二域名系统请求信息，其中，所述第二域名系统请求信息包括密文敏感信息和第一密文标记信息，所述第一密文标记信息用于指示所述密文敏感信息为密文信息；

将所述第二域名系统请求信息发送给权威域名系统服务器，使得所述权威域名系统服务器根据所述密文敏感信息和所述第一密文标记信息进行信息处理。

2. 根据权利要求 1 所述的方法，其中，所述第一域名系统请求信息包括第一扩展域名系统附加选项信息，其中，所述第一扩展域名系统附加选项信息包括源端敏感信息；

所述根据所述第一域名系统请求信息得到第二域名系统请求信息，包括：

获取所述第一扩展域名系统附加选项信息中的所述源端敏感信息；

对所述源端敏感信息进行加密处理得到所述密文敏感信息；

构建第一附加选项信息，其中，所述第一附加选项信息包括所述第一密文标记信息；

根据所述密文敏感信息和所述第一附加选项信息得到第二域名系统请求信息。

3. 根据权利要求 2 所述的方法，其中，所述第一附加选项信息包括第一加密签名字段；

所述根据所述密文敏感信息和所述第一附加选项信息得到第二域名系统请求信息，包括：

将所述密文敏感信息填充进所述第一加密签名字段；

根据包括所述第一密文标记信息和所述密文敏感信息的所述第一附加选项信息，得到第二域名系统请求信息。

4. 根据权利要求 2 所述的方法，其中，所述根据所述密文敏感信息和所述第一附加选项信息得到第二域名系统请求信息，包括：

将所述第一扩展域名系统附加选项信息中的所述源端敏感信息更新为所述密文敏感信息；

根据更新后的所述第一扩展域名系统附加选项信息和所述第一附加选项信息得到第二域名系统请求信息。

5. 根据权利要求 4 所述的方法，其中，所述第一附加选项信息包括第一加密签名字段；

所述根据更新后的所述第一扩展域名系统附加选项信息和所述第一附加选项信息得到第二域名系统请求信息，包括：

在所述第一加密签名字段中填充密钥信息或者第一签名信息，其中，所述密钥信息用于解密所述密文敏感信息，所述第一签名信息用于验证加密后的所述源端敏感信息的完整性；

根据更新后的所述第一扩展域名系统附加选项信息，以及包括所述密钥信息或者所述第一签名信息的所述第一附加选项信息，得到第二域名系统请求信息。

6. 根据权利要求 2 所述的方法，其中，所述对所述源端敏感信息进行加密处理得到所述密文敏感信息，包括：

根据所述源端敏感信息的信息长度确定第一加密策略信息，其中，所述第一加密策略信息包括第一密文长度；

根据所述第一加密策略信息对所述源端敏感信息进行加密处理得到所述密文敏感信息，

其中，所述密文敏感信息的信息长度与所述第一密文长度相匹配。

7. 根据权利要求 6 所述的方法，其中，所述根据所述第一加密策略信息对所述源端敏感信息进行加密处理得到所述密文敏感信息，包括：

根据所述第一加密策略信息对所述源端敏感信息进行第一加密处理得到第一密文信息；

根据所述第一加密策略信息对所述第一密文信息进行第二加密处理得到所述密文敏感信息，其中，所述密文敏感信息的信息长度小于所述第一密文信息的信息长度。

8. 根据权利要求 1 所述的方法，其中，所述第一域名系统请求信息不包括第一扩展域名系统附加选项信息；

所述根据所述第一域名系统请求信息得到第二域名系统请求信息，包括：

根据所述第一域名系统请求信息获取本地敏感信息；

对所述本地敏感信息进行加密处理得到所述密文敏感信息；

构建第二附加选项信息，其中，所述第二附加选项信息包括所述第一密文标记信息；

根据所述密文敏感信息和所述第二附加选项信息得到第二域名系统请求信息。

9. 根据权利要求 8 所述的方法，其中，所述第二附加选项信息包括第二加密签名字段；

所述根据所述密文敏感信息和所述第二附加选项信息得到第二域名系统请求信息，包括：

将所述密文敏感信息填充进所述第二加密签名字段；

根据包括所述第一密文标记信息和所述密文敏感信息的所述第二附加选项信息，得到第二域名系统请求信息。

10. 根据权利要求 8 所述的方法，其中，所述根据所述密文敏感信息和所述第二附加选项信息得到第二域名系统请求信息，包括：

根据所述密文敏感信息构建第二扩展域名系统附加选项信息，其中，所述第二扩展域名系统附加选项信息包括所述密文敏感信息；

根据所述第二扩展域名系统附加选项信息和所述第二附加选项信息得到第二域名系统请求信息。

11. 根据权利要求 10 所述的方法，其中，所述第二附加选项信息包括第二加密签名字段；

所述根据所述第二扩展域名系统附加选项信息和所述第二附加选项信息得到第二域名系统请求信息，包括：

在所述第二加密签名字段中填充密钥信息或者第二签名信息，其中，所述密钥信息用于解密所述密文敏感信息，所述第二签名信息用于验证加密后的所述本地敏感信息的完整性；

根据所述第二扩展域名系统附加选项信息，以及包括所述密钥信息或者所述第二签名信息的所述第二附加选项信息，得到第二域名系统请求信息。

12. 根据权利要求 8 所述的方法，其中，所述对所述本地敏感信息进行加密处理得到所述密文敏感信息，包括：

根据所述本地敏感信息的信息长度确定第二加密策略信息，其中，所述第二加密策略信息包括第二密文长度；

根据所述第二加密策略信息对所述本地敏感信息进行加密处理得到所述密文敏感信息，其中，所述密文敏感信息的信息长度与所述第二密文长度相匹配。

13. 根据权利要求 12 所述的方法，其中，所述根据所述第二加密策略信息对所述本地敏感信息进行加密处理得到所述密文敏感信息，包括：

根据所述第二加密策略信息对所述本地敏感信息进行第一加密处理得到第二密文信息；

根据所述第二加密策略信息对所述第二密文信息进行第二加密处理得到所述密文敏感信息，其中，所述密文敏感信息的信息长度小于所述第二密文信息的信息长度。

14. 根据权利要求 1 至 13 任意一项所述的方法，其中，所述将所述第二域名系统请求信息发送给权威域名系统服务器之后，所述方法还包括：

接收所述权威域名系统服务器根据所述密文敏感信息和所述第一密文标记信息发送的反馈信息，其中，所述反馈信息包括反馈类型信息和第二密文标记信息；

根据所述反馈类型信息和所述第二密文标记信息进行信息处理。

15. 根据权利要求 14 所述的方法，其中，所述根据所述反馈类型信息和所述第二密文标记信息进行信息处理，包括：

当所述反馈类型信息表示所述权威域名系统服务器无法识别所述第二域名系统请求信息，并且所述第二密文标记信息表示所述权威域名系统服务器无法解密所述密文敏感信息，根据所述第一域名系统请求信息重构第三域名系统请求信息，其中，所述第三域名系统请求信息不包括所述密文敏感信息；

将所述第三域名系统请求信息发送给所述权威域名系统服务器，使得所述权威域名系统服务器根据所述第三域名系统请求信息进行信息处理。

16. 根据权利要求 14 所述的方法，其中，所述根据所述反馈类型信息和所述第二密文标记信息进行信息处理，包括：

当所述反馈类型信息表示所述权威域名系统服务器正常识别所述第二域名系统请求信息，并且所述第二密文标记信息表示所述权威域名系统服务器没有解密所述密文敏感信息，根据所述第一域名系统请求信息重构第四域名系统请求信息，其中，所述第四域名系统请求信息包括所述密文敏感信息对应的明文敏感信息；

将所述第四域名系统请求信息发送给所述权威域名系统服务器，使得所述权威域名系统服务器根据所述明文敏感信息进行信息处理。

17. 根据权利要求 14 所述的方法，其中，所述反馈信息还包括目标网际互连协议地址；所述根据所述反馈类型信息和所述第二密文标记信息进行信息处理，包括：

当所述反馈类型信息表示所述权威域名系统服务器正常识别所述第二域名系统请求信息，并且所述第二密文标记信息表示所述权威域名系统服务器正确解密所述密文敏感信息，缓存所述第一域名系统请求信息与所述目标网际互连协议地址之间的映射关系；

将所述反馈信息转发回所述第一域名系统请求信息的发起方。

18. 一种中间解析器，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如权利要求 1 至 17 任意一项所述的信息处理方法。

19. 一种网络设备，包括有如权利要求 18 所述的中间解析器。

20. 一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于执行权利要求 1 至 17 任意一项所述的信息处理方法。

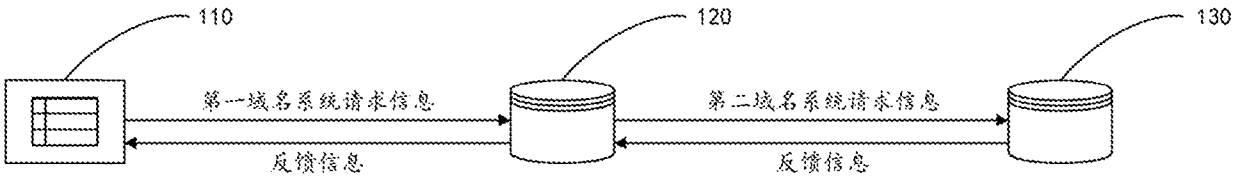
110
120
130
第一域名系统请求信息
反馈信息
第二域名系统请求信息
反馈信息

图 1

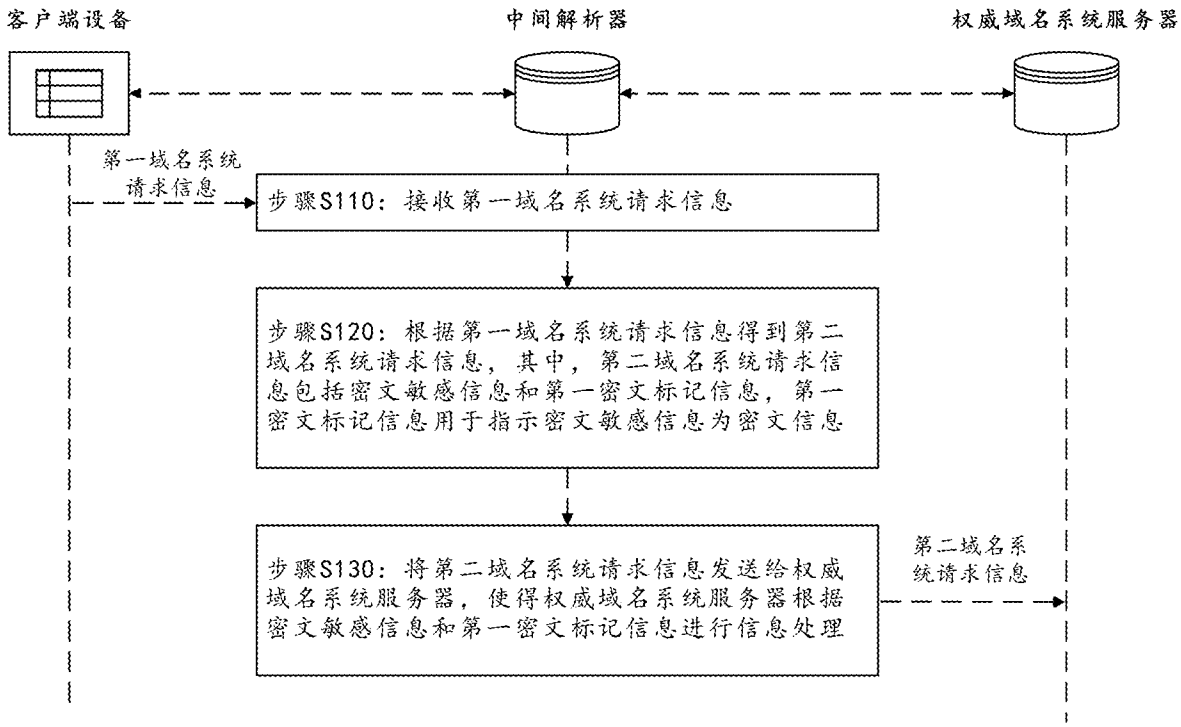
客户端设备
中间解析器
权威域名系统服务器
第一域名系统请求信息
步骤S110：接收第一域名系统请求信息
步骤S120：根据第一域名系统请求信息得到第二域名系统请求信息，其中，第二域名系统请求信息包括密文敏感信息和第一密文标记信息，第一密文标记信息用于指示密文敏感信息为密文信息
步骤S130：将第二域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据密文敏感信息和第一密文标记信息进行信息处理
第二域名系统请求信息

图 2

| EXTENDED-RCODE | VERSION |
| --- | --- |
| DO | Z |

图 3

| OPTION-CODE |
| --- |
| OPTION-LENGTH |
| OPTION-DATA |

图 4

| OPTION-CODE | |
| --- | --- |
| OPTION-LENGTH | |
| FAMILY | |
| ENCRYPTION TYPE | ENCRYPTION FLAG |
| SIGNATURE | |

图 5

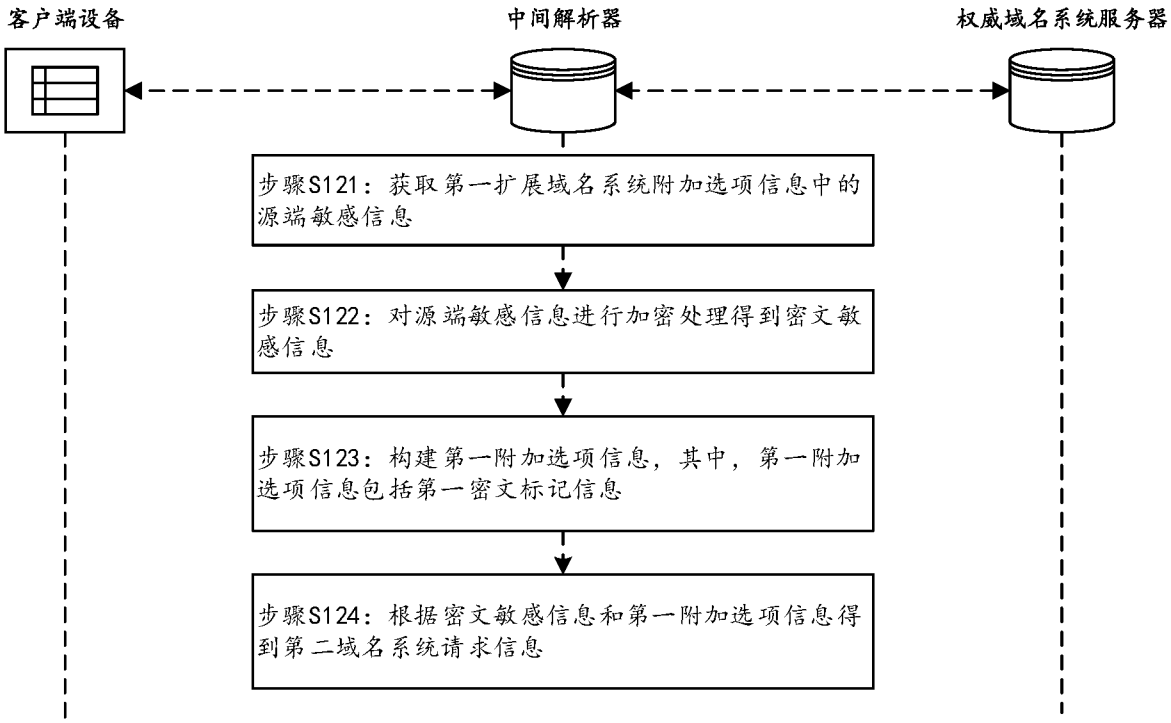
客户端设备
中间解析器
权威域名系统服务器
步骤S121：获取第一扩展域名系统附加选项信息中的源端敏感信息
步骤S122：对源端敏感信息进行加密处理得到密文敏感信息
步骤S123：构建第一附加选项信息，其中，第一附加选项信息包括第一密文标记信息
步骤S124：根据密文敏感信息和第一附加选项信息得到第二域名系统请求信息

图 6

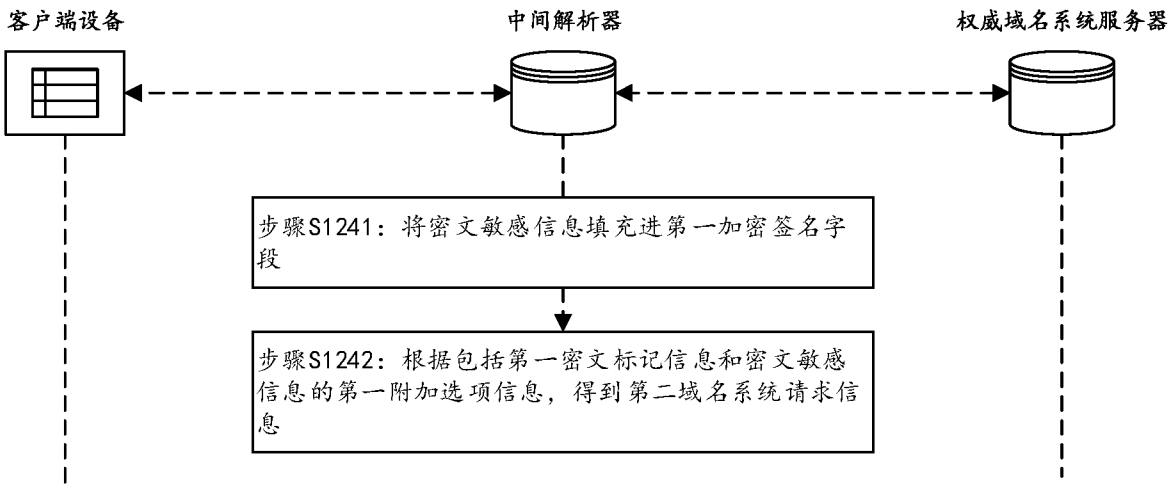
客户端设备
中间解析器
权威域名系统服务器
步骤S1241：将密文敏感信息填充进第一加密签名字段
步骤S1242：根据包括第一密文标记信息和密文敏感信息的第一附加选项信息，得到第二域名系统请求信息

图 7

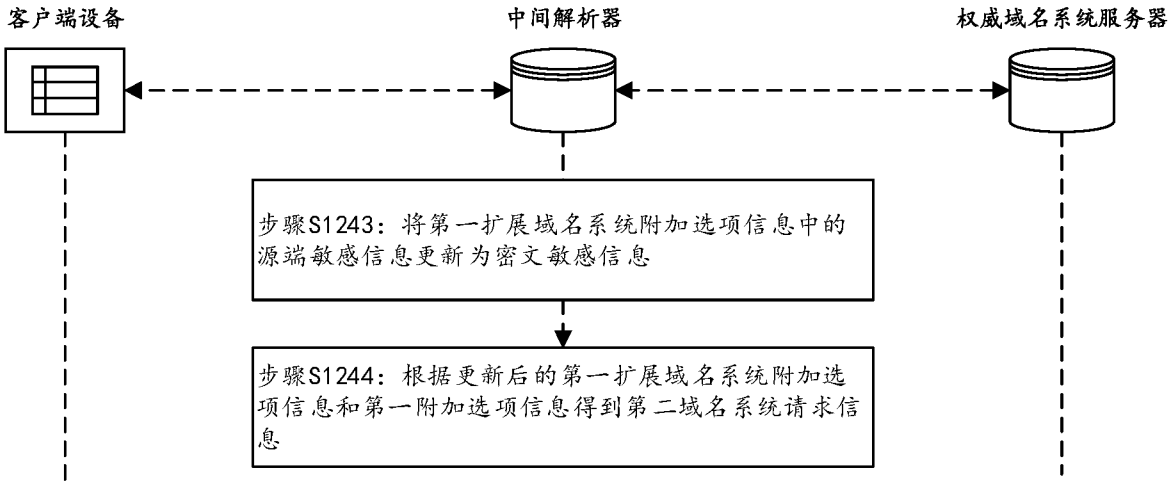
客户端设备
中间解析器
权威域名系统服务器
步骤S1243：将第一扩展域名系统附加选项信息中的源端敏感信息更新为密文敏感信息
步骤S1244：根据更新后的第一扩展域名系统附加选项信息和第一附加选项信息得到第二域名系统请求信息

图 8

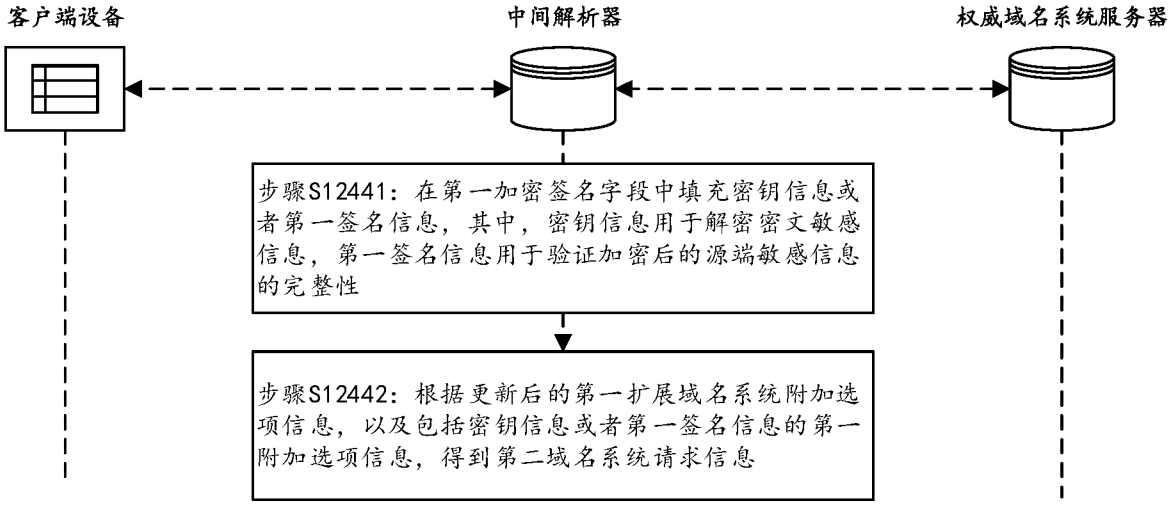
客户端设备
中间解析器
权威域名系统服务器
步骤S12441：在第一加密签名字段中填充密钥信息或者第一签名信息，其中，密钥信息用于解密密文敏感信息，第一签名信息用于验证加密后的源端敏感信息的完整性
步骤S12442：根据更新后的第一扩展域名系统附加选项信息，以及包括密钥信息或者第一签名信息的第一附加选项信息，得到第二域名系统请求信息

图 9

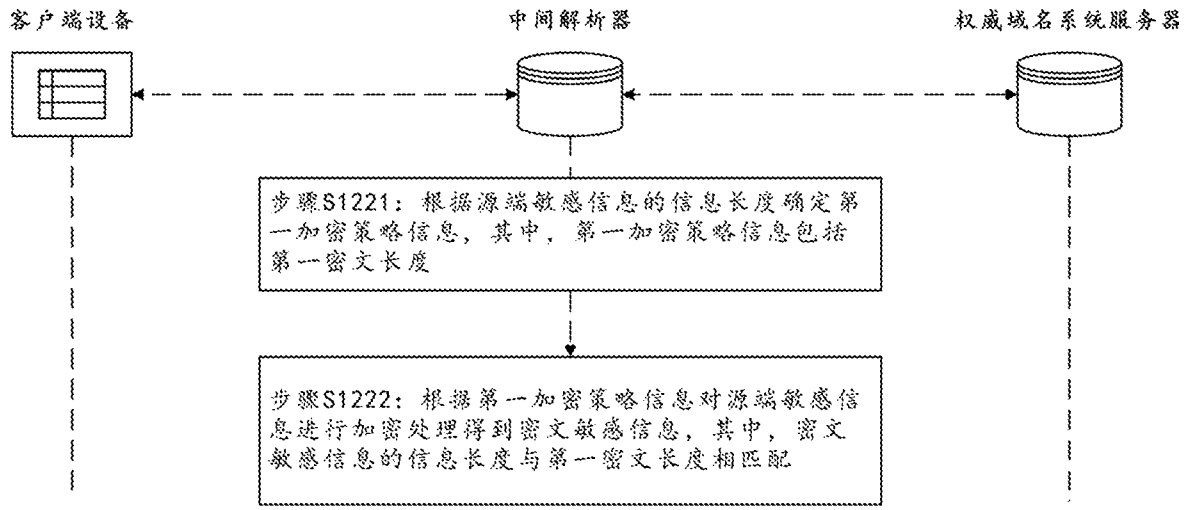
客户端设备
中间解析器
权威域名系统服务器
步骤S1221：根据源端敏感信息的信息长度确定第一加密策略信息，其中，第一加密策略信息包括第一密文长度
步骤S1222：根据第一加密策略信息对源端敏感信息进行加密处理得到密文敏感信息，其中，密文敏感信息的信息长度与第一密文长度相匹配

图 10

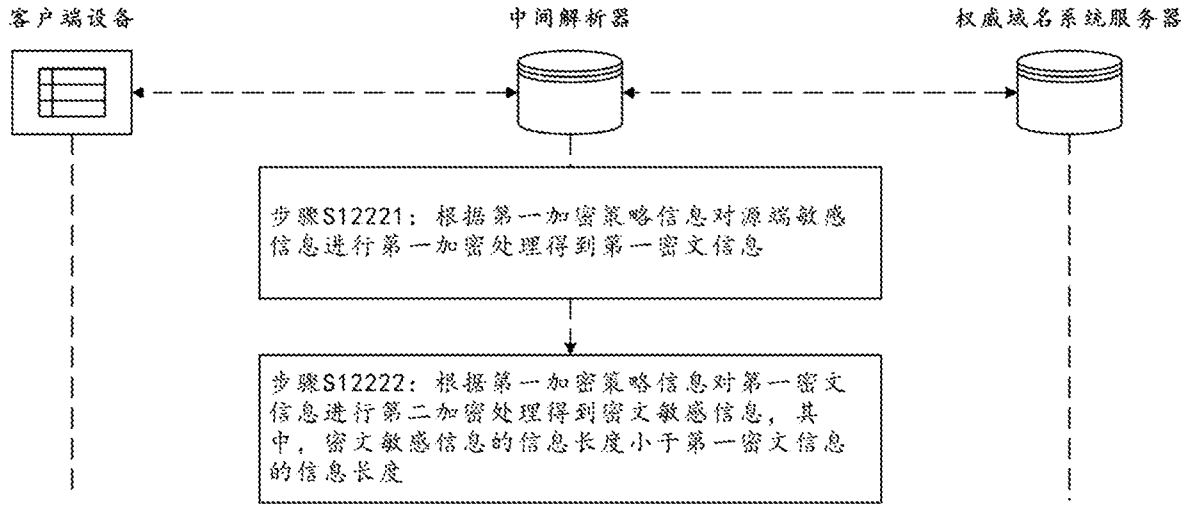
客户端设备
中间解析器
权威域名系统服务器
步骤S12221：根据第一加密策略信息对源端敏感信息进行第一加密处理得到第一密文信息
步骤S12222：根据第一加密策略信息对第一密文信息进行第二加密处理得到密文敏感信息，其中，密文敏感信息的信息长度小于第一密文信息的信息长度

图 11

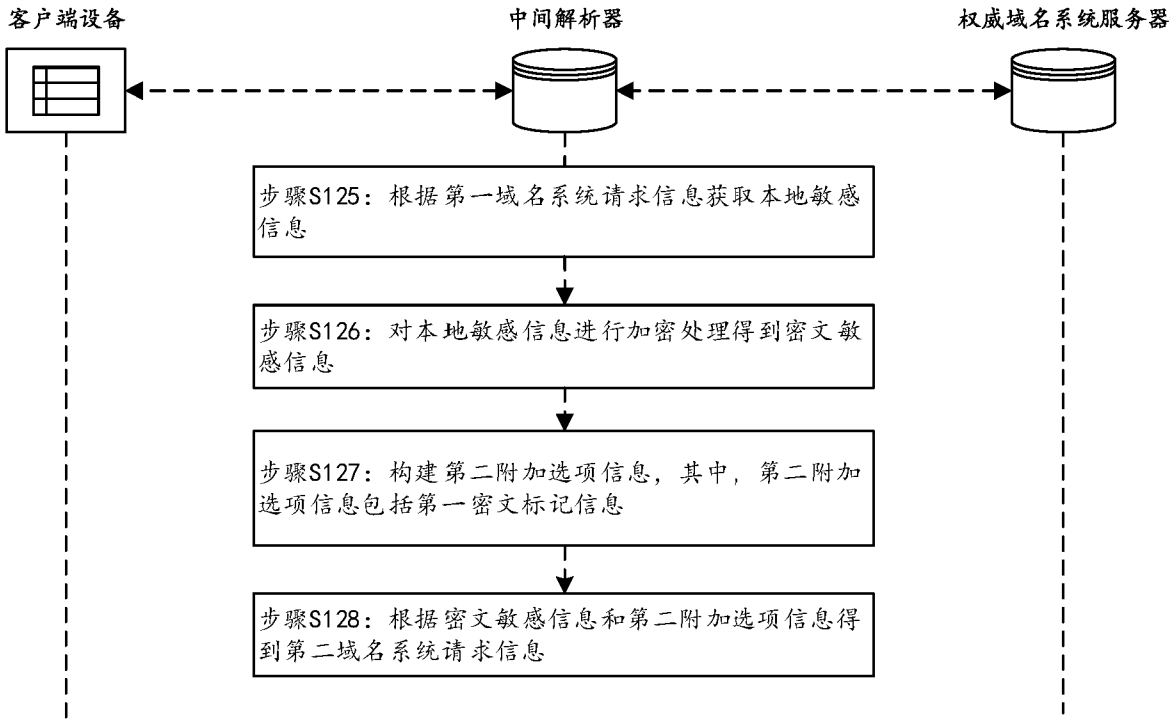
客户端设备
中间解析器
权威域名系统服务器
步骤S125：根据第一域名系统请求信息获取本地敏感信息
步骤S126：对本地敏感信息进行加密处理得到密文敏感信息
步骤S127：构建第二附加选项信息，其中，第二附加选项信息包括第一密文标记信息
步骤S128：根据密文敏感信息和第二附加选项信息得到第二域名系统请求信息

图 12

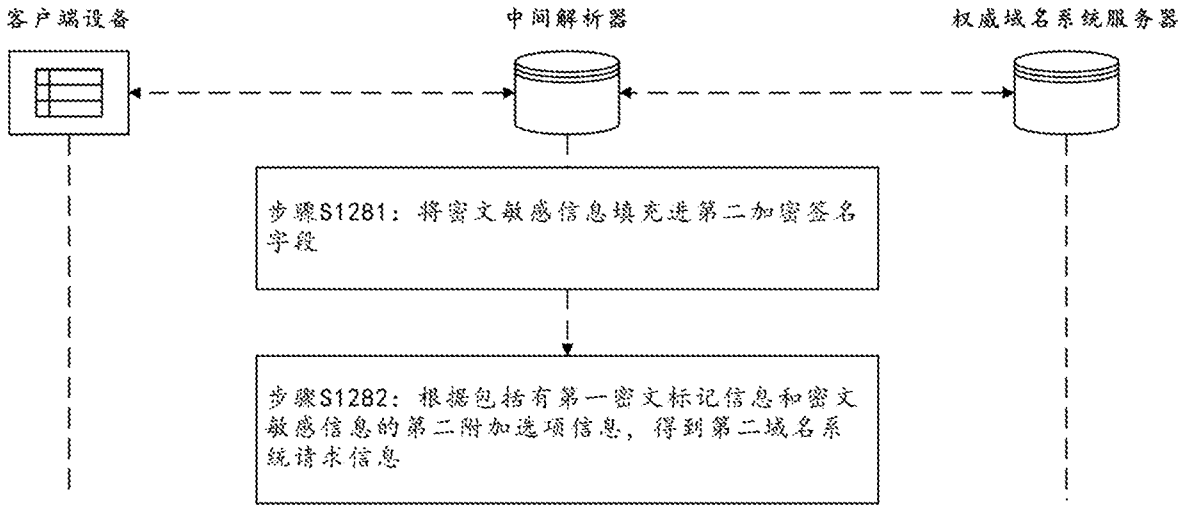
客户端设备
中间解析器
权威域名系统服务器
步骤S1281：将密文敏感信息填充进第二加密签名字段
步骤S1282：根据包括有第一密文标记信息和密文敏感信息的第二附加选项信息，得到第二域名系统请求信息

图 13

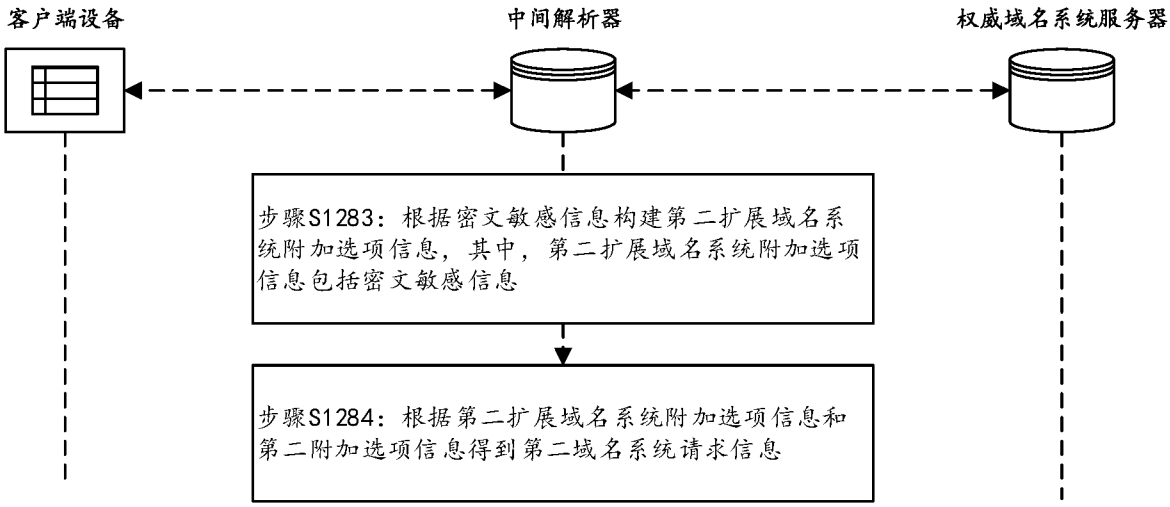
客户端设备
中间解析器
权威域名系统服务器
步骤S1283：根据密文敏感信息构建第二扩展域名系统附加选项信息，其中，第二扩展域名系统附加选项信息包括密文敏感信息
步骤S1284：根据第二扩展域名系统附加选项信息和第二附加选项信息得到第二域名系统请求信息

图 14

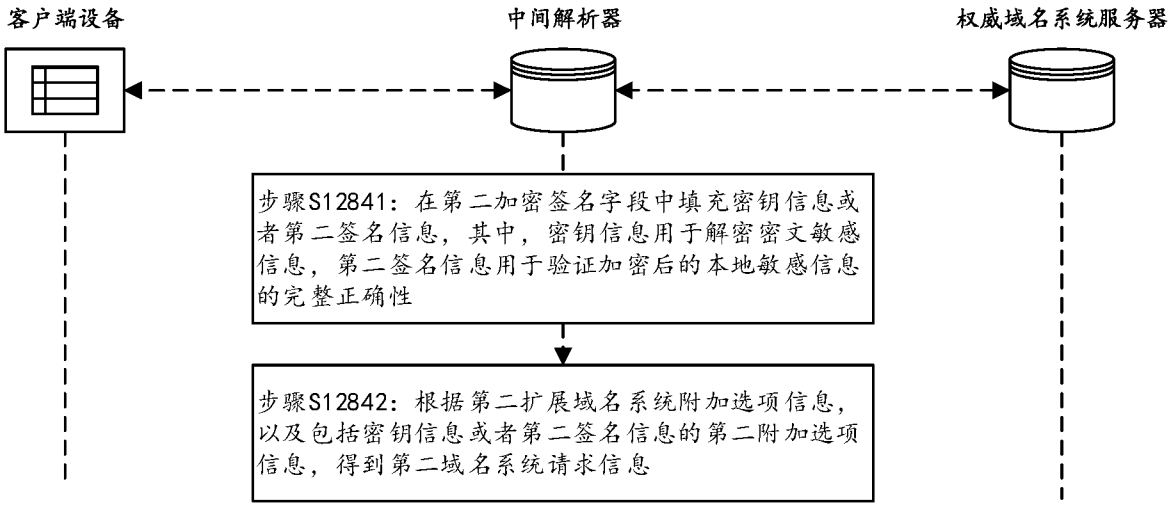
客户端设备
中间解析器
权威域名系统服务器
步骤S12841：在第二加密签名字段中填充密钥信息或者第二签名信息，其中，密钥信息用于解密密文敏感信息，第二签名信息用于验证加密后的本地敏感信息的完整正确性
步骤S12842：根据第二扩展域名系统附加选项信息，以及包括密钥信息或者第二签名信息的第二附加选项信息，得到第二域名系统请求信息

图 15

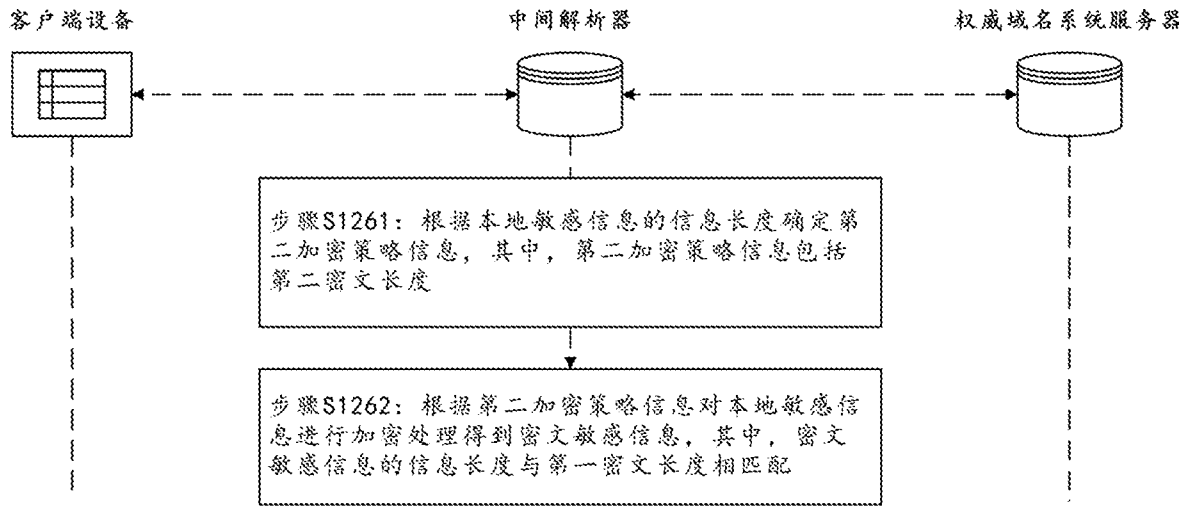
客户端设备
中间解析器
权威域名系统服务器
步骤S1261：根据本地敏感信息的信息长度确定第二加密策略信息，其中，第二加密策略信息包括第二密文长度
步骤S1262：根据第二加密策略信息对本地敏感信息进行加密处理得到密文敏感信息，其中，密文敏感信息的信息长度与第一密文长度相匹配

图 16

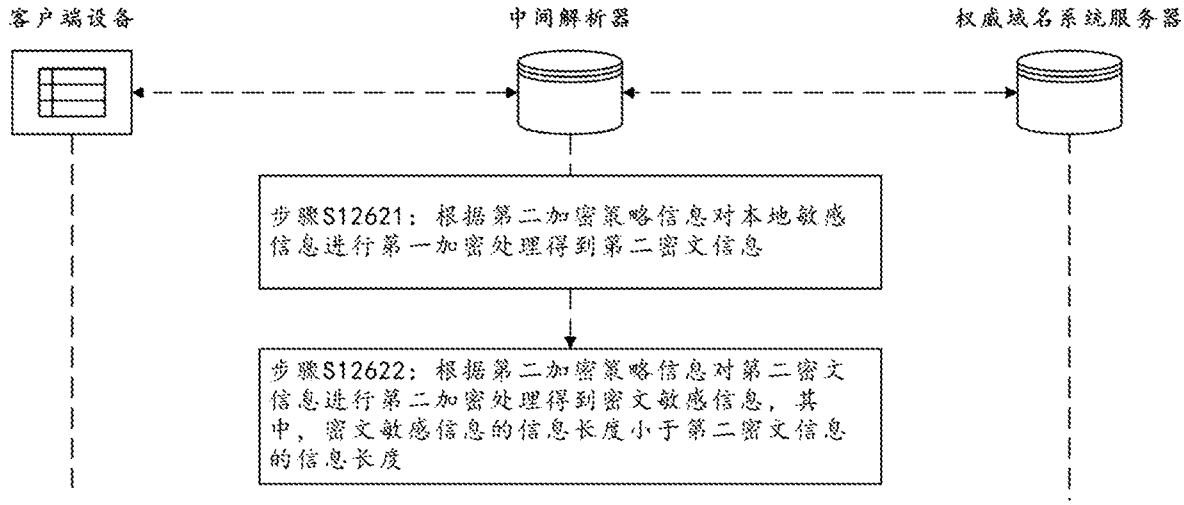
客户端设备
中间解析器
权威域名系统服务器
步骤S12621：根据第二加密策略信息对本地敏感信息进行第一加密处理得到第二密文信息
步骤S12622：根据第二加密策略信息对第二密文信息进行第二加密处理得到密文敏感信息，其中，密文敏感信息的信息长度小于第二密文信息的信息长度

图 17

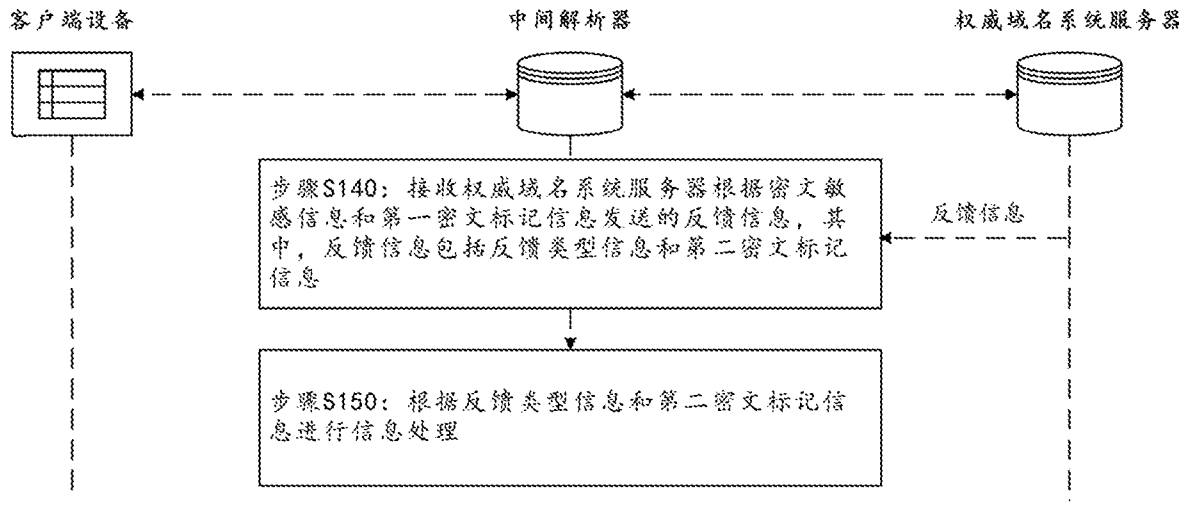
客户端设备
中间解析器
权威域名系统服务器
步骤S140：接收权威域名系统服务器根据密文敏感信息和第一密文标记信息发送的反馈信息，其中，反馈信息包括反馈类型信息和第二密文标记信息
反馈信息
步骤S150：根据反馈类型信息和第二密文标记信息进行信息处理

图 18

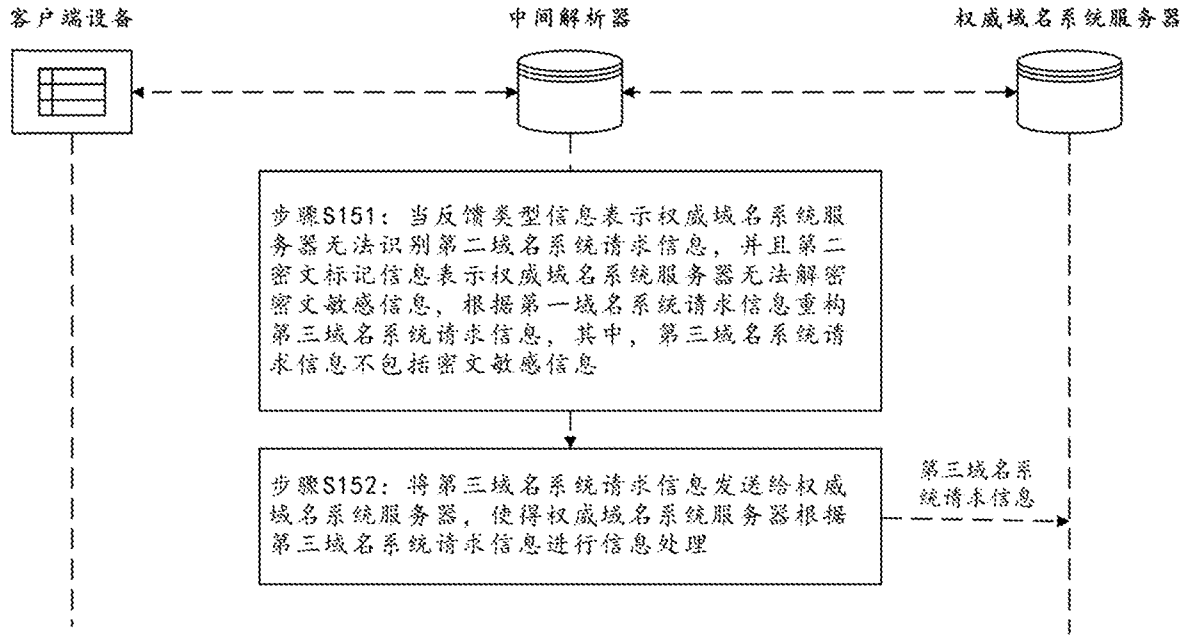
客户端设备
中间解析器
权威域名系统服务器
步骤S151：当反馈类型信息表示权威域名系统服务器无法识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器无法解密密文敏感信息，根据第一域名系统请求信息重构第三域名系统请求信息，其中，第三域名系统请求信息不包括密文敏感信息
步骤S152：将第三域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据第三域名系统请求信息进行信息处理
第三域名系统请求信息

图 19

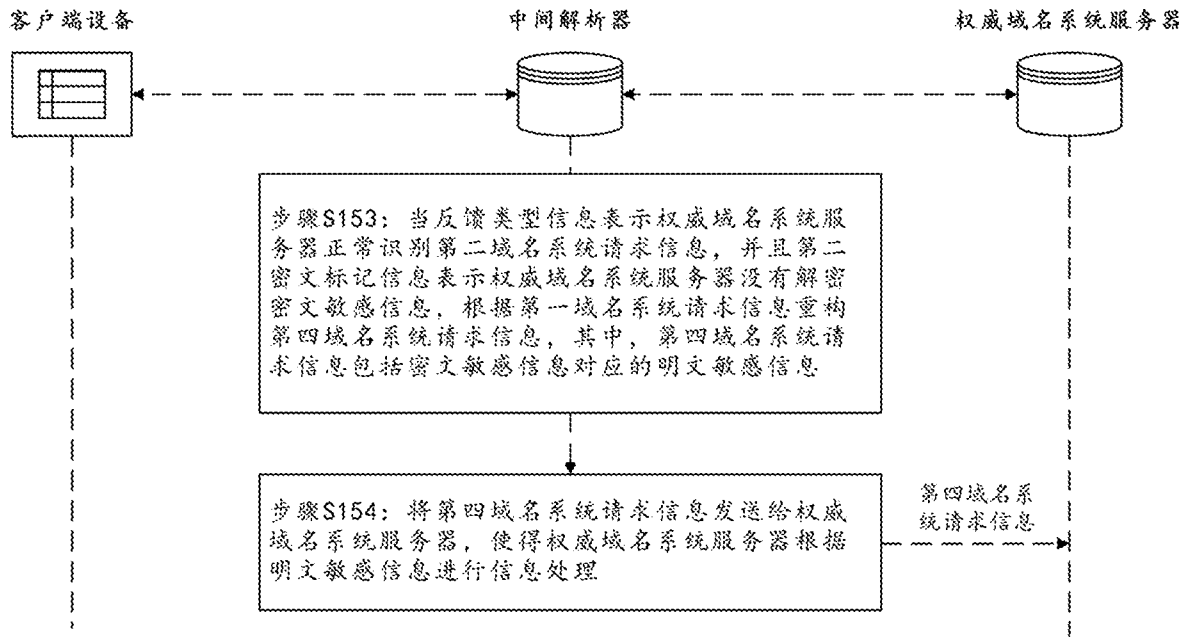
客户端设备
中间解析器
权威域名系统服务器
步骤S153：当反馈类型信息表示权威域名系统服务器正常识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器没有解密密文敏感信息，根据第一域名系统请求信息重构第四域名系统请求信息，其中，第四域名系统请求信息包括密文敏感信息对应的明文敏感信息
步骤S154：将第四域名系统请求信息发送给权威域名系统服务器，使得权威域名系统服务器根据明文敏感信息进行信息处理
第四域名系统请求信息

图 20

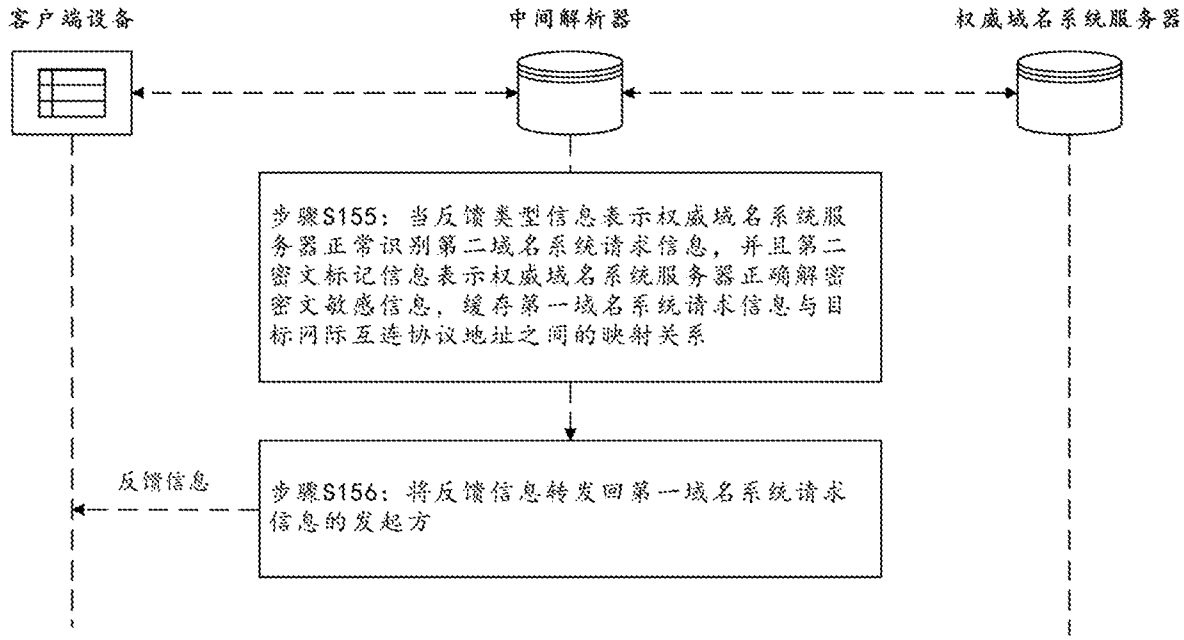
客户端设备
中间解析器
权威域名系统服务器
步骤S155：当反馈类型信息表示权威域名系统服务器正常识别第二域名系统请求信息，并且第二密文标记信息表示权威域名系统服务器正确解密密文敏感信息，缓存第一域名系统请求信息与目标网际互连协议地址之间的映射关系
反馈信息
步骤S156：将反馈信息转发回第一域名系统请求信息的发起方

图 21

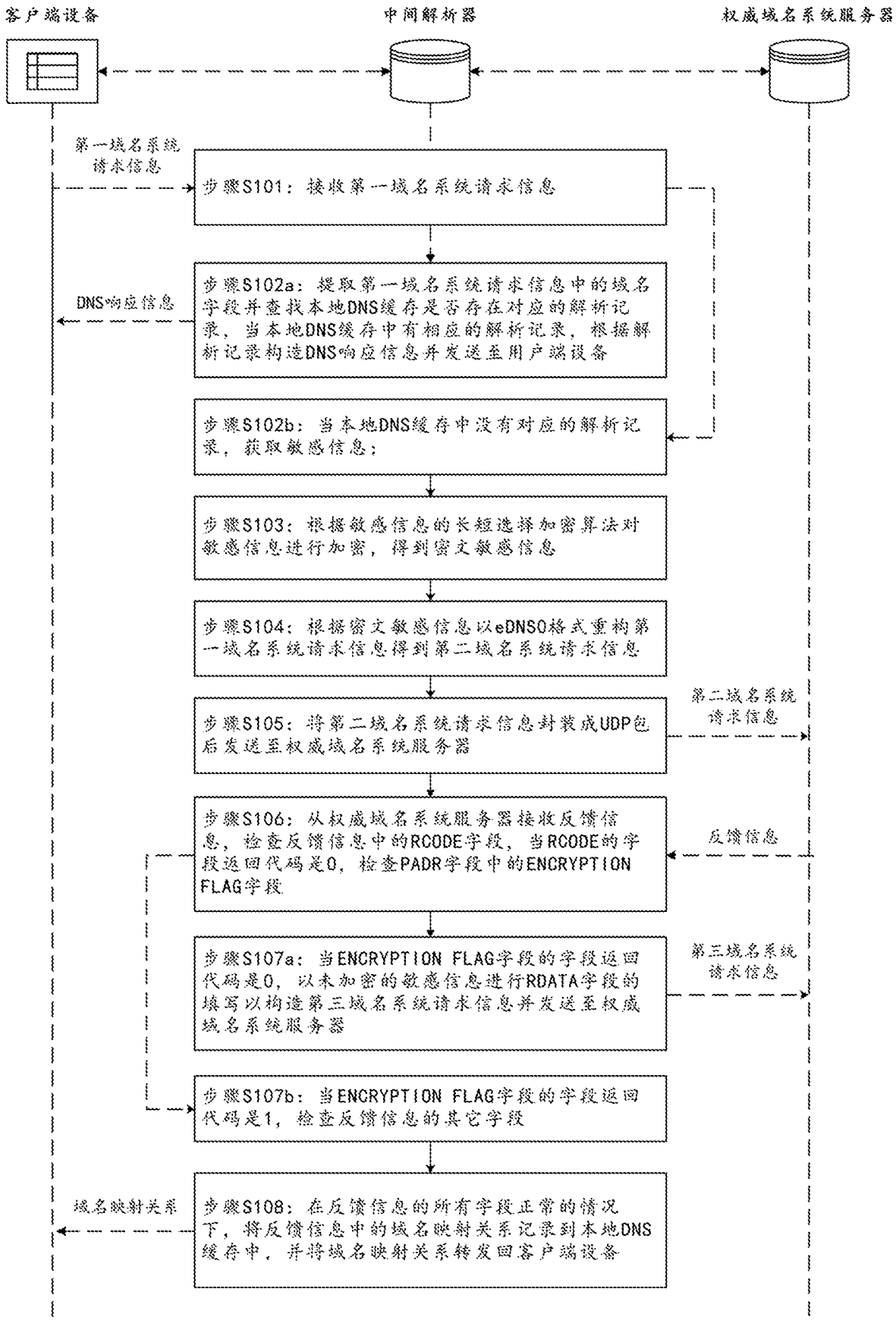
客户端设备
中间解析器
权威域名系统服务器
第一域名系统请求信息
步骤S101：接收第一域名系统请求信息
步骤S102a：提取第一域名系统请求信息中的域名字段并查找本地DNS缓存是否存在对应的解析记录，当本地DNS缓存中有相应的解析记录，根据解析记录构造DNS响应信息并发送至用户端设备
DNS响应信息
步骤S102b：当本地DNS缓存中没有对应的解析记录，获取敏感信息；
步骤S103：根据敏感信息的长短选择加密算法对敏感信息进行加密，得到密文敏感信息
步骤S104：根据密文敏感信息以eDNS0格式重构第一域名系统请求信息得到第二域名系统请求信息
步骤S105：将第二域名系统请求信息封装成UDP包后发送至权威域名系统服务器
第二域名系统请求信息
步骤S106：从权威域名系统服务器接收反馈信息，检查反馈信息中的RCODE字段，当RCODE的字段返回代码是0，检查PADR字段中的ENCRYPTION FLAG字段
反馈信息
步骤S107a：当ENCRYPTION FLAG字段的字段返回代码是0，以未加密的敏感信息进行RDATA字段的填写以构造第三域名系统请求信息并发送至权威域名系统服务器
第三域名系统请求信息
步骤S107b：当ENCRYPTION FLAG字段的字段返回代码是1，检查反馈信息的其它字段
域名映射关系
步骤S108：在反馈信息的所有字段正常的情况下，将反馈信息中的域名映射关系记录到本地DNS缓存中，并将域名映射关系转发回客户端设备

图 22

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2022/099220**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 61/45(2022.01)i; H04L 9/40(2022.01)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)

CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 域名, 请求, 解析, 敏感, 密文, 加密, 安全, 仅, 只, 权威, 标记, 标识, 中间, DNS, domain, request, parse, sensitive, ciphertext, encryption, safety, only, authority, label, identification, ID, middle

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 105959433 A (WUXI CHINAC DATA TECHNOLOGY SERVICE CO., LTD.) 21 September 2016 (2016-09-21)<br>description, paragraphs [0042]-[0091] | 1-20 |
| X | CN 103825969 A (UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA) 28 May 2014 (2014-05-28)<br>description, paragraphs [0024]-[0066] | 1-20 |

☐ 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 | Date of mailing of the international search report |
|---|---|
| **03 August 2022** | **29 August 2022** |

| Name and mailing address of the ISA/CN | Authorized officer |
|---|---|
| **China National Intellectual Property Administration (ISA/CN)**<br>**No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** | |
| Facsimile No. **(86-10)62019451** | Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2022/099220**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 105959433 A | 21 September 2016 | None | |
| CN 103825969 A | 28 May 2014 | None | |

# 国际检索报告

国际申请号
PCT/CN2022/099220

A. 主题的分类

H04L 61/45(2022.01)i; H04L 9/40(2022.01)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））

CNABS;CNTXT;CNKI;VEN;USTXT;EPTXT;WOTXT：域名，请求，解析，敏感，密文，加密，安全，仅，只，权威，标记，标识，中间，DNS，domain，request，parse，sensitive，ciphertext，encryption，safety，only，authority，label，identification，ID，middle

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 105959433 A (无锡华云数据技术服务有限公司) 2016年9月21日 (2016-09-21)<br>说明书第[0042]-[0091]段 | 1-20 |
| X | CN 103825969 A (电子科技大学) 2014年5月28日 (2014-05-28)<br>说明书第[0024]-[0066]段 | 1-20 |

☐ 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 | 国际检索报告邮寄日期 |
|---|---|
| 2022年8月3日 | 2022年8月29日 |

| ISA/CN的名称和邮寄地址 | 受权官员 |
|---|---|
| 中国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088 | 苏星晔 |
| 传真号 (86-10)62019451 | 电话号码 86-(512)-88996074 |

# 国际检索报告
## 关于同族专利的信息

国际申请号
PCT/CN2022/099220

| 检索报告引用的专利文件 | 公布日<br>(年/月/日) | 同族专利 | 公布日<br>(年/月/日) |
|---|---|---|---|
| CN 105959433 A | 2016年9月21日 | 无 | |
| CN 103825969 A | 2014年5月28日 | 无 | |