

(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 6 月 2 日 (02.06.2022)



(10) 国际公布号
WO 2022/110968 A1

- (51) 国际专利分类号:
H04L 9/08 (2006.01)
- (21) 国际申请号: PCT/CN2021/117514
- (22) 国际申请日: 2021 年 9 月 9 日 (09.09.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202011356965.6 2020 年 11 月 27 日 (27.11.2020) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。
- (72) 发明人: 汤之雄(TANG, Zhixiong); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 沈玺(SHEN, Xi); 中国上海市浦东新区含

笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。
孔丽(KONG, Li); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 张怡(ZHANG, Yi); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 肖彦均(XIAO, Yanjun); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: 北京市中伦律师事务所 (ZHONG LUN LAW FIRM); 中国北京市朝阳区金和东路 20 号院正大中心南塔 24 层, Beijing 100020 (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, IT, 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,

(54) Title: DYNAMIC KEY GENERATION METHOD AND SYSTEM

(54) 发明名称: 一种动态密钥生成方法和系统

100

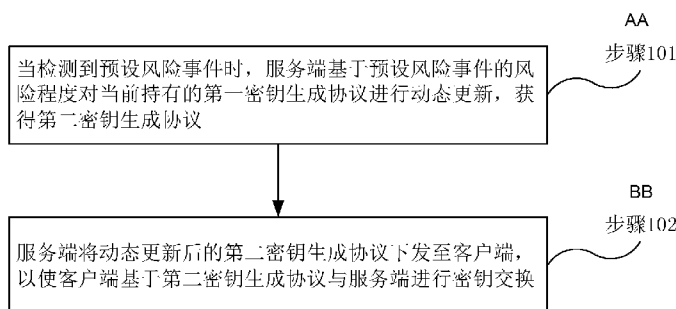


图 1

- AA Step 101: Upon detecting a preset risk event, a server dynamically updates, on the basis of a risk degree of the preset risk event, a first key generation protocol currently held by the server, so as to obtain a second key generation protocol
- BB Step 102: The server sends, to a client, the second key generation protocol obtained by means of the dynamic updating, such that the client and the server exchange keys on the basis of the second key generation protocol

(57) Abstract: The present invention provides a dynamic key generation method and system. The method comprises: upon detecting a preset risk event, dynamically updating, on the basis of a risk degree of the preset risk event, a first key generation protocol currently held by a server, so as to obtain a second key generation protocol; and the server sending, to a client, the second key generation protocol obtained by means of the dynamic updating, such that the client and the server exchange keys on the basis of the second key generation protocol. The method can increase the cost to attackers when cracking protocols, thereby achieving key security.



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)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

(57) 摘要: 本发明提供了一种动态密钥生成方法和系统, 该方法包括: 当检测到预设风险事件时, 基于预设风险事件的风险程度对服务端当前持有的第一密钥生成协议进行动态更新, 获得第二密钥生成协议; 服务端将动态更新后的第二密钥生成协议下发至客户端, 以使客户端基于第二密钥生成协议与服务端进行密钥交换。利用上述方法, 能够提高攻击者破解协议的成本, 提供密钥安全性。

一种动态密钥生成方法和系统

本申请要求于 2020 年 11 月 27 日提交的、申请号为 202011356965.6、标题为“一种动态密钥生成方法和系统”的中国专利申请的优先权，该中国专利申请的公开内容以引用的方式并入本文。

技术领域

本发明属于加密通讯领域，具体涉及一种动态密钥生成方法和系统。

背景技术

本部分旨在为权利要求书中陈述的本发明的实施方式提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

随着移动互联网的发展，应用程序呈现出爆炸式的增长，与此同时，互联网黑灰产业也随之诞生发展，规模达到了千亿元。互联网黑灰产业通过抓包、逆向分析等方式获取到客户端跟服务端通信的请求接口以及参数，直接伪造接口协议和参数来实现自动化操作，客户端与服务端之间的安全通讯受到了挑战。

传统技术中，出于对通讯安全的要求，市面上应用软件一般采取开源协议 TLS（Transport Layer Security，传输层安全性协议）握手方案。开源协议 TLS 握手方案能协助客户端与服务端选择连接时所使用的加密算法、MAC 算法及相关密钥。在传送应用程序的数据前，双方使用握手协议来完成上述事项。

然而，在上述开源协议 TLS 握手方案中，客户端需要预置一些公开的加密算法以及散列方法，因此客户端密钥生成算法固定不变，攻击者可以通过逆向破解客户端逻辑的获取这些固定的密钥生成算法，从而破解客户端与服务端之间的加密通讯，对通讯安全造成不利影响。

发明内容

针对上述现有技术中存在的问题，提出了一种动态密钥生成方法和系统，利用这种方法和系统，能够解决上述问题。

本发明提供了以下方案。

第一方面，提供一种动态密钥生成方法，包括：当检测到预设风险事件时，基于预设风险事件的风险程度对服务端当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议；服务端将动态更新后的第二密钥生成协议下发至客户端，以使客户端基于第二密钥生成协议与服务端进行密钥交换。

在一些实施方式中，服务端将动态更新后的第二密钥生成协议下发至客户端，方法还包括：服务端接收客户端上送的密钥交换请求，密钥交换请求包括客户端当前持有的密钥生成协议的版本号；当服务端检测到密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，服务端将动态更新后的第二密钥生成协议下发至客户端。

在一些实施方式中，服务端基于预设风险事件的风险程度对当前持有的第一密钥生成协议进行动态更新，还包括：

当检测到预设风险事件时，服务端使当前持有的第一密钥生成协议失效，并根据预设风险事件的风险程度生成对应安全级别的第二密钥生成协议；

其中，第二密钥生成协议包括预置的密钥算子层和协议主体，协议主体包括协议逻辑以及协议数据，协议逻辑用于指示第二密钥生成协议采用的一个或多个目标密钥算子的组成规则，协议数据用于指示一个或多个目标密钥算子的算子参数的。

在一些实施方式中，密钥算子层包含多个密钥算子且预置于服务端和客户端，并且密钥算子层中包含的多个密钥算子预先被划分为多个安全等级；以及，第二密钥生成协议的安全级别由采用的一个或多个目标密钥算子的安全等级确定。

在一些实施方式中，密钥算子层包含：采用安全加密算法的一种或多种密钥算子，和/或采用自定义变化算法的一种或多种密钥算子，和/或采用摘要算法的一种或多种密钥算子。

在一些实施方式中，方法还包括：采用白盒加密技术保护算子参数的安全性。

在一些实施方式中，预设风险事件至少包括风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；其中，第一预设风险事件用于指示连接至服务端的不可信客户端的数量占比超过预设阈值；第二预设风险事件用于指示接收外部发来的协议更新指令；第三预设风险事件用于指示服务端当前持有的第一密钥生成协议的工作时间超过预设安全时长。

在一些实施方式中，服务端连接至多个客户端，且客户端上送的密钥交换请求还包括设备指纹信息；方法还包括：服务端收集每个客户端上送的设备指纹信息，根据设备指纹信息判断每个客户端是否为不可信客户端，并周期性判断连接至服务端的不可信客户端的数量占比是否超过预设阈值，其中，若超过预设阈值，则检测到第一预设风险事件。

在一些实施方式中，预设风险事件还包括风险程度大于第一预设风险事件的第四预设风险事件；其中，第四预设风险事件用于指示服务端重复检测到多次第一预设风险事件。

在一些实施方式中，服务端将动态更新后的第二密钥生成协议下发至客户端，还包括：服务端将第二密钥生成协议的版本号下发至客户端；客户端向服务端发起协议更新请求，协议更新请求携带第二密钥生成协议的版本号；服务端向客户端下发第二密钥生成协议的协议逻辑和协议数据；客户端基于预置的密钥算子层、协议逻辑和协议数据，将第二密钥生成协议落地，并重新基于第二密钥生成协议向服务端发起密钥交换请求。

在一些实施方式中，服务端通过热更新方式向客户端下发第二密钥生成协议的协议逻辑。

在一些实施方式中，客户端基于第二密钥生成协议与服务端进行密钥交换，还包括：客户端向服务端发送密钥交换请求，密钥交换请求包括客户端当前持有的第二密钥生成协议的版本号；当服务端检测到密钥交换请求中携带的版本号与服务端当前持有的第二密钥生成协议的版本号一致时，生成服务端随机数，并将服务端随机数发送至客户端；客户端根据服务端随机数生成预主密钥，将预主密钥发送至服务端；客户端和服务端各自利用第二密钥生成协议、预主密钥、客户端随机数以及服务端随机数生成工作密钥；客户端和服务端通过交换各自生成的工作密钥进行加密通讯。

在一些实施方式中，方法还包括：客户端根据服务端随机数生成预主密钥之后，利用服务端下送的公钥对预主密钥进行加密，并将加密的预主密钥发送至服务端；服务端利用私钥对加密的预主密钥进行解密，得到解密的预主密钥。

第二方面，提供一种动态密钥生成系统，系统包括：服务端和客户端；其中，服务端用于执行：当检测到预设风险事件时，基于预设风险事件的风险程度对服务端当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议；将动态更新后的第二密钥生成协议下发至客户端；客户端用于执行：基于第二密钥生成协议与服务端进行密钥交换。

在一些实施方式中，服务端还用于：接收客户端上送的密钥交换请求，密钥交换请求包括客户端当前持有的密钥生成协议的版本号；当检测到密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，将动态更新后的第二密钥生成协议下发至客户端。

在一些实施方式中，服务端还用于：当检测到预设风险事件时，使当前持有的第一密钥生成协议失效，并根据预设风险事件的风险程度生成对应安全级别的第二密钥生成协议；其中，第二密钥生成协议包括预置的密钥算子层和协议主体，协议主体包括协议逻辑以及协议数据，协议逻辑用于指示第二密钥生成协议采用的一个或多个目标密钥算子的组成规则，协议数据用于指示一个或多个目标密钥算子的算子参数的。

在一些实施方式中，密钥算子层包含多个密钥算子且预置于服务端和客户端，并且密钥算子层中包含的多个密钥算子预先被划分为多个安全等级；以及，第二密钥生成协议的安全级别由采用的一个或多个目标密钥算子的安全等级确定。

在一些实施方式中，密钥算子层包含：采用安全加密算法的一种或多种密钥算子，和/或采用自定义变化算法的一种或多种密钥算子，和/或采用摘要算法的一种或多种密钥算子。

在一些实施方式中，系统还用于：采用白盒加密技术保护算子参数的安全性。

在一些实施方式中，预设风险事件至少包括风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；其中，第一预设风险事件用于指示连接至服务端的不可信客户端的数量占比超过预设阈值；第二预设风险事件用于指示接收外部发来的协议更新指令；第三预设风险事件用于指示服务端当前持有的第一密钥生成协议的工作时间超过预设安全时长。

在一些实施方式中，服务端连接至多个客户端，且客户端上送的密钥交换请求还包括设备指纹信息；服务端还用于：收集每个客户端上送的设备指纹信息，根据设备指纹信息判断每个客户端是否为不可信客户端，并周期性判断连接至服务端的不可信客户端的数量占比是否超过预设阈值，其中，若超过预设阈值，则检测到第一预设风险事件。

在一些实施方式中，预设风险事件还包括风险程度大于第一预设风险事件的第四预设风险事件；其中，第四预设风险事件用于指示服务端重复检测到多次第一预设风险事件。

在一些实施方式中，服务端还用于：当检测到密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，将第二密钥生成协议的版本号下发至客户端；客户端还用于：向服务端发起协议更新请求，协议更新请求携带第二密钥生成协议的版本号；服务端还用于：向客户端下发第二密钥生成协议的协议逻辑和协议数据；客户端还用于：基于预置的密钥算子层、协议逻辑和协议数据，将第二密钥生成协议落地，并重新基于第二密钥生成协议向服务端发起密钥交换请求。

在一些实施方式中，服务端通过热更新方式向客户端下发第二密钥生成协议的协议逻辑。

在一些实施方式中，客户端还用于：当基于第二密钥生成协议进行动态更新之后，向服务端发送密钥交换请求，密钥交换请求包括客户端当前持有的第二密钥生成协议的版本号；服务端还用于：当检测到密钥交换请求中携带的版本号与服务端当前持有的第二密钥生成协议的版本号一致时，生成服务端随机数，并将服务端随机数发送至客户端；客户端还用于：根据服务端随机数生成预主密钥，将预主密钥发送至服务端；客户端和服务端还用于：各自

利用第二密钥生成协议、预主密钥、客户端随机数以及服务端随机数生成工作密钥，通过交换各自生成的工作密钥进行加密通讯。

在一些实施方式中，客户端还用于：根据服务端随机数生成预主密钥之后，利用服务端下送的公钥对预主密钥进行加密，并将加密的预主密钥发送至服务端；服务端还用于：利用私钥对加密的预主密钥进行解密，得到解密的预主密钥。

第三方面，提供一种计算机可读存储介质，计算机可读存储介质存储有程序，当所述程序被处理器执行时，使得所述处理器执行如第一方面的方法。

本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：本实施例中，服务端可以基于预设风控机制而动态更新服务端持有的密钥生成协议并下发至客户端，客户端根据服务端下发的该动态更新的密钥生成协议与服务端进行密钥交换，从而提高攻击者破解协议的成本，提供密钥安全性。

应当理解，上述说明仅是本发明技术方案的概述，以便能够更清楚地了解本发明的技术手段，从而可依照说明书的内容予以实施。为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举例说明本发明的具体实施方式。

附图说明

通过阅读下文的示例性实施例的详细描述，本领域普通技术人员将明白本文所述的优点和益处以及其他优点和益处。附图仅用于示出示例性实施例的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的标号表示相同的部件。在附图中：

图 1 为根据本发明一实施例的动态密钥生成方法的流程示意图；

图 2 为根据本发明一实施例的密钥生成协议的示意图；

图 3 为根据本发明一实施例的动态密钥生成系统的示意图；

图 4 为根据本发明一实施例的更新密钥生成协议的时序示意图；

图 5 为根据本发明一实施例的生成动态密钥的时序示意图；

图 6 为根据本发明一实施例的动态密钥生成系统的示意图。

在附图中，相同或对应的标号表示相同或对应的部分。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。

相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

在本发明中，应理解，诸如“包括”或“具有”等术语旨在指示本说明书中所公开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不旨在排除一个或多个其他特征、数字、步骤、行为、部件、部分或其组合存在的可能性。

另外还需要说明的是，在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

针对现有技术方案的缺点，本发明实施例提出一种动态密钥生成方法，下面，首先对方法的发明构思进行介绍。

服务端对环境中的风险情况进行检测，当检测到预设风险事件时，基于该预设风险事件的风险程度对当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议。基于此，服务端将动态更新后的第二密钥生成协议下发至客户端，以使客户端基于第二密钥生成协议与服务端进行密钥交换。换言之，服务端可以基于预设风控机制而动态更新服务端持有的密钥生成协议，并下发至客户端，客户端和服务端基于动态更新的密钥生成协议进行数据交换，从而提高攻击者破解协议的成本，提高通信安全性能。

本领域技术人员可以理解，所描述的应用场景仅是本发明的实施方式可以在其中得以实现的一个示例。本发明实施方式的适用范围不受任何限制。在介绍了本发明的基本原理之后，下面具体介绍本发明的各种非限制性实施方式。

图1为根据本申请一实施例的动态密钥生成方法100的流程示意图。

如图1所示，该方法100可以包括步骤101和步骤102。

步骤101、当检测到预设风险事件时，服务端基于预设风险事件的风险程度对当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议。

其中，该预设风险事件是指可能对服务端和客户端当前持有的密钥生成协议的安全性造成风险的事件。例如，该预设风险事件可以是连接至服务端的客户端为不可信客户端，还可以是当前持有的密钥生成协议的工作时间超过安全时长阈值，诸如此类。

在一种可能的实施方式中，在上述步骤101中，服务端基于预设风险事件的风险程度对当前持有的第一密钥生成协议进行动态更新还可以包括：当检测到预设风险事件时，服务端使当前持有的第一密钥生成协议失效，并根据预设风险事件的风险程度生成对应安全级别的第二密钥生成协议。

可以理解，基于在先经验、历史统计数据等风险程度判断因素，可以将多种类型的预设风险事件按照风险程度分为多个级别，比如检测到的某一预设风险事件指示当前持有的密钥

生成协议已被攻破时，则可以认为该预设风险事件为一级风险事件。又比如检测到的另一预设风险事件指示当前持有的密钥生成协议可能存在被攻破风险时，则可以认为该预设风险事件为二级风险事件。又比如检测到的预设风险事件指示当前持有的密钥生成协议的工作时间已经超过安全时长阈值，则可以认为该预设风险事件为三级风险事件，诸如此类。基于此，可以生成安全级别对应于该风险程度的第二密钥生成协议，从而持续提高攻击者破解密钥生成协议的成本。

其中，第二密钥生成协议包括预置的密钥算子层和协议主体，协议主体包括协议逻辑以及协议数据，协议逻辑用于指示第二密钥生成协议采用的一个或多个目标密钥算子的组成规则，协议数据用于指示一个或多个目标密钥算子的算子参数。

具体来说，在服务端和客户端均预置包含多种密钥算子的密钥算子层。可选地，密钥算子层包含：采用诸如 AES、SM4 的安全加密算法的一种或多种密钥算子，和/或采用诸如矩阵乘法算法、大数取余算法的自定义变化算法的一种或多种密钥算子，和/或采用诸如 SHA256、SM3 的摘要算法的一种或多种密钥算子。

举例来说，图 2 示出一种密钥生成协议的示例，其包含预置的密钥算子层和动态生成的协议主体，其中预置的密钥算子层包含 AES 变换算子、矩阵变换算子和 SHA 变换算子等密钥算子等。动态生成的协议主体部分包括逻辑区和数据区，逻辑区包括协议逻辑，其用于指示该密钥生成协议所采用目标密钥算子的组成规则与顺序，该部分内容可通过热更新的方式下发至客户端。数据区包含密钥算子层中各级密钥算子的算子参数。可选地，其中一些密钥算子的算子参数可以是白盒数据，另外一些密钥算子的算子参数可以是明文参数。

在一种可能的实施方式中，密钥算子层包含多个密钥算子且同时预置于服务端和客户端，并且密钥算子层中包含的多个密钥算子预先被划分为多个安全等级；以及，第二密钥生成协议的安全级别由采用的一个或多个目标密钥算子的安全等级确定。

举例来说，可以按照各个密钥算子的变换安全性将密钥算子层中的多种密钥算子分为一级算子、二级算子、三级算子。其中，一级算子可表示安全等级最高的算子，接受密钥因子和算子参数作为输入，采用诸如 AES 算法、SM4 算法等安全加密算法来保护变换结果的安全性。二级算子可表示安全等级仅次于一级的算子，其接受密钥因子和算子参数作为输入，并采用诸如矩阵乘法算法、大数取余算法等自定义变化算法来保护变换结果的安全性。二级算子相较于一级算子具有更简单的算法，对客户端的性能要求更低。可选地，可采用白盒技术保护一级算子和二级算子的算子参数的安全性。三级算子可表示安全等级较弱的算子，其接受密钥因子和算子参数作为输入，可采用先用的摘要算法保护变换结果的安全性，其中摘要算法的算子参数为摘要算法的盐，摘要算法比如可以是 SHA256、SM3 等。三级算子算法相较

于一、二级算子则更为简单，对客户端性能要求更低。基于此，可以理解，当第二密钥生成协议采用一级算子作为目标密钥算子，相较于采用二级算子具有更高的安全等级。当第二密钥生成协议组合采用一、二级算子作为目标密钥算子，相较于单独采用一级算子具有更高的安全等级。因此可以由采用的一个或多个目标密钥算子的安全等级确定第二密钥生成协议的安全级别，并根据检测到的预设风险事件的风险程度生成对应安全级别的第二密钥生成协议。

在一种可能的实施方式中，方法还包括：采用白盒加密技术保护算子参数的安全性。

举例来说，参考图 2，其中的 AES 变换算子和矩阵变换算子的算子参数采用白盒数据形式保存。

在一种可能的实施方式中，预设风险事件至少包括风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；该第一预设风险事件可以用于指示连接至服务端的不可信客户端的数量占比超过预设阈值；第二预设风险事件用于指示接收外部发来的协议更新指令；第三预设风险事件用于指示服务端当前持有的第一密钥生成协议的工作时间超过预设安全时长。

举例来说，参考图 3，可以在服务端设置风控模块，该风控模块设置有多个风险驱动单元，比如第一风险驱动单元、第二风险驱动单元和第三风险驱动单元。基于此，比如，第一风险驱动单元检测到第一预设风险事件发生时，也即检测到连接至服务端的不可信客户端的数量占比超过预设阈值时，驱动强制更新该服务端当前持有的第一密钥生成协议，动态更新后的第二密钥生成协议可以由 AES 算子（一级算子）、矩阵变化算子（二级算子）和 SHA 变换算子（三级算子）组合参与。可选地，若第一风险驱动单元检测到第一预设风险事件重复发生时，则更新后的第二密钥生成协议可以包含增加数量的 AES 变换算子。又比如，在业务方需要上线安全性要求较高的业务之前，向服务端发送协议更新指令（即发生该第二预设风险事件），第二风险驱动单元检测到第二预设风险事件发生，驱动强制更新该服务端当前持有的第一密钥生成协议，动态更新后的第二密钥生成协议可以由矩阵变化算子（二级算子）和 SHA 变换算子（三级算子）组合参与。又比如，第一密钥生成协议的工作时间超过预设安全时长（即发生该第三预设风险事件），第三风险驱动单元检测到该第三预设风险事件，驱动强制更新该服务端当前持有的第一密钥生成协议，动态更新后的第二密钥生成协议可以由 SHA 变换算子（三级算子）参与。可以看出，第一预设风险事件、第二预设风险事件和第三预设风险事件的风险程度依次递减，动态更新后生成的第二密钥生成协议的安全级别也相应依次递减。

在一种可能的实施方式中，服务端连接至多个客户端，且客户端上送的密钥交换请求还包括设备指纹信息；方法还包括：服务端收集每个客户端上送的设备指纹信息，根据设备指

纹信息判断每个客户端是否为不可信客户端，并周期性判断连接至服务端的不可信客户端的数量占比是否超过预设阈值，其中，若超过预设阈值，则检测到第一预设风险事件。

在一种可能的实施方式中，预设风险事件还包括风险程度大于第一预设风险事件的第四预设风险事件；其中，第四预设风险事件用于指示服务端检测到重复多次的第一预设风险事件。举例来说，当检测到第一预设风险事件重复多次发生时，驱动强制更新该服务端当前持有的第一密钥生成协议，动态更新后的第二密钥生成协议可以由多个 AES 算子（一级算子）、矩阵变化算子（二级算子）和 SHA 变换算子（三级算子）组合参与。由此具有更高的安全级别。

步骤 102、服务端将动态更新后的第二密钥生成协议下发至客户端，以使客户端基于第二密钥生成协议与服务端进行密钥交换。

在一种可能的实施方式中，步骤 102 中的服务端将动态更新后的第二密钥生成协议下发至客户端，还包括：服务端接收客户端上送的密钥交换请求，密钥交换请求包括客户端当前持有的密钥生成协议的版本号；当服务端判断密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，服务端将动态更新后的第二密钥生成协议下发至客户端。

相反，当服务端判断客户端上送的密钥交换请求携带的版本号与第二密钥生成协议的版本号一致时，则说明客户端和服务端的密钥生成协议是一致的，则服务端无需进一步向客户端下发其持有的第二密钥生成协议。

在一种可能的实施方式中，上述服务端将动态更新后的第二密钥生成协议下发至客户端，还可以进一步包括：服务端将第二密钥生成协议的版本号下发至客户端；客户端向服务端发起协议更新请求，协议更新请求携带第二密钥生成协议的版本号；服务端向客户端下发对应于第二密钥生成协议的协议逻辑和协议数据；客户端基于预置的密钥算子层、协议逻辑和协议数据，将第二密钥生成协议落地，并重新基于第二密钥生成协议向服务端发起密钥交换请求。

在一种可能的实施方式中，服务端通过热更新方式向客户端下发第二密钥生成协议的协议逻辑。

举例来说，参考图 3，服务端向客户端下发的协议逻辑是热更新 JS 文件，客户端在接收到该热更新 JS 文件之后转为热更新模块，并进一步结合接收到的协议数据、预置的密钥算子层生成更新后的第二密钥生成协议。

图 4 示出对服务端和客户端持有的密钥生成协议依次进行更新的流程示意图。参考图 3，图 4 所示出客户端和服务端之间的通信均是通过图 3 中的安全通讯模块而实现的。

S41、服务端将当前持有的第一密钥生成协议置为失效状态，同时生成第二密钥生成协议、热更新补丁以及白盒跳转表。

S42、客户端生成客户端随机数。其中，上述 S41 可以在 S42 之前或之后，本申请对此不作具体限制。

S43、客户端向服务端发起密钥交换请求，密钥交换请求包括：客户端当前持有的密钥生成协议的版本号、客户端随机数以及设备指纹信息。

S44、服务端收到密钥交换请求，判断密钥交换请求携带的版本号已过期，则终止当前密钥交换请求。

S45、将动态更新后持有的第二密钥生成协议的版本号和证书下发至客户端。

S46、客户端收到对接收的证书进行验证。

S47、客户端在证书验证通过之后向服务端发起协议更新请求，该协议更新请求携带该第二密钥生成协议的版本号且用于请求热更新文件以及白盒跳转表。

S48、服务端根据客户端上送的版本号，下发第二密钥生成协议对应的热更新 js 文件（例如，通过协议逻辑模块）以及算子参数（例如，通过协议数据模块）。

S49、客户端收到热更新 js 文件和算子参数后，基于预置的密钥算子层执行热更新，并存储第二密钥生成协议的版本号、热更新文件以及白盒跳转表。

S50、客户端和服务端基于当前持有的第二密钥生成协议进行密钥交换。

在一种可能的实施方式中，客户端基于第二密钥生成协议与服务端进行密钥交换，还包括：客户端向服务端发送密钥交换请求，密钥交换请求包括客户端当前持有的第二密钥生成协议的版本号；当服务端检测到密钥交换请求中携带的版本号与服务端当前持有的第二密钥生成协议的版本号一致时，生成服务端随机数，并将服务端随机数发送至客户端；客户端根据服务端随机数生成预主密钥，将预主密钥发送至服务端；客户端和服务端各自利用第二密钥生成协议、预主密钥、客户端随机数以及服务端随机数生成工作密钥；客户端和服务端通过交换各自生成的工作密钥进行加密通讯。

在一种可能的实施方式中，方法还包括：客户端根据服务端随机数生成预主密钥之后，利用服务端下送的公钥对预主密钥进行加密，并将加密的预主密钥发送至服务端；服务端利用私钥对加密的预主密钥进行解密，得到解密的预主密钥。

举例来说，客户端与服务端同时持有动态更新后的第二密钥生成协议后，服务端和客户端通过基于该第二密钥生成协议各自生成最终的工作密钥（Skey），具体密钥生成工作过程如图 5 所示，包括：

S51、客户端生成客户端随机数（cliRand）。

S52、客户端向服务端发起密钥交换请求，上送客户端随机数、协议版本号、以及设备信息。

S53、服务端收到客户端请求信息后，判断协议版本号为最新版本号，生成服务端随机数(srvRand)。

S54、服务端将服务端随机数(srvRand)、第二密钥生成协议的版本号、证书下发至客户端。

S55、客户端收到服务端随机数后，对证书进行验证。

S56、客户端在证书验证通过之后生成预主密钥(preMasterKey)，并用服务端下发的公钥加密预主密钥。

S57、客户端将加密的预主密钥上送至服务端。

S58、客户端利用当前持有的第二密钥生成协议，并根据预主密钥、服务端随机数、客户端随机数生成工作密钥。其中，S57可以在S58之前或之后执行，本申请对此不作具体限制。

S59、服务端收到加密的预主密钥后，用私钥解密预主密钥，并使用当前持有的第二密钥生成协议，并根据预主密钥、服务端随机数、客户端随机数生成工作密钥。

S60、客户端和服务端同时持有工作密钥，后续业务报文可以进行密钥加密通讯。

参考图3，在S60之前，上述客户端和服务端之间的通信均是通过客户端和服务端的安全通讯模块而实现的，其中，密钥因子包括预主密钥、服务端随机数、客户端随机数。S60之后，通过客户端和服务器的业务报文加密模块进行加密之后进行密钥加密通讯。

基于相同的技术构思，本发明实施例还提供一种动态密钥生成系统，用于执行上述任一实施例所提供的动态密钥生成方法。图6为本发明实施例提供的一种动态密钥生成系统的结构示意图。

如图6所示，系统600包括：服务端601和客户端602。其中，服务端用于执行：当检测到预设风险事件时，基于预设风险事件的风险程度对服务端当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议；将动态更新后的第二密钥生成协议下发至客户端；客户端用于执行：基于第二密钥生成协议与服务端进行密钥交换。

在一些实施方式中，服务端还用于：接收客户端上送的密钥交换请求，密钥交换请求包括客户端当前持有的密钥生成协议的版本号；当检测到密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，将动态更新后的第二密钥生成协议下发至客户端。

在一些实施方式中，服务端还用于：当检测到预设风险事件时，使当前持有的第一密钥生成协议失效，并根据预设风险事件的风险程度生成对应安全级别的第二密钥生成协议；其

中，第二密钥生成协议包括预置的密钥算子层和协议主体，协议主体包括协议逻辑以及协议数据，协议逻辑用于指示第二密钥生成协议采用的一个或多个目标密钥算子的组成规则，协议数据用于指示一个或多个目标密钥算子的算子参数的。

在一些实施方式中，密钥算子层包含多个密钥算子且预置于服务端和客户端，并且密钥算子层中包含的多个密钥算子预先被划分为多个安全等级；以及，第二密钥生成协议的安全级别由采用的一个或多个目标密钥算子的安全等级确定。

在一些实施方式中，密钥算子层包含：采用安全加密算法的一种或多种密钥算子，和/或采用自定义变化算法的一种或多种密钥算子，和/或采用摘要算法的一种或多种密钥算子。

在一些实施方式中，系统还用于：采用白盒加密技术保护算子参数的安全性。

在一些实施方式中，预设风险事件至少包括风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；其中，第一预设风险事件用于指示连接至服务端的不可信客户端的数量占比超过预设阈值；第二预设风险事件用于指示接收外部发来的协议更新指令；第三预设风险事件用于指示服务端当前持有的第一密钥生成协议的工作时间超过预设安全时长。

在一些实施方式中，服务端连接至多个客户端，且客户端上送的密钥交换请求还包括设备指纹信息；服务端还用于：收集每个客户端上送的设备指纹信息，根据设备指纹信息判断每个客户端是否为不可信客户端，并周期性判断连接至服务端的不可信客户端的数量占比是否超过预设阈值，其中，若超过预设阈值，则检测到第一预设风险事件。

在一些实施方式中，预设风险事件还包括风险程度大于第一预设风险事件的第四预设风险事件；其中，第四预设风险事件用于指示服务端重复检测到多次第一预设风险事件。

在一些实施方式中，服务端还用于：当检测到密钥交换请求携带的版本号与第二密钥生成协议的版本号不一致时，将第二密钥生成协议的版本号下发至客户端；客户端还用于：向服务端发起协议更新请求，协议更新请求携带第二密钥生成协议的版本号；服务端还用于：向客户端下发第二密钥生成协议的协议逻辑和协议数据；客户端还用于：基于预置的密钥算子层、协议逻辑和协议数据，将第二密钥生成协议落地，并重新基于第二密钥生成协议向服务端发起密钥交换请求。

在一些实施方式中，服务端通过热更新方式向客户端下发第二密钥生成协议的协议逻辑。

在一些实施方式中，客户端还用于：当基于第二密钥生成协议进行动态更新之后，向服务端发送密钥交换请求，密钥交换请求包括客户端当前持有的第二密钥生成协议的版本号；服务端还用于：当检测到密钥交换请求中携带的版本号与服务端当前持有的第二密钥生成协议的版本号一致时，生成服务端随机数，并将服务端随机数发送至客户端；客户端还用于：

根据服务端随机数生成预主密钥，将预主密钥发送至服务端；客户端和服务端还用于：各自利用第二密钥生成协议、预主密钥、客户端随机数以及服务端随机数生成工作密钥，通过交换各自生成的工作密钥进行加密通讯。

在一些实施方式中，客户端还用于：根据服务端随机数生成预主密钥之后，利用服务端下送的公钥对预主密钥进行加密，并将加密的预主密钥发送至服务端；服务端还用于：利用私钥对加密的预主密钥进行解密，得到解密的预主密钥。

需要说明的是，本申请实施例中的系统可以实现前述方法的实施例的各个过程，并达到相同的效果和功能，这里不再赘述。

提供一种计算机可读存储介质，计算机可读存储介质存储有程序，当所述程序被处理器执行时，使得所述处理器执行如前述实施例的各个过程，并达到相同的效果和功能。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。此外，尽管在附图中以特定顺序描述了本发明方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示的操作才能实现期望的结果。附加地或备选地，可以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个步骤执行。

虽然已经参考若干具体实施方式描述了本发明的精神和原理，但是应该理解，本发明并不限于所公开的具体实施方式，对各方面的划分也不意味着这些方面中的特征不能组合以进行受益，这种划分仅是为了表述的方便。本发明旨在涵盖所附权利要求的精神和范围内所包括的各种修改和等同布置。

权 利 要 求 书

1、一种动态密钥生成方法，其特征在于，所述方法包括：

当检测到预设风险事件时，基于所述预设风险事件的风险程度对所述服务端当前持有的

5 第一密钥生成协议进行动态更新，获得第二密钥生成协议；

所述服务端将动态更新后的所述第二密钥生成协议下发至客户端，以使所述客户端基于
所述第二密钥生成协议与所述服务端进行密钥交换。

2、根据权利要求 1 所述的方法，其特征在于，所述服务端将动态更新后的所述第二密
钥生成协议下发至客户端，所述方法还包括：

10 所述服务端接收所述客户端上送的密钥交换请求，所述密钥交换请求包括所述客户端当
前持有的密钥生成协议的版本号；

当所述服务端检测到所述密钥交换请求携带的版本号与所述第二密钥生成协议的版本
号不一致时，所述服务端将动态更新后的所述第二密钥生成协议下发至所述客户端。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述服务端基于所述预设风险事件
15 的风险程度对当前持有的第一密钥生成协议进行动态更新，还包括：

当检测到所述预设风险事件时，所述服务端使当前持有的所述第一密钥生成协议失效，
并根据所述预设风险事件的风险程度生成对应安全级别的第二密钥生成协议；

其中，所述第二密钥生成协议包括预置的密钥算子层和协议主体，所述协议主体包括协
议逻辑以及协议数据，所述协议逻辑用于指示所述第二密钥生成协议采用的一个或多个目标
20 密钥算子的组成规则，所述协议数据用于指示所述一个或多个目标密钥算子的算子参数。

4、根据权利要求 3 所述的方法，其特征在于，所述密钥算子层包含多个密钥算子且预
置于所述服务端和所述客户端，并且所述密钥算子层中包含的多个密钥算子预先被划分为多
个安全等级；以及，所述第二密钥生成协议的安全级别由采用的所述一个或多个目标密钥算
子的安全等级确定。

25 5、根据权利要求 4 所述的方法，其特征在于，

所述密钥算子层包含：采用安全加密算法的一种或多种密钥算子，和/或采用自定义变
化算法的一种或多种密钥算子，和/或采用摘要算法的一种或多种密钥算子。

6、根据权利要求 3-5 中任一项所述的方法，其特征在于，所述方法还包括：采用白盒
加密技术保护所述算子参数的安全性。

30 7、根据权利要求 3-6 中任一项所述的方法，其特征在于，所述预设风险事件至少包括
风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；其中，

所述第一预设风险事件用于指示连接至所述服务端的不可信客户端的数量占比超过预设阈值；

所述第二预设风险事件用于指示接收外部发来的协议更新指令；

5 所述第三预设风险事件用于指示所述服务端当前持有的所述第一密钥生成协议的工作时间超过预设安全时长。

8、根据权利要求 7 所述的方法，其特征在于，所述服务端连接至多个所述客户端，且所述客户端上送的所述密钥交换请求还包括设备指纹信息；所述方法还包括：

10 所述服务端收集每个所述客户端上送的所述设备指纹信息，根据所述设备指纹信息判断每个所述客户端是否为不可信客户端，并周期性判断连接至所述服务端的所述不可信客户端的数量占比是否超过所述预设阈值，其中，若超过所述预设阈值，则检测到所述第一预设风险事件。

9、根据权利要求 7 或 8 所述的方法，其特征在于，所述预设风险事件还包括风险程度大于所述第一预设风险事件的第四预设风险事件；其中，

所述第四预设风险事件用于指示所述服务端重复检测到多次所述第一预设风险事件。

15 10、根据权利要求 3-9 中任一项所述的方法，其特征在于，所述服务端将动态更新后的所述第二密钥生成协议下发至客户端，还包括：

所述服务端将所述第二密钥生成协议的版本号下发至所述客户端；

所述客户端向所述服务端发起协议更新请求，所述协议更新请求携带所述第二密钥生成协议的版本号；

20 所述服务端向所述客户端下发所述第二密钥生成协议的所述协议逻辑和所述协议数据；

所述客户端基于预置的密钥算子层、所述协议逻辑和所述协议数据，将所述第二密钥生成协议落地，并重新基于所述第二密钥生成协议向所述服务端发起所述密钥交换请求。

11、根据权利要求 10 所述的方法，其特征在于，所述服务端通过热更新方式向所述客户端下发所述第二密钥生成协议的协议逻辑。

25 12、根据权利要求 1-11 中任一项所述的方法，其特征在于，所述客户端基于所述第二密钥生成协议与所述服务端进行密钥交换，还包括：

所述客户端向所述服务端发送密钥交换请求，所述密钥交换请求包括所述客户端当前持有的所述第二密钥生成协议的版本号；

30 当所述服务端检测到所述密钥交换请求中携带的版本号与所述服务端当前持有的所述第二密钥生成协议的版本号一致时，生成服务端随机数，并将所述服务端随机数发送至所述客户端；

所述客户端根据所述服务端随机数生成预主密钥，将所述预主密钥发送至所述服务端；

所述客户端和所述服务端各自利用所述第二密钥生成协议、所述预主密钥、所述客户端随机数以及所述服务端随机数生成工作密钥；

所述客户端和所述服务端通过交换各自生成的所述工作密钥进行加密通讯。

5 13、根据权利要求 12 所述的方法，其特征在于，所述方法还包括：

所述客户端根据所述服务端随机数生成所述预主密钥之后，利用所述服务端下送的公钥对所述预主密钥进行加密，并将加密的所述预主密钥发送至所述服务端；

所述服务端利用私钥对加密的所述预主密钥进行解密，得到解密的所述预主密钥。

14、一种动态密钥生成系统，其特征在于，所述系统包括：服务端和客户端；其中，

10 所述服务端用于执行：当检测到预设风险事件时，基于所述预设风险事件的风险程度对所述服务端当前持有的第一密钥生成协议进行动态更新，获得第二密钥生成协议；将动态更新后的所述第二密钥生成协议下发至客户端；

所述客户端用于执行：基于所述第二密钥生成协议与所述服务端进行密钥交换。

15、根据权利要求 14 所述的系统，其特征在于，

15 所述服务端还用于：接收所述客户端上送的密钥交换请求，所述密钥交换请求包括所述客户端当前持有的密钥生成协议的版本号；当检测到所述密钥交换请求携带的版本号与所述第二密钥生成协议的版本号不一致时，将动态更新后的所述第二密钥生成协议下发至所述客户端。

16、根据权利要求 14 或 15 所述的系统，其特征在于，

20 所述服务端还用于：当检测到所述预设风险事件时，使当前持有的所述第一密钥生成协议失效，并根据所述预设风险事件的风险程度生成对应安全级别的第二密钥生成协议；

其中，所述第二密钥生成协议包括预置的密钥算子层和协议主体，所述协议主体包括协议逻辑以及协议数据，所述协议逻辑用于指示所述第二密钥生成协议采用的一个或多个目标密钥算子的组成规则，所述协议数据用于指示所述一个或多个目标密钥算子的算子参数的。

25 17、根据权利要求 16 所述的系统，其特征在于，所述密钥算子层包含多个密钥算子且预置于所述服务端和所述客户端，并且所述密钥算子层中包含的多个密钥算子预先被划分为多个安全等级；以及，所述第二密钥生成协议的安全级别由采用的所述一个或多个目标密钥算子的安全等级确定。

18、根据权利要求 17 所述的系统，其特征在于，

30 所述密钥算子层包含：采用安全加密算法的一种或多种密钥算子，和/或采用自定义变化算法的一种或多种密钥算子，和/或采用摘要算法的一种或多种密钥算子。

19、根据权利要求 16-18 中任一项所述的系统，其特征在于，

所述系统还用于：采用白盒加密技术保护所述算子参数的安全性。

20、根据权利要求 16-19 中任一项所述的系统，其特征在于，所述预设风险事件至少包括风险程度不同的第一预设风险事件、第二预设风险事件和第三预设风险事件；其中，

5 所述第一预设风险事件用于指示连接至所述服务端的不可信客户端的数量占比超过预设阈值；

所述第二预设风险事件用于指示接收外部发来的协议更新指令；

所述第三预设风险事件用于指示所述服务端当前持有的所述第一密钥生成协议的工作时间超过预设安全时长。

10 21、根据权利要求 20 所述的系统，其特征在于，所述服务端连接至多个所述客户端，且所述客户端上送的所述密钥交换请求还包括设备指纹信息；

所述服务端还用于：收集每个所述客户端上送的所述设备指纹信息，根据所述设备指纹信息判断每个所述客户端是否为不可信客户端，并周期性判断连接至所述服务端的所述不可信客户端的数量占比是否超过所述预设阈值，其中，若超过所述预设阈值，则检测到所述第
15 一预设风险事件。

22、根据权利要求 20 或 21 所述的系统，其特征在于，所述预设风险事件还包括风险程度大于所述第一预设风险事件的第四预设风险事件；其中，

所述第四预设风险事件用于指示所述服务端重复检测到多次所述第一预设风险事件。

23、根据权利要求 16-22 中任一项所述的系统，其特征在于，

20 所述服务端还用于：当检测到所述密钥交换请求携带的版本号与所述第二密钥生成协议的版本号不一致时，将所述第二密钥生成协议的版本号下发至所述客户端；

所述客户端还用于：向所述服务端发起协议更新请求，所述协议更新请求携带所述第二密钥生成协议的版本号；

25 所述服务端还用于：向所述客户端下发所述第二密钥生成协议的所述协议逻辑和所述协议数据；

所述客户端还用于：基于预置的密钥算子层、所述协议逻辑和所述协议数据，将所述第二密钥生成协议落地，并重新基于所述第二密钥生成协议向所述服务端发起所述密钥交换请求。

24、根据权利要求 23 所述的系统，其特征在于，所述服务端通过热更新方式向所述客户端
30 下发所述第二密钥生成协议的协议逻辑。

25、根据权利要求 14-24 中任一项所述的系统，其特征在于，

所述客户端还用于：当基于所述第二密钥生成协议进行动态更新之后，向所述服务端发送密钥交换请求，所述密钥交换请求包括所述客户端当前持有的所述第二密钥生成协议的版本号；

5 所述服务端还用于：当检测到所述密钥交换请求中携带的版本号与所述服务端当前持有的所述第二密钥生成协议的版本号一致时，生成服务端随机数，并将所述服务端随机数发送至所述客户端；

所述客户端还用于：根据所述服务端随机数生成预主密钥，将所述预主密钥发送至所述服务端；

10 所述客户端和所述服务端还用于：各自利用所述第二密钥生成协议、所述预主密钥、所述客户端随机数以及所述服务端随机数生成工作密钥，通过交换各自生成的所述工作密钥进行加密通讯。

26、根据权利要求 25 所述的系统，其特征在于，

所述客户端还用于：根据所述服务端随机数生成所述预主密钥之后，利用所述服务端下送的公钥对所述预主密钥进行加密，并将加密的所述预主密钥发送至所述服务端；

15 所述服务端还用于：利用私钥对加密的所述预主密钥进行解密，得到解密的所述预主密钥。

27、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有程序，当所述程序被处理器执行时，使得所述处理器执行如权利要求 1-13 中任一项所述的方法。

100

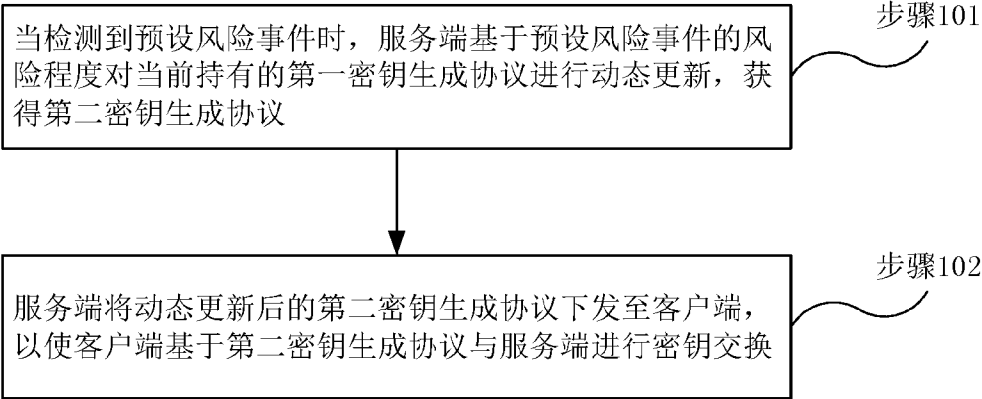


图 1

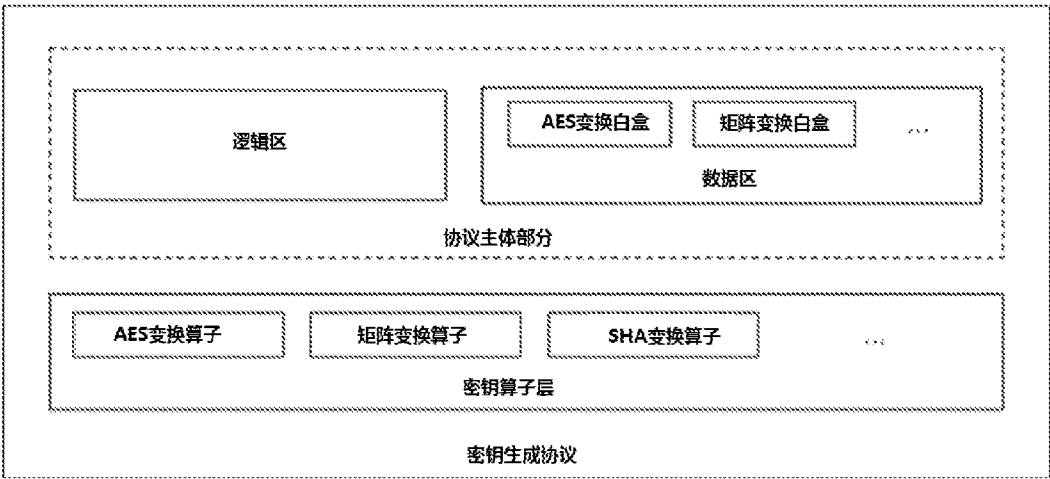


图 2

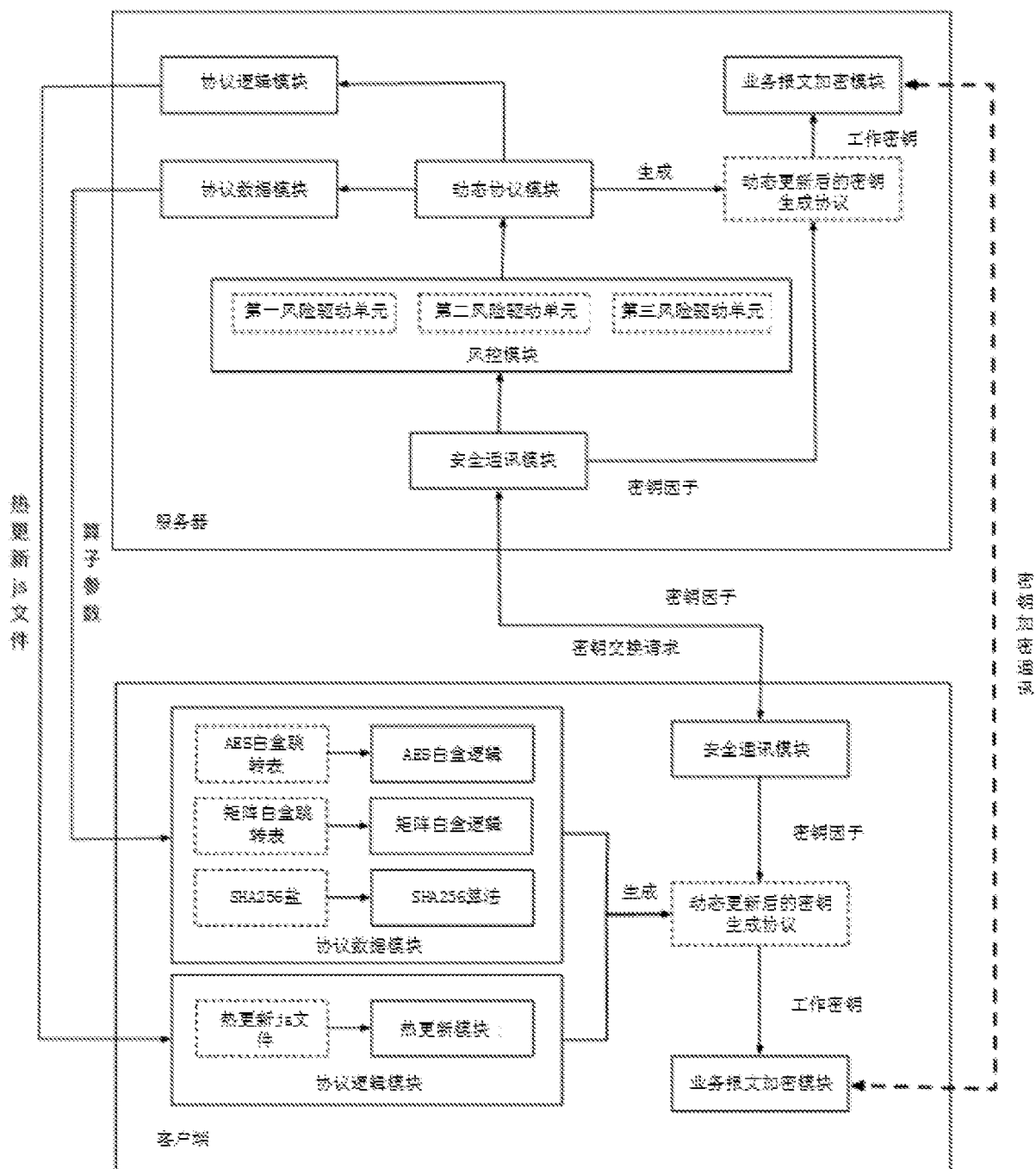


图 3

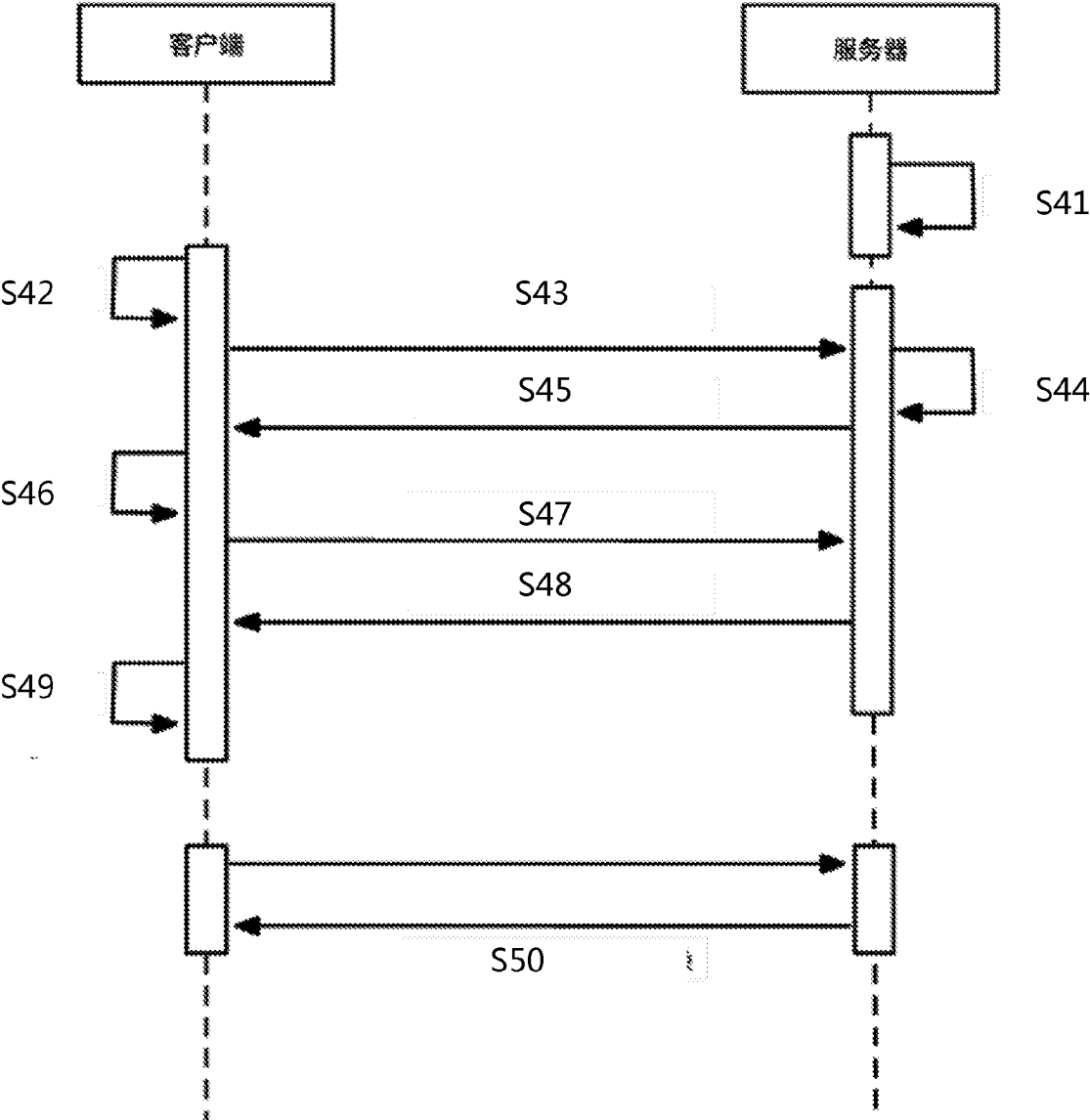


图 4

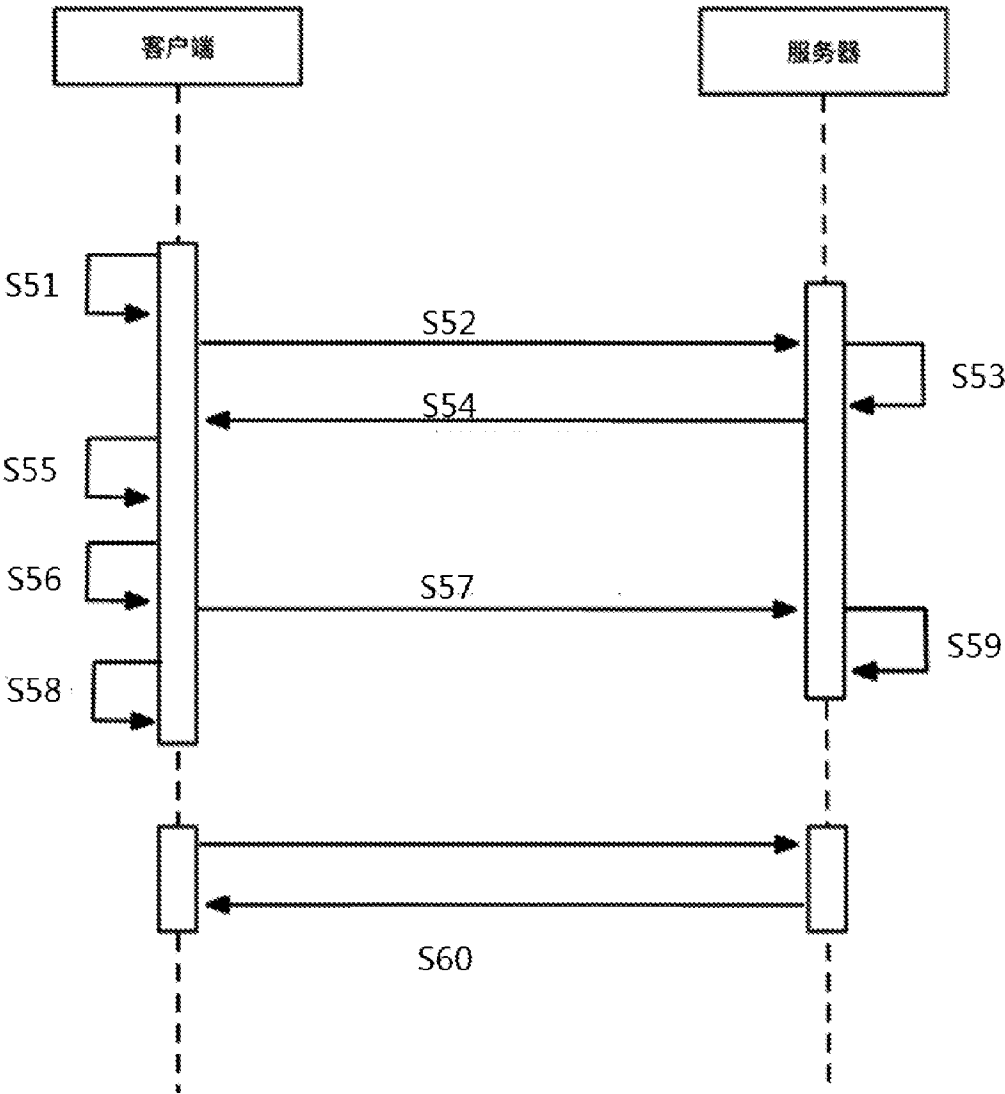


图 5

600

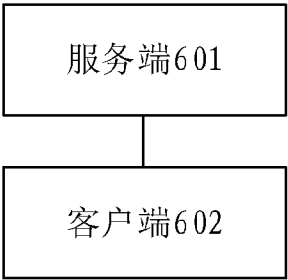


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/117514

A. CLASSIFICATION OF SUBJECT MATTER

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)

CNPAT, CNKI, WPI, EPODOC, IEEE: 风险, 安全, 事件, 密钥, 动态, 更新, 协议, 生成, 版本, 失效, 参数, risk, security, event, key, dynamic, update, protocol, generation, version, invalidation, parameter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101127595 A (HUAWEI TECHNOLOGIES CO., LTD.) 20 February 2008 (2008-02-20) description, pages 6-9	1-27
X	CN 111988143 A (BAIDU TIMES NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 24 November 2020 (2020-11-24) description, paragraphs [0021]-[0083], [0104]	1-27
A	CN 106533659 A (BEIJING ZHONGZHI XINWEI TECHNOLOGY CO., LTD. et al.) 22 March 2017 (2017-03-22) entire document	1-27
A	CN 108040071 A (SHENZHEN GRANDSTREAM NETWORKS INC. et al.) 15 May 2018 (2018-05-15) entire document	1-27
A	US 2018115414 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 26 April 2018 (2018-04-26) entire document	1-27

☐ 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

05 November 2021

Date of mailing of the international search report

08 December 2021

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

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/117514

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101127595	A	20 February 2008	EP	2056521	A1	06 May 2009
				WO	2008022520	A1	28 February 2008
				CN	101313511	A	26 November 2008
				US	2009271612	A1	29 October 2009
CN	111988143	A	24 November 2020	None			
CN	106533659	A	22 March 2017	None			
CN	108040071	A	15 May 2018	None			
US	2018115414	A1	26 April 2018	CN	107534554	A	02 January 2018
				JP	WO2016175105	A1	15 February 2018
				WO	2016175105	A1	03 November 2016
				EP	3291483	A1	07 March 2018

国际检索报告

国际申请号

PCT/CN2021/117514

A. 主题的分类

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))

CNPAT, CNKI, WPI, EPDOC, IEEE: 风险, 安全, 事件, 密钥, 动态, 更新, 协议, 生成, 版本, 失效, 参数, risk, security, event, key, dynamic, update, protocol, generation, version, invalidation, parameter

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 101127595 A (华为技术有限公司) 2008年2月20日 (2008 - 02 - 20) 说明书第6-9页	1-27
X	CN 111988143 A (百度时代网络技术北京有限公司) 2020年11月24日 (2020 - 11 - 24) 说明书第[0021]-[0083], [0104]段	1-27
A	CN 106533659 A (北京中质信维科技有限公司 等) 2017年3月22日 (2017 - 03 - 22) 全文	1-27
A	CN 108040071 A (深圳市潮流网络技术有限公司 等) 2018年5月15日 (2018 - 05 - 15) 全文	1-27
A	US 2018115414 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 2018年4月26日 (2018 - 04 - 26) 全文	1-27

☐ 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

2021年11月5日

国际检索报告邮寄日期

2021年12月8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

杨丹

电话号码 86-(10)-53961569

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/117514

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	101127595	A	2008年2月20日	EP	2056521	A1	2009年5月6日
				WO	2008022520	A1	2008年2月28日
				CN	101313511	A	2008年11月26日
				US	2009271612	A1	2009年10月29日
CN	111988143	A	2020年11月24日	无			
CN	106533659	A	2017年3月22日	无			
CN	108040071	A	2018年5月15日	无			
US	2018115414	A1	2018年4月26日	CN	107534554	A	2018年1月2日
				JP	W02016175105	A1	2018年2月15日
				WO	2016175105	A1	2016年11月3日
				EP	3291483	A1	2018年3月7日