

(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



(10) 国际公布号

WO 2020/233033 A1

(43) 国际公布日

2020 年 11 月 26 日 (26.11.2020)

(51) 国际专利分类号:

H04L 29/06 (2006.01) H04L 9/08 (2006.01)

H04L 9/32 (2006.01)

(21) 国际申请号:

PCT/CN2019/120084

(22) 国际申请日:

2019 年 11 月 22 日 (22.11.2019)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201910423011.3 2019年5月20日 (20.05.2019) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201

室(入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(72) 发明人: 李全程(LI, Quanchen); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司(SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, IR, IS,

(54) Title: INFORMATION INTERACTION METHOD, DEVICE AND STORAGE MEDIUM

(54) 发明名称: 信息交互方法、装置及存储介质

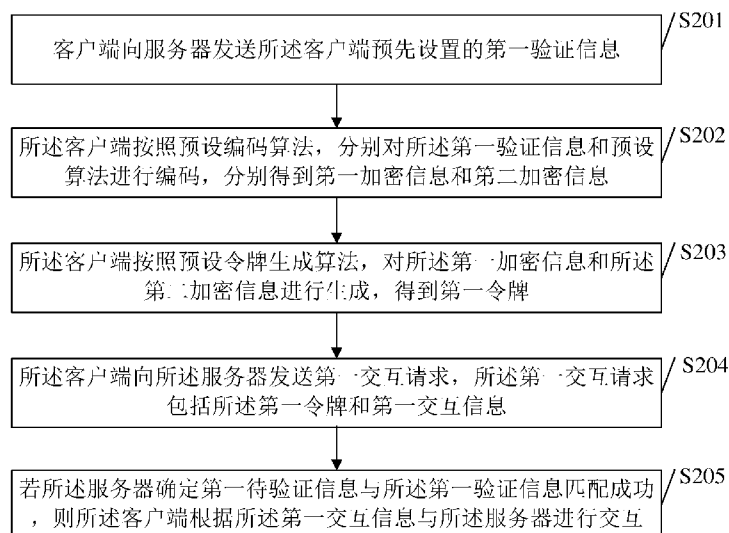


图 2

S201 A client sending to a server first verification information pre-configured by the client
S202 The client respectively encoding the first verification information and a preset algorithm according to a preset encoding algorithm to obtain first encrypted information and second encrypted information, respectively
S203 The client generating the first encrypted information and the second encrypted information according to a preset token generation algorithm to obtain a first token
S204 The client sending a first interaction request to the server, the first interaction request comprising the first token and the first interaction information
S205 If the server determines that first information to be verified successfully matches the first verification information, the client interacting with the server according to the first interaction information

(57) Abstract: Disclosed by embodiments of the present application are an information interaction method, a device and a storage medium, the method comprising: a client sending to a server first verification information pre-configured by the client; the client respectively encoding the first verification information and a preset algorithm according to a preset encoding algorithm to obtain first encrypted information and second encrypted information, respectively; the client generating the first encrypted information and the second encrypted information according to a preset token generation algorithm to obtain a first token; and if the server determines that

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))。

first information to be verified successfully matches the first verification information, the client interacting with the server according to the first interaction information. By using the present application, the security of information interaction may be improved.

(57) 摘要: 本申请实施例公开了一种信息交互方法、装置及存储介质, 其中方法包括: 客户端向服务器发送所述客户端预先设置的第一验证信息; 所述客户端按照预设编码算法分别对所述第一验证信息和预设算法进行编码分别得到第一加密信息和第二加密信息; 所述客户端按照预设令牌生成算法对所述第一加密信息和所述第二加密信息进行生成得到第一令牌; 若所述服务器确定第一待验证信息与所述第一验证信息匹配成功, 则所述客户端根据所述第一交互信息与所述服务器进行交互。采用本申请, 可提高信息交互的安全性。

信息交互方法、装置及存储介质

本申请要求于 2019 年 05 月 20 日提交中国专利局、申请号为 201910423011.3、申请名称为“信息交互方法、装置及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术领域，主要涉及了一种信息交互方法、装置及存储介质。

背景技术

在现有技术中，服务器与客户端之间的信息交互基于验证会话对象（Session 对象）的方式，即通过服务器创建 Session 对象，并将 Session 对象的用户标识回传给客户端，这样，只要客户端的浏览器不关，再去访问服务器时，都会携带该用户标识，使得客户端访问服务器。然而，若第三方能获得到该用户标识，则可依据该用户标识进行模拟登录，从而导致安全隐患，因此，如何提高信息交互的安全性是本领域技术人员待解决的技术问题。

发明内容

本申请实施例提供了一种信息交互方法、装置及存储介质，可提高信息交互的安全性。

第一方面，本申请实施例提供一种信息交互方法，应用于客户端，其中：

所述客户端向服务器发送所述客户端预先设置的第一验证信息；

所述客户端按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；

所述客户端按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

所述客户端向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；

若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则所述客户端根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

第二方面，本申请实施例提供另一种信息交互方法，应用于服务器，其中：

所述服务器接收客户端发送的所述客户端预先设置的第一验证信息；

所述服务器接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

所述服务器按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；

所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；

若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则所述服务器根据所述第一交互信息与所述客户端进行交互。

第三方面，本申请实施例提供一种信息交互装置，应用于客户端，其中：

通信单元，用于向服务器发送所述客户端预先设置的第一验证信息；

加密单元，用于按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

通信单元，还用于向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

第四方面，本申请实施例提供另一种信息交互装置，应用于服务器，其中：

通信单元，用于接收客户端发送的所述客户端预先设置的第一验证信息；接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

解密单元，用于按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述客户端进行交互。

第五方面，本申请实施例提供一种客户端，包括处理器、存储器、通信接口以及一个或多个程序，其中，上述一个或多个程序被存储在上述存储器中，并且被配置由上述处理器执行，所述程序包括用于如第一方面中所描述的部分或全部步骤的指令。

第六方面，本申请实施例提供一种服务器，包括处理器、存储器、通信接口以及一个或多个程序，其中，上述一个或多个程序被存储在上述存储器中，并且被配置由上述处理器执行，所述程序包括用于如第二方面中所描述的部分或全部步骤的指令。

第七方面，本申请实施例提供了一种计算机非易失性可读存储介质，其中，所述计算机非易失性可读存储介质存储计算机程序，其中，所述计算机程序使得计算机执行以实现如第一方面中所描述的部分或全部步骤，所述计算机包括客户端。

第八方面，本申请实施例提供了另一种计算机非易失性可读存储介质，其中，所述计算机非易失性可读存储介质存储计算机程序，其中，所述计算机程序使得计算机执行以实现如第二方面中所描述的部分或全部步骤，所述计算机包括服务器。

实施本申请实施例，将具有如下有益效果：

采用了上述的信息交互方法、装置及存储介质之后，客户端与服务器之间基于预设编码算法和预设令牌生成算法得到的令牌进行交互，提高了信息交互的安全性。

附图说明

为了更清楚地说明本申请实施例技术方案，下面将对实施例描述中所需要使用的附图进行说明。

图1为本申请实施例提供的一种信息交互系统的结构示意图；

图2为本申请实施例提供的一种信息交互方法的流程示意图；

图3为本申请实施例提供的另一种信息交互方法的流程示意图；

图4为本申请实施例提供的一种信息交互系统的流程示意图；

图 5 为本申请实施例提供的一种信息交互装置的逻辑结构示意图；

图 6 为本申请实施例提供的一种信息交互装置的实体结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。

请参见图 1，图 1 为应用本申请实施例的网络架构示意图。该网络架构示意图包括服务器 101、客户端 102 和用户 103。需要说明的是，图 1 所示的网络架构示意图中的各个设备的数量和形态用于举例，并不构成对本申请实施例的限定。

其中，客户端 102 可以是图 1 所示的个人计算机（personal computer，PC）、笔记本电脑或智能手机，还可以是一体机、掌上电脑、平板电脑（pad）、智能电视播放终端、车载终端或便捷式设备等电子设备。PC 端客户端，例如一体机等，其操作系统可以包括但不限于 Linux 系统、Unix 系统、Windows 系列系统（例如 Windows xp、Windows 7 等）、Mac OS X 系统（苹果电脑的操作系统）等操作系统。移动端客户端，例如智能手机等，其操作系统可以包括但不限于安卓系统、IOS（苹果手机的操作系统）、Window 系统等操作系统。

服务器 101 与通用的计算机架构类似，包括处理器、硬盘、内存、系统总线等，用于为客户端 102 提供服务。该服务器 101 可以运行于单独的设备，也可以运行于多个服务器组成的客户端集群，在此不做限定。

用户 103 可以是实际操作客户端 102 的用户，也可以是开发人员。用户 103 可以对客户端 102 输入操作指令，以控制客户端 102 执行相应地操作。

下面对本申请实施例提供的信息交互方法的具体流程进一步进行说明。

请参照图 2，本申请实施例提供一种信息交互方法的流程示意图。该信息交互方法应用于客户端，具体的，如图 2 所示，一种信息交互方法，其中：

S201：客户端向服务器发送所述客户端预先设置的第一验证信息。

在本申请实施例中，第一验证信息用于验证客户端对应的用户的身份信息，服务器可在接收到客户端发送的第一验证信息之后，存储于服务器中。第一验证信息是客户端预先设置的验证信息，可包括动态信息和用户信息等，在此不做限定。

其中，用户信息包括身份标识和身份标识对应的类型，身份标识可以是身份证号码、电话号码、联系邮箱等，具有唯一性，其类型可包括用户名、电话、邮箱等，在此均不做限定。

动态信息用于当前交互的验证，也就是说，每次交互完成之后或提交交互信息时，均生成一个动态信息。可以理解，通过验证该动态信息，可进一步提高信息交互的安全性。

在本申请实施例中，动态信息可以是时间，例如，上一次客户端向服务器提交交互请求的时间、本次客户端向服务器提交交互请求的时间、上一次服务器响应客户端的交互请求的时间，或者上一次服务器响应客户端的交互请求与客户端发送该交互请求之间的时间间隔；动态信息也可以是交互次数、交互频率等，在此也不做限定。

S202：所述客户端按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息。

在本申请实施例中，预设算法可包括安全散列算法（Secure Hash Algorithm，SHA），例如：SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512，预设算法也可包括消息摘要算法（Message-Digest Algorithm，MD5），预设算法还可包括基于哈希消息认证码（Hash-based Message Authentication Code，HMAC）的算法等，在此不做限定。

在本申请实施例中，第一加密信息由客户端按照预设编码算法对第一验证信息进行编码得到，第二加密信息由客户端按照预设编码算法对预设算法进行编码得到。其中，预设

编码算法可以基于美国信息交换标准代码 (American Standard Code for Information Interchange , ASCII)、ISO-8859-1、GB2312、GBK、UTF (Unicode Transformation Format) -8、UTF-16、base64 等中编码算法的一种或多种, 在此不做限定。

其中, ASCII 是基于拉丁字母的一套电脑编码系统, 主要用于显示现代英语和其他西
5 欧语言。ASCII 总共有 128 个, 用一个字节的低 7 位表示, 其中, 0~31 是控制字符如换行回车删除等, 32~126 是打印字符。

ISO-8859-1 是单字节编码, 用于扩展 ASCII, 其编码范围是 0x00-0xFF, 0x00-0x7F 之间完全和 ASCII 一致, 0x80-0x9F 之间是控制字符, 0xA0-0xFF 之间是文字符号。

GB2312 全称是信息交换的汉字编码字符集, 是双字节编码, 总的编码范围是 A1-F7, 其中从 A1-A9 是符号区, 总共包含 682 个符号, 从 B0-F7 是汉字区, 包含 6763 个汉字。
10

GBK 全称是汉字内码扩展规范, 用于扩展 GB2312。它的编码范围是 8140~FEFE (去掉 XX7F) 总共有 23940 个码位, 它能表示 21003 个汉字。

UTF-16 具体定义了 Unicode 字符在计算机中存取方法。UTF-16 用两个字节来表示 Unicode 转化格式, 是定长的表示方法。

UTF-8 采用了一种变长技术, 每个编码区域有不同的字码长度。不同类型的字符可以
15 是由 1~6 个字节组成。

base64 是网络上最常见的用于传输 8Bit 字节码的编码方式之一, 可用于在 HTTP 环境下传递较长的标识信息。具体可根据一系列以编号排定的文件(Request For Comments ,RFC) 中多用途的网际邮件扩充协议 (Multipurpose Internet Mail Extensions , MIME) 的详细规范
20 进行转换以得到字符串。

本申请以 ASCII 编码和 base64 编码进行举例说明, 先将按照 ASCII 编码将第一验证信息和预设算法对应的字符串转换为二进制, 再分别按照 base64 编码将第一验证信息和预设算法对应的二进制转换为字符串。

例如, 若转换前的字符串为 s13, 则先转成美国信息交换标准代码 (American Standard
25 Code for Information Interchange ,ASCII)可得到 115 49 51 ,再转换为 2 进制可得到 01110011 00110001 00110011 ,将 6 个分为一组可得到 011100 110011 000100 110011 ,由于计算机是 8 位的存数 则高位补 0 可得到 00011100 00110011 00000100 00110011 ,也就是十进制的 28 51 4 51 ,通过查照下表 1 所示的 RFC2045 可得到转换后的字符串为: czEz。

表 1

索引	对应字符	索引	对应字符	索引	对应字符	索引	对应字符
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	G	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/

13	N	30	e	47	v		
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

可以理解，按照预设编码算法分别对第一验证信息和预设算法进行编码，也就是分别对第一验证信息和预设算法进行编码，可提高验证第一验证信息的安全性。

S203：所述客户端按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌。

5 在本申请实施例中，第一令牌为客户端与服务器之间信息交互的验证信息。

本申请对于预设令牌生成算法不做限定，可分别提取第一加密信息和第二加密信息中的部分字符，例如：首尾字符，再将其部分字符进行编码；也可组合第一加密信息和第二加密信息，再将其组合信息进行编码等。

10 在一种可能的示例中，所述客户端按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌，包括：所述客户端按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；所述客户端按照所述预设算法对所述第三加密信息进行编码，得到第四加密信息；所述客户端按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；所述客户端按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述
15 第一令牌。

其中，第三加密信息为第一加密信息和第二加密信息按照预设组合算法进行组合得到的信息，本申请对于预设组合算法不做限定，可采用特定符号或特定字符进行拼接，例如“+”、“-”、“/”、“000”等，举例来说，第一加密信息为 kc ds，第二加密信息为 jos d，则第三加密信息为 kc ds+jos d。预设组合算法也可先将每一部分的首字母进行大写，其他则为小写，再
20 直接进行组合，例如：第一加密信息为 kc ds，第二加密信息为 jos d，第三加密信息为 Kc dsJos d。

第四加密信息为第三加密信息按照预设算法进行编码得到的信息，其中预设算法可参照步骤 S101 的描述，在此不再赘述。可以理解，经过加密第一加密信息和第二加密信息组合得到的第三加密信息，使得第四加密信息的安全性更高，便于提高信息交互的安全性。

25 第五加密信息为第一加密信息、第二加密信息和第四加密信息按照预设组合算法进行组合得到的信息，其预设组合算法可参照第三加密信息的描述，在此不再赘述。

第一令牌为第五加密信息按照预设缩短算法进行缩短处理得到的信息。本申请对于预设缩短算法的方法不做限定，在一种可能的示例中，所述第五加密信息包括多个字符，所述客户端对所述第五加密信息进行缩短处理，得到所述第一令牌，包括：所述客户端获取所述多个字符中每一字符对应的序号和数量；所述客户端根据所述多个字符中每一字符的
30 序列和数量获取所述字符对应的权值，得到多个权值；所述客户端根据所述多个权值将所述多个字符进行哈夫曼编码，得到所述第一令牌。

其中，序号的获取方法可基于字母顺序排列的单词按字母顺序排列的方法，即按照字母表的顺序确定各个字母的序号。

35 哈夫曼编码(Huffman Coding)，又称霍夫曼编码，是一种编码方式，哈夫曼编码是可变字长编码的一种，该方法完全依据字符出现概率来构造异字头的平均长度最短的码字。

在上述可能的示例中，客户端先获取各个字符的数量，以及各个字符对应的序号，再依据各个字符的数量和序号确定各个字符的权值，然后进行哈夫曼编码得到第一令牌，如此，使得第一令牌的字符长度小于第五加密信息的字符长度，可提高信息交互的效率和安全性。

可以理解，客户端对第一加密信息和第二加密信息进行组合以得到第三加密信息，然后由预设算法对第三加密信息进行编码以得到第四加密信息。再对第一加密信息、第二加密信息和第四加密信息进行组合，可得到较长的第五加密信息，再通过缩短处理第五加密信息得到较短的第一令牌，从而缩短了第一令牌的传输长度，提高了交互的效率和安全性。

且第一令牌经过组合、加密和再组合的操作，可进一步提高了信息交互的安全性。

S204：所述客户端向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息。

在本申请实施例中，第一交互信息可包括待访问网址、预存储信息等，在此不做限定，第一交互信息用于指示服务器如何与客户端进行信息交互。

S205：若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则所述客户端根据所述第一交互信息与所述服务器进行交互。

其中，第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，即为客户端按照预设编码算法对第一验证信息进行编码得到第一加密信息的逆过程。第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到，即为客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到第一令牌的逆过程，在此均不做赘述。

在如图2所示的信息交互方法中，客户端按照预设编码算法分别对该客户端预先设置的第一验证信息和预设算法进行编码分别得到第一加密信息和第二加密信息。然后，客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到第一令牌，向服务器发送包括第一令牌和第一交互信息的第一交互请求。然后，服务器按照该预设令牌生成算法对第一令牌进行解密得到第一解密信息，按照预设编码算法对第一解密信息进行解码得到第一待验证信息。若该第一待验证信息与该客户端预先向服务器发送的第一验证信息匹配成功，则客户端根据第一交互信息与服务器进行交互。如此，客户端与服务器之间基于预设编码算法和预设令牌生成算法得到的令牌进行交互，提高了信息交互的安全性。

在一种可能的示例中，在所述客户端根据所述第一交互信息与所述服务器进行交互之后，所述方法还包括：所述客户端对所述第一验证信息中的动态信息进行更新，得到第二验证信息；所述客户端向所述服务器发送所述第二验证信息；所述客户端按照所述预设编码算法，对所述第二验证信息进行编码，得到第六加密信息；所述客户端按照所述预设令牌生成算法，对所述第六加密信息和所述第一加密信息进行生成，得到第二令牌；所述客户端向所述服务器发送第二交互请求，所述第二交互请求包括所述第二令牌和第二交互信息；若所述服务器确定第二待验证信息与所述第二验证信息匹配成功，则所述客户端根据所述第二交互信息与所述服务器进行交互，所述第二待验证信息由所述服务器按照所述预设编码算法对第二解密信息进行解码得到，所述第二解密信息由所述服务器按照所述预设令牌生成算法对所述第二令牌进行拆分得到。

其中，动态信息如前所述，用于当前交互的验证。第二验证信息为更新的第一验证信息。第六加密信息可参照第一加密信息和第二加密信息的编码步骤，第二令牌可参照第一令牌的描述，第二交互信息可参照第一交互信息的描述，第二解密信息可参照第一解密信息的描述，第二待验证信息可参照第一待验证信息的描述，在此均不再赘述。

可以理解，客户端对第一验证信息中的动态信息进行更新得到第二验证信息，再按照步骤S202、S203的方法对第二验证信息进行编码得到第二令牌，从而客户端可基于该第二令牌与服务器进行信息交互。如此，更新了服务器中存储的验证信息，以免第三方利用使用原始的第一令牌与服务器进行交互，进一步提高信息交互的安全性。

本申请对于更新第一验证信息的方法不做限定，在一种可能的示例中，所述客户端对

所述第一验证信息中的动态信息进行更新，得到第二验证信息，包括：所述客户端获取所述客户端向所述服务器发送所述第一交互请求的请求时间；所述客户端将所述第一验证信息中的动态信息更新为所述请求时间，得到所述第二验证信息。

可以理解，将客户端与服务器发送第一交互请求的请求时间作为第一验证信息中的动态信息，也就是说，将上一次客户端向服务器提出交互请求的请求时间作为动态信息，然后，服务器更新该动态信息以得到第二验证信息。如此，提高了动态信息的灵活性，即提高了令牌的灵活性，便于提高信息交互安全。

与图 2 所示的实施例一致，请参照图 3，图 3 是本申请实施例提供的另一种信息交互方法的流程示意图，该方法应用于服务器，具体的，如图 3 所示，一种信息交互方法，包括：

S301：服务器接收客户端发送的所述客户端预先设置的第一验证信息。

S302：服务器接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息。

其中，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到，可参照步骤 S202、S203 的描述，在此均不再赘述。

S303：所述服务器按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息。

其中，第一解密信息和第二解密信息由服务器按照预设令牌生成算法对第一令牌进行拆分得到，即为客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到第一令牌的逆过程，在此不再赘述。

S304：所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息。

其中，第一待验证信息和第二待验证信息由服务器按照预设编码算法对第一解密信息进行解码得到，即为客户端按照预设编码算法对第一验证信息进行编码得到第一加密信息的逆过程，在此不再赘述。

S305：若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则所述服务器根据所述第一交互信息与所述客户端进行交互。

本申请对于验证第一待验证信息与第一验证信息的方法不做限定，可先分别对动态信息进行验证，若动态信息验证成功，则再分别验证用户信息，否则返回异常。若用户信息验证成功，则确定第一待验证信息与第一验证信息验证成功，否则返回异常。

在如图 3 所示的信息交互方法中，服务器接收客户端发送的第一验证信息和包括第一令牌的第一交互请求，并按照预设令牌生成算法对该第一令牌进行拆分得到第一解密信息和第二解密信息，然后按照预设编码算法分别对该第一解密信息和该第二解密信息进行解码得到第一待验证信息和第二待验证信息。若该第二待验证信息与预设算法匹配成功，该第一待验证信息与该第一验证信息匹配成功，则服务器根据该第一交互请求中的第一交互信息与客户端进行交互。如此，客户端与服务器之间基于预设编码算法和预设令牌生成算法得到的令牌进行交互，提高了信息交互的安全性。

在另一种可能的示例中，所述服务器按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息；所述服务器按照所述预设组合算法，对所述第五解密信息进行拆分，得到第一解密信息和第二解密信息和第四解密信息；所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息和所述第四解密信息进行解码，分

别得到第一信息、第二信息和第三信息；若所述第二信息与所述预设算法匹配成功，则所述服务器确定所述第二信息为所述第二待验证信息；所述服务器按照所述预设组合算法，对所述第二信息和所述第一信息进行组合，得到第一组合信息，所述服务器按照所述预设组合算法，对所述第二信息和所述第三信息进行组合，得到第二组合信息；若所述第一组
5 合信息与所述第三信息匹配成功，则所述服务器确定所述第一信息为所述第一待验证信息。

其中，第五解密信息为第一令牌按照预设缩短算法进行延长处理得到的信息，即第五信息按照预设缩短算法进行缩短处理得到的第一令牌的逆过程。

在一种可能的示例中，所述第一令牌包括多个字符，所述服务器按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息，包括：所述服务器对所述多个字符中每一字符进行哈夫曼解码，以得到多个权值，每一权值对应一个字符；所述服务器根据所述多个权值获取所述多个字符中每一字符的序列和数量；所述服务器根据所述多个字
10 符中每一字符的序列和数量获取所述第五解密信息。

其中，哈夫曼解码为哈夫曼编码的逆过程。

可以理解，服务器先对第一令牌中的字符进行哈夫曼解码以得到多个权值，再获取各个字符的序列和数量，然后根据各个字符的序列和数量获取第五信息，如此，恢复了缩短的字符串，提高了获取第五解密信息的准确性。

在本申请中，第一解密信息和第二解密信息和第四解密信息分别按照预设组合算法对第五解密信息进行拆分得到的信息，即按照预设组合算法对第一加密信息、第二加密信息和第四加密信息进行组合得到第五加密信息的逆过程。

第一解密信息、第二解密信息和第三解密信息分别按照预设编码算法对第一解密信息和第二解密信息和第四解密信息进行解码得到的信息，即分别按照预设编码算法对预设算法、第一验证信息、第三加密信息进行编码分别得到第一加密信息、第二加密信息和第三加密信息的逆过程。

在本申请中，第三加密信息为第一加密信息和第二加密信息的组合信息，则在第二信息与预设算法匹配成功时，则确定第二信息与第一加密信息匹配。然后，服务器按照预设组合算法分别对第二信息和第一信息，第二信息和第三信息进行组合，分别得到第一组合信息和第二组合信息。若确定第一组合信息与第三信息匹配成功，则确定第三信息与第四加密信息匹配，将第一解密信息作为第一待验证信息。

可以理解，在拆分第一令牌的过程中，获取第一待验证信息，若第一待验证信息与第一验证信息验证成功，则允许客户端与服务器进行交互，从而进一步提高信息交互的安全性。

需要说明的是，服务器也可按照步骤 S202、S203 的方法获取待验证令牌，若该待验证令牌与第一令牌匹配成功，则允许客户端根据第一交互信息与服务器进行交互。

在一种可能的示例中，在所述服务器根据所述第一交互信息与所述客户端进行交互之后，所述方法还包括：所述服务器接收所述客户端发送的第二验证信息，所述第二验证信息由所述客户端对所述第一验证信息中的动态信息进行更新得到。

需要说明的是，服务器也可参照第二验证信息的更新方法进行更新，如此，在信息交互完成之后，自动更新了服务器中存储的验证信息，提高了更新操作的便利性和信息交互的安全性。

与图 2 和图 3 所示的实施例一致，请参照图 4，图 4 是本申请提出的一种信息交互系统执行的时序图。如图 4 所示，包括：

S401：客户端向服务器发送所述客户端预先设置的第一验证信息。

S402：所述客户端按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，

分别得到第一加密信息和第二加密信息。

S403：所述客户端按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌。

5 S404：所述客户端向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息。

S405：所述服务器按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息。

S406：所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息。

10 S407：若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则所述服务器根据所述第一交互信息与所述客户端进行交互。

在如图4所示的信息交互系统中，客户端分别基于预设编码算法和预设令牌生成算法对第一验证信息进行加密得到第一令牌，并向服务器发送包括第一令牌的第一交互请求。然后，服务器再分别基于预设编码算法和预设令牌生成算法对该第一令牌进行解密得到第一待验证信息。若第一待验证信息与第一验证信息匹配成功，则允许客户端根据第一交互请求中的第一交互信息与服务器进行交互，从而提高了信息交互的安全性。

15

上述详细阐述了本申请实施例的方法，下面提供了本申请实施例的装置。

与图2所示的实施例一致，请参照图5，图5是本申请提出的一种信息交互装置的结构示意图，所述装置应用于客户端。如图5所示，上述信息交互装置500包括：

20 通信单元501，用于向服务器发送客户端预先设置的第一验证信息；

加密单元502，用于按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

通信单元501，还用于向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

25

在一种可能的示例中，在所述按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌方面，所述加密单元502具体用于按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；按照所述预设编码算法，对所述第三加密信息进行编码，得到第四加密信息；按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌。

30

在一种可能的示例中，所述第五加密信息包括多个字符，在所述对所述第五加密信息进行缩短处理，得到所述第一令牌方面，所述加密单元502具体用于获取所述多个字符中每一字符对应的序号和数量；根据所述多个字符中每一字符的序列和数量获取所述字符对应的权值，得到多个权值；根据所述多个权值对所述多个字符中每一字符进行哈夫曼编码，得到所述第一令牌。

35

在一种可能的示例中，在所述根据所述第一交互信息与所述服务器进行交互之后，所述加密单元502还用于对所述第一验证信息中的动态信息进行更新，得到第二验证信息；所述通信单元501还用于向所述服务器发送所述第二验证信息；所述加密单元502还用于按照所述预设编码算法，对所述第二验证信息进行编码，得到第六加密信息；按照所述预

40

设令牌生成算法，对所述第六加密信息和所述第一加密信息进行生成，得到第三令牌；所述通信单元 501 还用于向所述服务器发送第二交互请求，所述第二交互请求包括所述第二令牌和第二交互信息；若所述服务器确定第二待验证信息与所述第二验证信息匹配成功，则根据所述第二交互信息与所述服务器进行交互，所述第二待验证信息由所述服务器按照所述预设编码算法对第二解密信息进行解码得到，所述第二解密信息由所述服务器按照所述预设令牌生成算法对所述第二令牌进行拆分得到。

在一种可能的示例中，在所述对所述第一验证信息中的动态信息进行更新，得到第二验证信息方面，所述加密单元 502 具体用于获取所述客户端向所述服务器发送所述第一交互请求的请求时间；将所述第一验证信息中的动态时间更新为所述请求时间，得到所述第二验证信息。

与图 3 所示的实施例一致，请参照图 5，该装置应用于服务器。如图 5 所示，上述信息交互装置 500 包括：

通信单元 501，用于接收客户端发送的所述客户端预先设置的第一验证信息；接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

解密单元 502，用于按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述客户端进行交互。

在另一种可能的示例中，所述解密单元 502 还用于按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息；按照所述预设组合算法，对所述第五解密信息进行拆分，得到第一解密信息和第二解密信息和第四解密信息；按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息和所述第四解密信息进行解码，分别得到第一信息、第二信息和第三信息；若所述第二信息与所述预设算法匹配成功，则确定所述第二信息为所述第二待验证信息；按照所述预设组合算法，对所述第二信息和所述第一信息进行组合，得到第一组合信息，按照所述预设组合算法，对所述第二信息和所述第三信息进行组合，得到第二组合信息；若所述第一组合信息与所述第三信息匹配成功，则确定所述第一信息为所述第一待验证信息。

在一种可能的示例中，所述第一令牌包括多个字符，在所述按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息方面，所述解密单元 502 具体用于对所述多个字符中每一字符进行哈夫曼解码，以得到多个权值，每一权值对应一个字符；根据所述多个权值获取所述多个字符中每一字符的序列和数量；根据所述多个字符中每一字符的序列和数量获取所述第五解密信息。

在一种可能的示例中，在所述根据所述第一交互信息与所述客户端进行交互之后，所述通信单元 501 还用于接收所述客户端发送的第二验证信息，所述第二验证信息由所述客户端对所述第一验证信息中的动态信息进行更新得到。

该信息交互装置 500 中各个单元执行详细过程可以参见前述方法实施例中的执行步骤，此处不在赘述。

与图 2 的实施例一致，请参照图 6，图 6 是本申请实施例提供的又一种信息交互装置的结构示意图，该信息交互装置为客户端。如图 6 所示，该信息交互装置 600 包括处理器

610、存储器 620、通信接口 630 以及一个或多个程序 640。图 5 所示的通信单元 501 所实现的相关功能可通过通信接口 630 来实现，图 5 所示的加密单元 502 所实现的相关功能可通过处理器 610 来实现。

上述一个或多个程序 640 被存储在上述存储器 620 中，并且被配置由上述处理器 610 执行，上述程序 640 包括用于执行以下步骤的指令：

向服务器发送所述客户端预先设置的第一验证信息；

按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；

按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；

若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

在一个可能的示例中，在所述按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌方面，所述程序 640 具体用于执行以下步骤的指令：

按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；

按照所述预设编码算法，对所述第三加密信息进行编码，得到第四加密信息；

按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；

按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌。

在一个可能的示例中，所述第五加密信息包括多个字符，在所述按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌方面，所述程序 640 具体用于执行以下步骤的指令：

获取所述多个字符中每一字符对应的序号和数量；

根据所述多个字符中每一字符的序列和数量获取所述字符对应的权值，以得到多个权值；

根据所述多个权值对所述多个字符中每一字符进行哈夫曼编码，以得到所述第一令牌。

在一个可能的示例中，在所述根据所述第一交互信息与所述服务器进行交互之后，所述程序 640 还用于执行以下步骤的指令：

对所述第一验证信息中的动态信息进行更新，得到第二验证信息；

向所述服务器发送所述第二验证信息；

按照所述预设编码算法，对所述第二验证信息进行编码，得到第六加密信息；

按照所述预设令牌生成算法，对所述第六加密信息和所述第二加密信息进行生成，得到第二令牌；

向所述服务器发送第二交互请求，所述第二交互请求包括所述第二令牌和第二交互信息；

若所述服务器确定第二待验证信息与所述第二验证信息匹配成功，则根据所述第二交互信息与所述服务器进行交互，所述第二待验证信息由所述服务器按照所述预设编码算法对第二解密信息进行解码得到，所述第二解密信息由所述服务器按照所述预设令牌生成算

法对所述第二令牌进行拆分得到。

在一个可能的示例中，在所述对所述第一验证信息中的动态信息进行更新，得到第二验证信息方面，所述程序 640 具体用于执行以下步骤的指令：

获取所述客户端向所述服务器发送所述第一交互请求的请求时间；

5 将所述第一验证信息中的动态时间更新为所述请求时间，得到所述第二验证信息。

与图 3 的实施例一致，请参照图 6，该信息交互装置应用于服务器。图 5 所示的通信单元 501 所实现的相关功能可通过通信接口 630 来实现，图 5 所示的解密单元 503 所实现的相关功能可通过处理器 610 来实现。如图 6 所示，上述程序 640 包括用于执行以下步骤的指令：

10 接收客户端发送的所述客户端预先设置的第一验证信息；

接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

15 按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；

按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；

20 若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述客户端进行交互。

在一个可能的示例中，所述程序 640 还用于执行以下步骤的指令：

按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息；

25 按照所述预设组合算法，对所述第五解密信息进行拆分，得到第一解密信息和第二解密信息和第四解密信息；

按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息和所述第四解密信息进行解码，分别得到第一信息、第二信息和第三信息；

若所述第二信息与所述预设算法匹配成功，则确定所述第二信息为所述第二待验证信息；

30 按照所述预设组合算法，对所述第二信息和所述第一信息进行组合，得到第一组合信息，按照所述预设组合算法，对所述第二信息和所述第三信息进行组合，得到第二组合信息；

若所述第一组合信息与所述第三信息匹配成功，则确定所述第一信息为所述第一待验证信息。

35 在一个可能的示例中，所述第一令牌包括多个字符，在所述按照所述预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息方面，所述程序 640 具体用于执行以下步骤的指令：

对所述多个字符中每一字符进行哈夫曼解码，以得到多个权值，每一权值对应一个字符；

40 根据所述多个权值获取所述多个字符中每一字符的序列和数量；

根据所述多个字符中每一字符的序列和数量获取所述第五解密信息。

在一种可能的示例中，在所述根据所述第一交互信息与所述客户端进行交互之后，所述程序 640 还用于执行以下步骤的指令：

接收所述客户端发送的第二验证信息，所述第二验证信息由所述客户端对所述第一验证信息中的动态信息进行更新得到。

本申请实施例还提供一种计算机存储介质，其中，该计算机存储介质存储用于存储计算机程序，该计算机程序使得计算机执行以实现方法实施例中记载的任一方法的部分或全部步骤，计算机包括客户端或服务器。

本申请实施例还提供一种计算机程序产品，计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，计算机程序可操作来使计算机执行以实现方法实施例中记载的任一方法的部分或全部步骤。该计算机程序产品可以为一个软件安装包，计算机包括客户端或服务器。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模式并不一定是本申请所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述的部分，可以参见其他实施例的相关描述。

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

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

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件程序模式的形式实现。

集成的单元如果以软件程序模式的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储器中。根据这样的理解，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全部或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器中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本申请各个实施例方法的全部或部分步骤。而前述的存储器包括：U 盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储器中，存储器可以包括：闪存盘、ROM、RAM、磁盘或光盘等。

以上对本申请实施例进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上，本说明书内容不应理解为对本申请的限制。

权利要求

1、一种信息交互方法，其特征在于，应用于客户端，所述方法包括：

所述客户端向服务器发送所述客户端预先设置的第一验证信息；

5 所述客户端按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；

所述客户端按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

所述客户端向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；

10 若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则所述客户端根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

2、根据权利要求1所述的方法，其特征在于，所述客户端按照预设令牌生成算法，对15 所述第一加密信息和所述第二加密信息进行生成，得到第一令牌，包括：

所述客户端按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；

所述客户端按照所述预设编码算法，对所述第三加密信息进行编码，得到第四加密信息；

20 所述客户端按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；

所述客户端按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌。

3、根据权利要求2所述的方法，其特征在于，所述第五加密信息包括多个字符，所述25 客户端按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌，包括：

所述客户端获取所述多个字符中每一字符对应的序号和数量；

所述客户端根据所述多个字符中每一字符的序列和数量获取所述字符对应的权值，得到多个权值；

30 所述客户端根据所述多个权值对所述多个字符中每一字符进行哈夫曼编码，得到所述第一令牌。

4、根据权利要求1-3任一项所述的方法，其特征在于，在所述客户端根据所述第一交互信息与所述服务器进行交互之后，所述方法还包括：

所述客户端对所述第一验证信息中的动态信息进行更新，得到第二验证信息；

所述客户端向所述服务器发送所述第二验证信息；

35 所述客户端按照所述预设编码算法，对所述第二验证信息进行编码，得到第六加密信息；

所述客户端按照所述预设令牌生成算法，对所述第六加密信息和所述第二加密信息进行生成，得到第二令牌；

40 所述客户端向所述服务器发送第二交互请求，所述第二交互请求包括所述第二令牌和第二交互信息；

若所述服务器确定第二待验证信息与所述第二验证信息匹配成功，则所述客户端根据所述第二交互信息与所述服务器进行交互，所述第二待验证信息由所述服务器按照所述预设编码算法对第二解密信息进行解码得到，所述第二解密信息由所述服务器按照所述预设

令牌生成算法对所述第二令牌进行拆分得到。

5、根据权利要求4所述的方法，其特征在于，所述客户端对所述第一验证信息中的动态信息进行更新，得到第二验证信息，包括：

所述客户端获取所述客户端向所述服务器发送所述第一交互请求的请求时间；

所述客户端将所述第一验证信息中的动态时间更新为所述请求时间，得到所述第二验证信息。

6、一种信息交互方法，其特征在于，应用于服务器，所述方法包括：

所述服务器接收客户端发送的所述客户端预先设置的第一验证信息；

所述服务器接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

所述服务器按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；

所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；

若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则所述服务器根据所述第一交互信息与所述客户端进行交互。

7、根据权利要求6所述的方法，其特征在于，所述服务器按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息，包括：

所述服务器按照预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息；

所述服务器按照预设组合算法，对所述第五解密信息进行拆分，得到第一解密信息、第二解密信息和第四解密信息；

所述服务器按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息，包括：

所述服务器按照所述预设编码算法，分别对所述第一解密信息、所述第二解密信息和所述第四解密信息进行解码，分别得到第一信息、第二信息和第三信息；

若所述第二信息与所述预设算法匹配成功，则所述服务器确定所述第二信息为所述第二待验证信息；

所述服务器按照预设组合算法，对所述第二信息和所述第一信息进行组合，得到第一组合信息，所述服务器按照所述预设组合算法，对所述第二信息和所述第三信息进行组合，得到第二组合信息；

若所述第一组合信息与所述第三信息匹配成功，则所述服务器确定所述第一信息为所述第一待验证信息。

8、根据权利要求7所述的方法，其特征在于，所述第一令牌包括多个字符，所述服务器按照预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息，包括：

所述服务器对所述多个字符中每一字符进行哈夫曼解码，以得到多个权值，每一权值对应一个字符；

所述服务器根据所述多个权值获取所述多个字符中每一字符的序列和数量；

所述服务器根据所述多个字符中每一字符的序列和数量获取所述第五解密信息。

9、一种信息交互装置，其特征在于，应用于客户端，所述装置包括：

通信单元，用于向服务器发送所述客户端预先设置的第一验证信息；

加密单元，用于按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

通信单元，还用于向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

10、根据权利要求 9 所述的装置，其特征在于，所述加密单元在按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌时，具体用于：

按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；

按照所述预设编码算法，对所述第三加密信息进行编码，得到第四加密信息；

按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；

按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌。

11、根据权利要求 10 所述的装置，其特征在于，所述第五加密信息包括多个字符，所述加密单元在按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌时，具体用于：

获取所述多个字符中每一字符对应的序号和数量；

根据所述多个字符中每一字符的序列和数量获取所述字符对应的权值，得到多个权值；

根据所述多个权值对所述多个字符中每一字符进行哈夫曼编码，得到所述第一令牌。

12、根据权利要求 9-11 任一项所述的装置，其特征在于，

所述加密单元，还用于在根据所述第一交互信息与所述服务器进行交互之后，对所述第一验证信息中的动态信息进行更新，得到第二验证信息；

所述通信单元，还用于向所述服务器发送所述第二验证信息；

所述加密单元，还用于按照所述预设编码算法，对所述第二验证信息进行编码，得到第六加密信息；按照所述预设令牌生成算法，对所述第六加密信息和所述第二加密信息进行生成，得到第二令牌；

所述通信单元，还用于向所述服务器发送第二交互请求，所述第二交互请求包括所述第二令牌和第二交互信息；若所述服务器确定第二待验证信息与所述第二验证信息匹配成功，根据所述第二交互信息与所述服务器进行交互，所述第二待验证信息由所述服务器按照所述预设编码算法对第二解密信息进行解码得到，所述第二解密信息由所述服务器按照所述预设令牌生成算法对所述第二令牌进行拆分得到。

13、根据权利要求 12 所述的装置，其特征在于，所述加密单元在对所述第一验证信息中的动态信息进行更新，得到第二验证信息时，具体用于：

获取向所述服务器发送所述第一交互请求的请求时间；

将所述第一验证信息中的动态时间更新为所述请求时间，得到所述第二验证信息。

14、一种信息交互装置，其特征在于，应用于服务器，所述装置包括：

通信单元，用于接收客户端发送的所述客户端预先设置的第一验证信息；接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述

第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

解密单元，用于按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述客户端进行交互。

15、根据权利要求 14 所述的装置，其特征在于，所述解密单元在按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息时，具体用于：

按照预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息；

按照预设组合算法，对所述第五解密信息进行拆分，得到第一解密信息、第二解密信息和第四解密信息；

所述解密单元在按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息时，具体用于：

按照所述预设编码算法，分别对所述第一解密信息、所述第二解密信息和所述第四解密信息进行解码，分别得到第一信息、第二信息和第三信息；

若所述第二信息与所述预设算法匹配成功，则确定所述第二信息为所述第二待验证信息；

按照预设组合算法，对所述第二信息和所述第一信息进行组合，得到第一组合信息，按照所述预设组合算法，对所述第二信息和所述第三信息进行组合，得到第二组合信息；

若所述第一组合信息与所述第三信息匹配成功，则确定所述第一信息为所述第一待验证信息。

16、根据权利要求 15 所述的装置，其特征在于，所述第一令牌包括多个字符，所述解密单元在按照预设缩短算法，对所述第一令牌进行延长处理，得到第五解密信息时，具体用于：

对所述多个字符中每一字符进行哈夫曼解码，以得到多个权值，每一权值对应一个字符；

根据所述多个权值获取所述多个字符中每一字符的序列和数量；

根据所述多个字符中每一字符的序列和数量获取所述第五解密信息。

17、一种信息交互装置，其特征在于，包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行以下步骤的指令：

向服务器发送预先设置的第一验证信息；

按照预设编码算法，分别对所述第一验证信息和预设算法进行编码，分别得到第一加密信息和第二加密信息；

按照预设令牌生成算法，对所述第一加密信息和所述第二加密信息进行生成，得到第一令牌；

向所述服务器发送第一交互请求，所述第一交互请求包括所述第一令牌和第一交互信息；

若所述服务器确定第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述服务器进行交互，所述第一待验证信息由所述服务器按照所述预设编码算法对第一解密信息进行解码得到，所述第一解密信息由所述服务器按照所述预设令牌生成算法对所述第一令牌进行拆分得到。

18、根据权利要求 17 所述的装置，其特征在于，在所述按照预设令牌生成算法，对所

述第一加密信息和所述第二加密信息进行生成，得到第一令牌时，所述程序具体包括用于执行以下步骤的指令：

按照预设组合算法，对所述第一加密信息和所述第二加密信息进行组合，得到第三加密信息；

5 按照所述预设编码算法，对所述第三加密信息进行编码，得到第四加密信息；

按照所述预设组合算法，对所述第一加密信息、所述第二加密信息和所述第四加密信息进行组合，得到第五加密信息；

按照预设缩短算法，对所述第五加密信息进行缩短处理，得到所述第一令牌。

10 19、一种信息交互装置，其特征在于，包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行以下步骤的指令：

接收客户端发送的所述客户端预先设置的第一验证信息；

15 接收所述客户端发送的第一交互请求，所述第一交互请求包括第一令牌和第一交互信息，所述第一令牌由所述客户端按照预设令牌生成算法对第一加密信息和第二加密信息进行生成得到，所述第一加密信息由所述客户端按照预设编码算法对所述第一验证信息进行编码得到，所述第二加密信息由所述客户端按照所述预设编码算法对预设算法进行编码得到；

按照所述预设令牌生成算法，对所述第一令牌进行拆分，得到第一解密信息和第二解密信息；

20 按照所述预设编码算法，分别对所述第一解密信息和所述第二解密信息进行解码，得到第一待验证信息和第二待验证信息；

若所述第二待验证信息与预设算法匹配成功，所述第一待验证信息与所述第一验证信息匹配成功，则根据所述第一交互信息与所述客户端进行交互。

25 20、一种计算机非易失性可读存储介质，其特征在于，所述计算机非易失性可读存储介质存储计算机程序，所述计算机程序使得计算机执行以实现权利要求 1-8 任一项所述的方法。

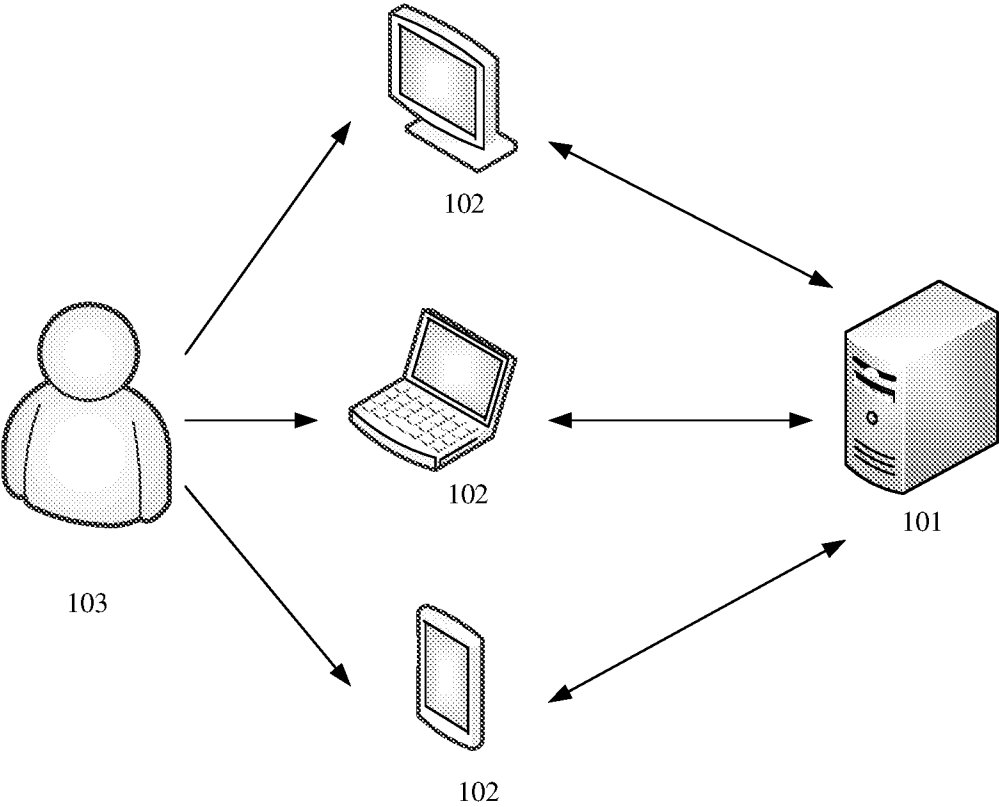


图 1

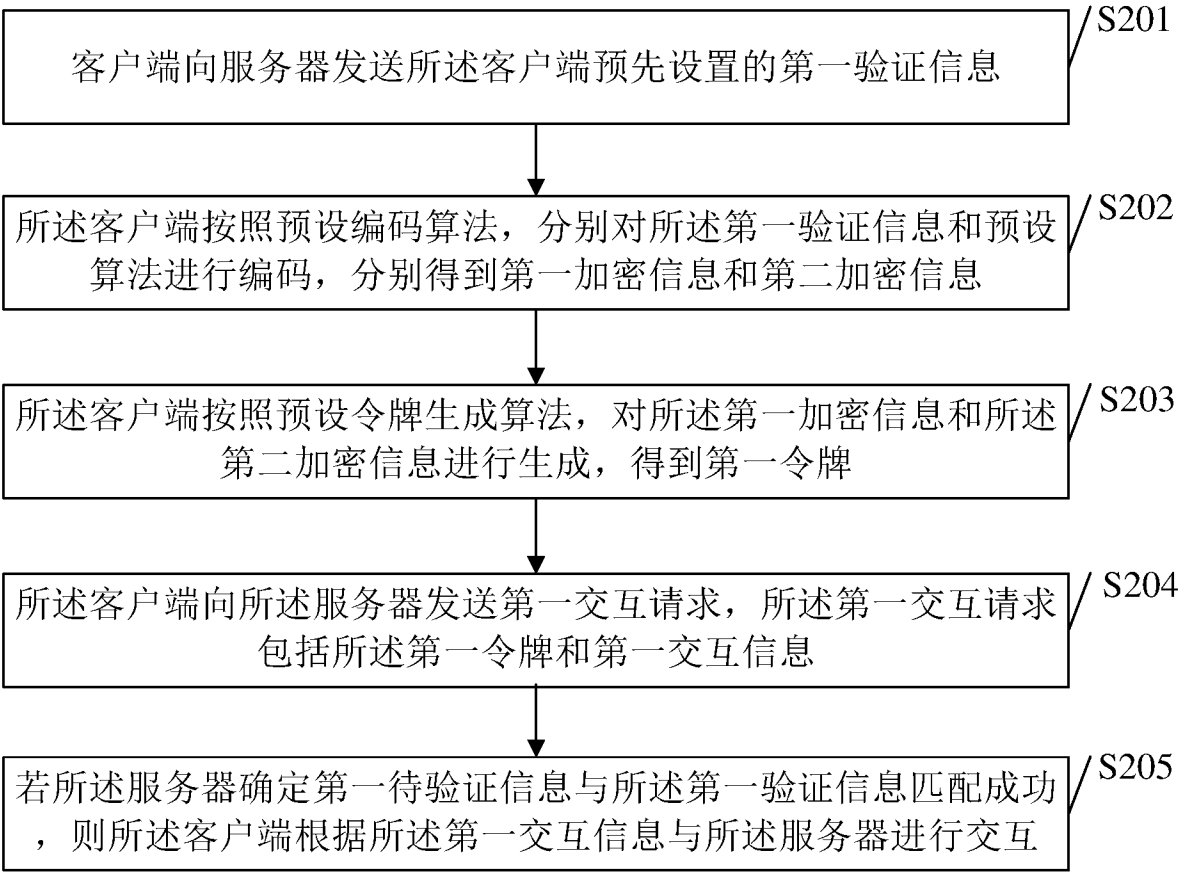


图 2

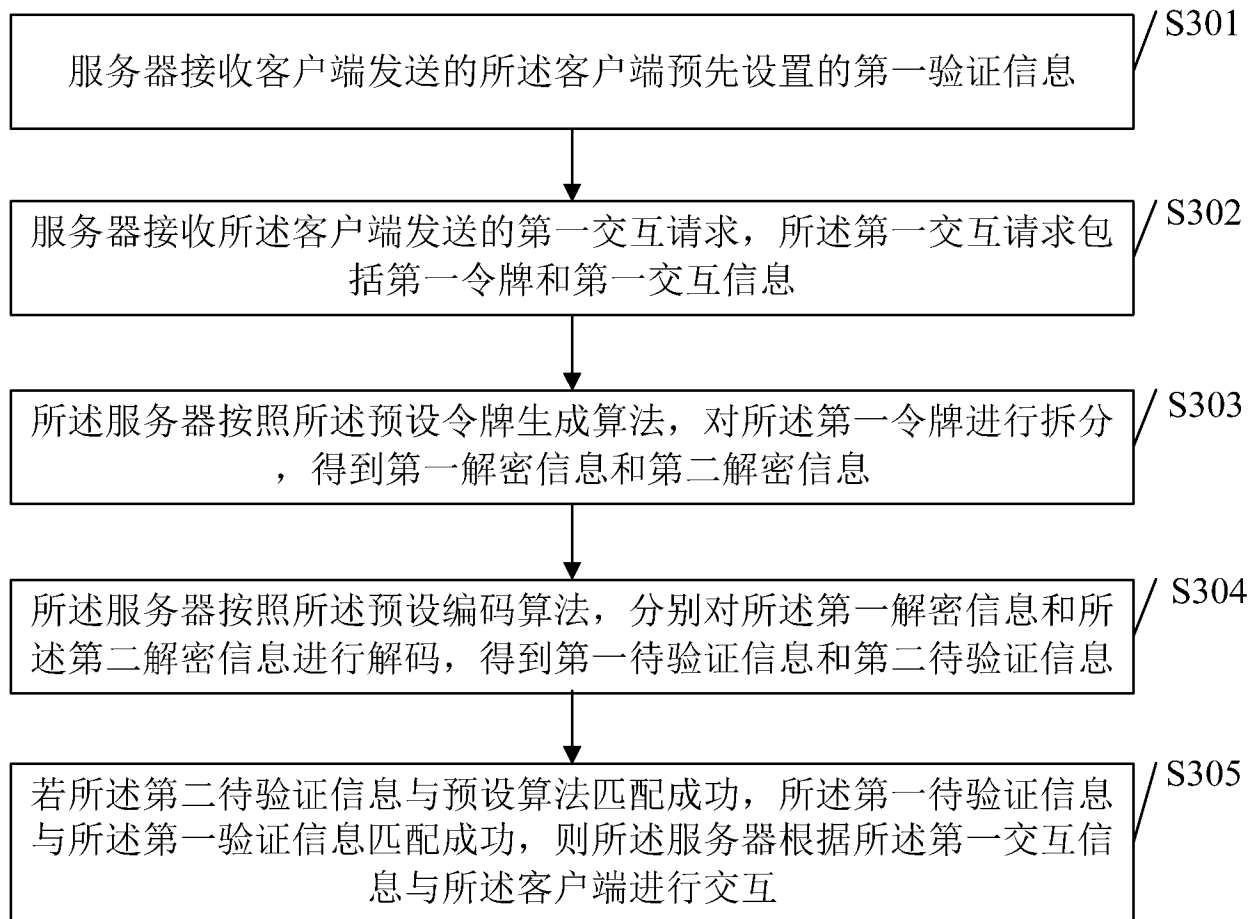


图 3

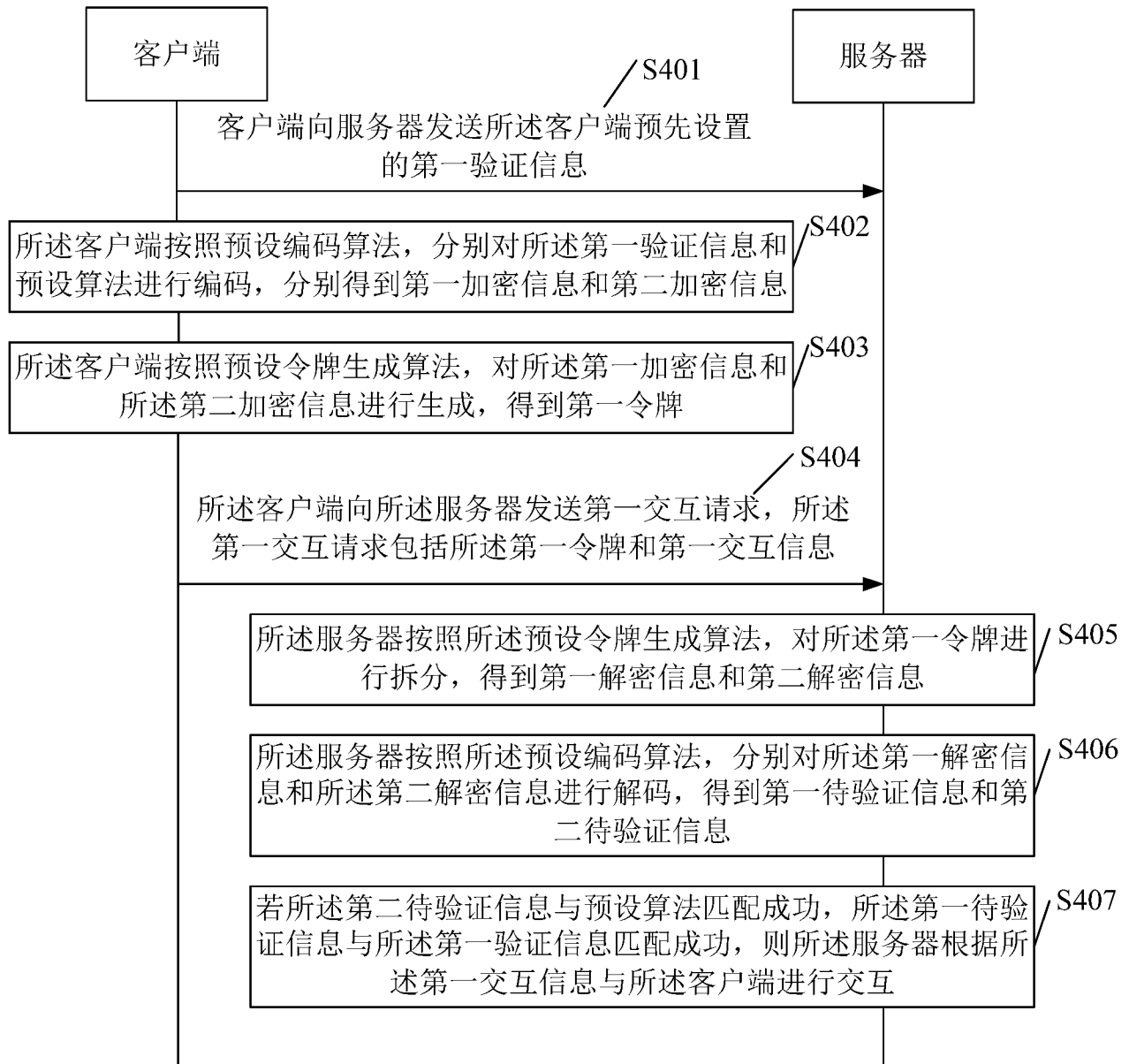


图 4

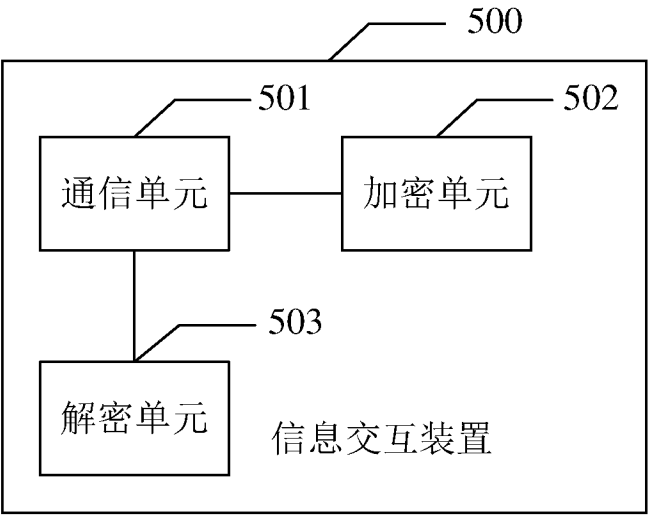


图 5

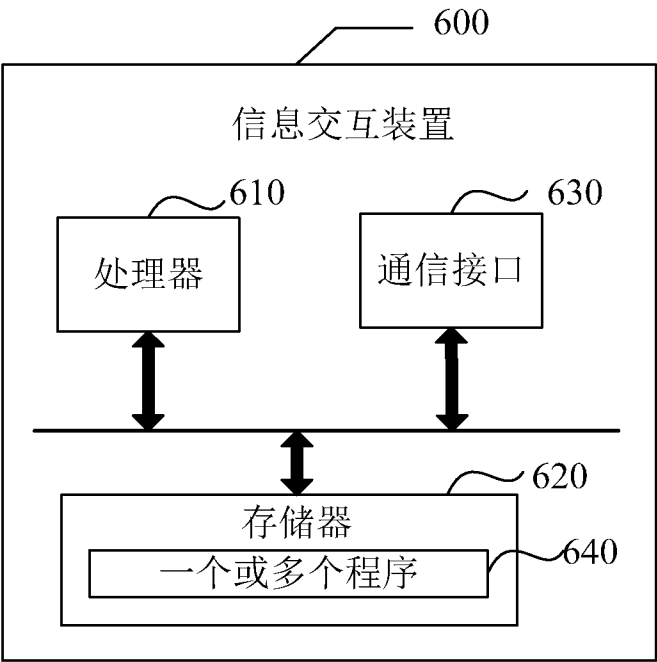


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/120084

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)n; H04L 9/08(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)

CNABS; CNTXT; DWPI; CNKI; EPTXT; WOTXT; USTXT: 交互, 会话, 连接, 访问, 请求, 令牌, 证书, 加密, 算法, 生成, 匹配, interact+, session, link, connect+, access, request+, token, certificat+, encrypt+, algorithm, generat+, match+, CPC: H04L9/3213, H04L63/0807

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110224999 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 10 September 2019 (2019-09-10) description, paragraphs 3-28	1-20
X	CN 104753953 A (CHENGDU SHUANG AOYANG TECHNOLOGY CO., LTD.) 01 July 2015 (2015-07-01) description, paragraphs 9-18, figure 1	1, 6, 9, 14, 17, 19-20
A	CN 106357409 A (CHINA UNIONPAY CO., LTD.) 25 January 2017 (2017-01-25) entire document	1-20
A	CN 109194484 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES) 11 January 2019 (2019-01-11) entire document	1-20
A	US 2015026468 A1 (WOWZA MEDIA SYSTEMS LLC.) 22 January 2015 (2015-01-22) entire document	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

18 January 2020

Date of mailing of the international search report

31 January 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
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/CN2019/120084

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110224999	A	10 September 2019	None			
CN	104753953	A	01 July 2015	None			
CN	106357409	A	25 January 2017	None			
CN	109194484	A	11 January 2019	None			
US	2015026468	A1	22 January 2015	US	9047482	B2	02 June 2015

国际检索报告

国际申请号

PCT/CN2019/120084

A. 主题的分类 H04L 29/06(2006.01)i; H04L 9/32(2006.01)n; H04L 9/08(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)) CNABS;CNTXT;DWPI;CNKI;EPTXT;WOTXT;USTXT: 交互, 会话, 连接, 访问, 请求, 令牌, 证书, 加密, 算法, 生成, 匹配, interact+, session, link, connect+, access, request+, token, certificat+, encrypt+, algorithm, generat+, match+, CPC: H04L9/3213, H04L63/0807																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 110224999 A (深圳壹账通智能科技有限公司) 2019年 9月 10日 (2019 - 09 - 10) 说明书第3-28段</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>CN 104753953 A (成都双奥阳科技有限公司) 2015年 7月 1日 (2015 - 07 - 01) 说明书第9-18段, 图1</td> <td>1, 6, 9, 14, 17, 19-20</td> </tr> <tr> <td>A</td> <td>CN 106357409 A (中国银联股份有限公司) 2017年 1月 25日 (2017 - 01 - 25) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 109194484 A (中国科学院信息工程研究所) 2019年 1月 11日 (2019 - 01 - 11) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2015026468 A1 (WOWZA MEDIA SYSTEMS LLC.) 2015年 1月 22日 (2015 - 01 - 22) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 110224999 A (深圳壹账通智能科技有限公司) 2019年 9月 10日 (2019 - 09 - 10) 说明书第3-28段	1-20	X	CN 104753953 A (成都双奥阳科技有限公司) 2015年 7月 1日 (2015 - 07 - 01) 说明书第9-18段, 图1	1, 6, 9, 14, 17, 19-20	A	CN 106357409 A (中国银联股份有限公司) 2017年 1月 25日 (2017 - 01 - 25) 全文	1-20	A	CN 109194484 A (中国科学院信息工程研究所) 2019年 1月 11日 (2019 - 01 - 11) 全文	1-20	A	US 2015026468 A1 (WOWZA MEDIA SYSTEMS LLC.) 2015年 1月 22日 (2015 - 01 - 22) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 110224999 A (深圳壹账通智能科技有限公司) 2019年 9月 10日 (2019 - 09 - 10) 说明书第3-28段	1-20																		
X	CN 104753953 A (成都双奥阳科技有限公司) 2015年 7月 1日 (2015 - 07 - 01) 说明书第9-18段, 图1	1, 6, 9, 14, 17, 19-20																		
A	CN 106357409 A (中国银联股份有限公司) 2017年 1月 25日 (2017 - 01 - 25) 全文	1-20																		
A	CN 109194484 A (中国科学院信息工程研究所) 2019年 1月 11日 (2019 - 01 - 11) 全文	1-20																		
A	US 2015026468 A1 (WOWZA MEDIA SYSTEMS LLC.) 2015年 1月 22日 (2015 - 01 - 22) 全文	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 2020年 1月 18日		国际检索报告邮寄日期 2020年 1月 31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		授权官员 蔡茹辛 电话号码 86-(010)-62089151																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/120084

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	110224999	A	2019年 9月 10日	无	
CN	104753953	A	2015年 7月 1日	无	
CN	106357409	A	2017年 1月 25日	无	
CN	109194484	A	2019年 1月 11日	无	
US	2015026468	A1	2015年 1月 22日	US 9047482 B2	2015年 6月 2日