(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
2009 年 10 月 29 日 (29.10.2009)

PCT

(10) 国际公布号
WO 2009/129734 A1

(51) 国际专利分类号:
H04L 9/28 (2006.01)

(21) 国际申请号: PCT/CN2009/071371

(22) 国际申请日: 2009 年 4 月 20 日 (20.04.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810093122.4 2008 年 4 月 21 日 (21.04.2008) CN

(71) 申请人 (对除美国外的所有指定国): **成都市华为赛门铁克科技有限公司 (HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **黄敏 (HUANG, Min)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。 **刘利锋 (LIU, Lifeng)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。 **万适 (WAN, Shi)** [CN/CN]; 中国四川省成都市高新区西部园区清水河片区天辰路 88 号, Sichuan 611731 (CN)。

(74) 代理人: **北京三高永信知识产权代理有限责任公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD..)**; 中国北京市海淀区学院路蓟门里和景园 A-1-102, Beijing 100088 (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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

[见续页]

(54) Title: METHOD, SYSTEM AND DEVICE FOR ACQUIRING KEY

(54) 发明名称: 一种获取密钥的方法、系统和设备

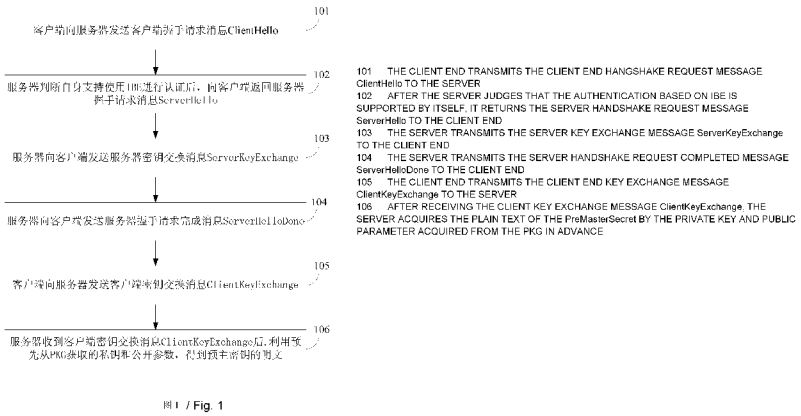

图 1 / Fig. 1

(57) **Abstract**: A method, system and device for acquiring key in communication field are disclosed. The method comprises: a server confirms that the security authentication based on identity based encryption IBE is supported; acquires the public parameter and private key used for the IBE, the server receives the PreMasterSecret encrypted by the IBE, and acquires the plain text of the PreMasterSecret according to the public parameter and the private key. The system comprises the client end and the server. The client end comprises the IBE negotiating module, the public key acquiring module, the server identity acquiring module and the processing module. The server comprises the IBE negotiating module, the public parameter acquiring module, the private key acquiring module and the processing module. By combining IBE technology and SSL/TLS technology, the encryption type of PreMasterSecret in the current SSL/TLS protocol can be enriched, and the purpose for extending the application scope of the current SSL/TLS protocol adequately can be realized.

[见续页]

WO 2009/129734 A1

(57) 摘要:

本发明公开了一种获取密钥的方法、系统和设备，属于通信领域。所述方法包括：服务器确认支持基于标识加密的安全认证 IBE；获取用于所述 IBE 的公开参数和私钥；所述服务器接收 IBE 加密的预主密钥，根据所述公开参数和私钥获取所述预主密钥的明文。所述系统包括：客户端和服务器。所述客户端包括：IBE 协商模块、公开参数获取模块、服务器标识获取模块和处理模块。所述服务器包括：IBE 协商模块、公开参数获取模块、私钥获取模块和处理模块。通过将 IBE 技术与 SSL/TLS 技术结合，丰富了现有 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的。

说 明 书

一种获取密钥的方法、系统和设备

本申请要求于 2008 年 4 月 21 日提交中国专利局、申请号为 200810093122.4、发明名称为“一种获取密钥的方法、系统和设备”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

本发明涉及通信领域，特别涉及一种获取密钥的方法、系统和设备。

背景技术

随着 Internet 因特网的迅速普及，基于 Web 的各种应用得到极大的发展，远程接入增多，随之而来的是各种安全问题的凸显。Nescape 公司为了解决浏览器访问互联网资源过程中出现的安全问题，提出了 SSL（Secure Socket Layer，安全套接层）协议。后来由国际标准组织 IETF(Internet Engineering Task Force,因特网工程任务组，又叫互联网工程任务组)对该协议进行了规范化，并取名为 TLS(Transport Layer Security Protocol,安全传输层协议)。

基于 SSL/TLS 技术的 VPN（Virtual Private Network，虚拟专用网）是通过 SSL/TLS 来保证用户远程接入网络的安全性和可靠性，以达到像专用网络一样的数据的安全传输。目前，SSL/TLS VPN 设备从过去单一的支持 Web 访问安全保证，到现在针对各种应用的安全支持，已经发展成为不可或缺的安全产品之一。

其中，SSL/TLS 通信双方使用相同的密钥导出函数，以相同的预主密钥（PreMasterSecret）和随机数为参数，计算出通信过程中所有的密钥。由于随机数以明文传输，因此，预主密钥的安全是 SSL/TLS 通信过程中最关键的因素。

发明人在实现本发明时发现，现有的 SSL/TLS 的握手协议中的预主密钥是由 SSL/TLS 通信双方中的客户端根据服务器的私钥生成并发送的，生成的形式单一，限制了 SSL/TLS 协议使用范围，不利于 SSL/TLS 协议的扩展。

发明内容

为了实现通信双方的安全通信握手，减少证书管理和维护的开销，本发明实施例提供了获取密钥的方法、系统和设备。所述技术方案如下：

一方面，提供了一种获取密钥的方法，所述方法包括：

服务器确认支持基于标识加密的安全认证 IBE；

获取用于所述 IBE 的公开参数和私钥；

所述服务器接收 IBE 加密的预主密钥，根据所述公开参数和私钥获取所述预主密钥的明文。

一方面，提供了一种获取密钥的系统，所述系统包括客户端和服务器；

所述客户端，用于和所述服务器进行基于标识加密的安全认证 IBE 的协商后，获取用于所述 IBE 的公开参数；并利用获取的所述服务器标识和所述获取的公开参数，生成并发送所述 IBE 加密的预主密钥；

所述服务器，用于和所述客户端进行基于标识加密的安全认证 IBE 的协商后，获取用于所述 IBE 的公开参数；并用于接收所述客户端发送的所述 IBE 加密的预主密钥，利用获取的公开参数和获取的私钥对所述 IBE 加密的预主密钥进行解密后，获取所述预主密钥的明文。

一方面，提供了一种客户端，所述客户端包括：

IBE 协商模块，用于和服务器进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块，用于获取用于所述 IBE 的公开参数；

服务器标识获取模块，用于获取所述服务器标识；

处理模块，用于根据所述服务器标识获取模块获取的服务器标识和所述公开参数获取模块协商获取的公开参数，生成并发送所述 IBE 加密的预主密钥。

另一方面，提供了一种服务器，所述服务器包括：

IBE 协商模块，用于和客户端进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块，用于获取用于进行 IBE 的公开参数；

私钥获取模块，用于获取私钥，所述私钥用于解密 IBE 加密的预主密钥；

处理模块，用于接收所述客户端发送的 IBE 加密的预主密钥，利用所述私钥获取模块获取的私钥和所述公开参数获取模块获取的公开参数对所述 IBE 加密的预主密钥进行解密后，获取所述预主密钥的明文。

再一方面，提供了一种提供设备，所述提供设备用于在服务器和客户端在基于 IBE 的安全套接层 SSL/TLS 协议的协商认证过程中，提供用于 IBE 的公开参数，其中，所述公开参数用于所述客户端根据所述公开参数和服务器标识生成 IBE 加密的预主密钥；相应地，所述服务器根据所述公开参数和获取的私钥，获取所述 IBE 加密的预主密钥的明文。

本发明实施例提供的技术方案的有益效果是：

通过 SSL/TLS 服务器支持基于 IBE 的 SSL/TLS 握手协商，利用获取的用于所述 IBE 的

公开参数和私钥，解密 IBE 加密的预主密钥，获取到预主密钥的明文，将 IBE 技术和 SSL/TLS 技术结合，简化了证书管理，节省了网络应用层的建设、管理 CA 的成本和维护一系列数字证书的开销，实现了通信双方的安全通信握手，并且，充分扩展了现有的 SSL/TLS 协议的使用范围，丰富现有了的 SSL/TLS 协议中预主密钥的加密形式。

附图说明

图 1 是本发明实施例 1 提供的获取密钥的方法流程图；

图 2 是本发明实施例 1 提供的获取密钥的信息交互示意图；

图 3 是本发明实施例 1 提供的获取密钥的一种通信场景示意图；

图 4 是本发明实施例 1 提供的实现获取密钥的 SSL/TLS VPN 的设备示意图；

图 5 是本发明实施例 2 提供的获取密钥的系统示意图；

图 6 是本发明实施例 3 提供的客户端示意图；

图 7 是本发明实施例 4 提供的服务器示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

本领域技术人员可以获知，IBE（Identity-Based Encryption，基于标识的加密）技术最早是由 Shamir 于 1984 年提出，其初衷是简化电子邮件系统中的证书管理，能够满足任何一对用户之间安全通信以及在不需要交换私钥和公钥的情况下验证每个人的签名。IBE 认证体系是一种将用户的公开标识作为公钥的加密方式，不需要通过证书绑定用户的身份及其公钥。其中，上述公开标识具体可以为能够代表用户身份的任意公开的字符串信息，例如用户的邮箱地址，IP 地址，身份证号或手机号码等。而对端用于解密的私钥则由 IBE 认证体系中的预设的 PKG(Private Key Generator，私钥生成器)发放的。

IBE 与基于 PKI(Public Key Infrastructure，公开密钥体系)的传统方案相比，由于取消了第三方认证机构(CA，Certification Authority)。因此在应用层面节省了建设、管理 CA 的成本，省去了产生，更新，撤销等一系列对数字证书的维护工作；在技术层面避免了交叉认证中信任的起点和信任如何传递，以及当用户数量增多时 CA 负担过重等难题，节省带宽资源，存储空间需求小。

本发明实施例提供的获取密钥的方法，利用上述 IBE 技术的优点，以将 IBE 技术与 SSL/TLS 技术结合为例，方法内容如下： SSL/TLS VPN 系统中的客户端和服务器进行基于

标识加密的安全认证 IBE 的协商，即服务器确认支持基于标识加密的安全认证 IBE；服务器获取用于 IBE 的公开参数（可通过和客户端协商获取）和私钥；服务器接收 IBE 加密的预主密钥（即客户端利用获取的服务器标识和客户端获取的公开参数，生成 IBE 加密的预主密钥后，发送的），服务器根据获取的公开参数和私钥获取预主密钥的明文。从而实现了通信双方的安全通信握手，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的。

实施例 1

参见图 1，本发明实施例提供了一种获取密钥的方法，为了与标准的 SSL/TLS 协议保持一致，SSL/TLS 使用 IBE 进行握手的过程详见下述内容：

101：客户端向服务器发送客户端握手请求消息 ClientHello，该 ClientHello 中携带使用 IBE 进行认证的密码套件。

其中，在客户端向服务器发送客户端握手请求消息 ClientHello 时，除了 SSL/TLS 标准中规定的各项内容外，还需要提供包含了使用 IBE 进行认证的密码套件列表，该密码套件列表中包含了 IBE 算法、认证算法、加密算法、摘要算法等内容，其中，该密码套件列表用于向服务器请求协商使用 IBE 进行认证。本发明实施例不限制在具体应用时，客户端向服务器发送客户端握手请求消息 ClientHello 中是否还携带使用其它方法进行认证的密码套件。

102：服务器收到客户端发送的客户端握手请求消息 ClientHello，判断自身支持使用 IBE 进行认证后，向客户端返回作为客户端握手请求消息 ClientHello 响应消息的服务器握手请求消息 ServerHello。

其中，服务器返回的服务器握手请求消息 ServerHello（或称服务器握手消息），该消息用于表明服务器同意使用 IBE 进行认证，例如，当在步骤 101 中客户端发送了包括 IBE 密码套件在内的多套用于进行认证的密码套件时，则可以通过该 ServerHello 消息中携带服务器确认选择的 IBE 认证的密码套件。本发明实施例不限制该服务器握手消息 ServerHello 的具体实现形式。如果服务器判断自身不支持使用 IBE 进行认证时，相应地，需要返回响应消息通告客户端不能进行 IBE 进行认证。

103：服务器同意使用 IBE 进行认证后，向客户端发送服务器密钥交换消息 ServerKeyExchange，用于和客户端协商进行 IBE 认证所需要的公开参数的相关信息。

其中，针对该步骤 103 中涉及到的公开参数，本领域技术人员可以获知使用 IBE 进行认证时，一方面需要使用随机数等特定的函数生成预主密钥，同时还需要使用公开参数和对端设备标识对生成的预主密钥进行加密后，需要将加密后的预主密钥发送到对端设备，

其中，用于进行 IBE 加密的公开参数通常为一套数据包含一系列的参数，例如根据系统的需要配置的安全曲线、算法等等。

104：服务器向客户端发送服务器握手请求完成消息 ServerHelloDone，用于通告客户端服务器方的认证准备工作已经完成。

其中，该步骤中服务器发送的服务器握手请求完成消息 ServerHelloDone 可以采用标准的 SSL/TLS 握手消息。

105：客户端向服务器发送客户端密钥交换消息 ClientKeyExchange。其中，该消息包括两部分内容：

1、协商 IBE 公开参数的相关信息，用于作为对步骤 103 中的服务器密钥交换消息 ServerKeyExchange 消息的响应。

2、向服务器发送通过协商得到的公开参数和预先获取的服务器标识完成 IBE 加密的预主密钥。

106：服务器收到客户端发送的客户端密钥交换消息 ClientKeyExchange 后，根据其中携带的 IBE 加密的预主密钥，利用预先从 PKG 获取的私钥和公开参数，对 IBE 加密的预主密钥进行解密，从而得到预主密钥的明文。

参见图 2，为基于本发明实施例提供的获取密钥的方法的 SSL/TLS 使用 IBE 的握手过程示意图，详细的交互过程如前文所述，不再赘述。

综上，客户端和服务器通过 ClientHello 和 ServerHello 消息确认使用 IBE 进行认证，使用 ServerKeyExchange 和 ClientKeyExchange 完成对公开参数的协商，其中，在具体实现时，协商方式可以有以下几种，说明如下：

（一）如果客户端和服务器预共享唯一的一套公开参数，服务器和客户端还不使用任何包含公开参数的消息进行交互，而表明双方默认使用了该预共享公开参数；

其中，具体实现时，上述步骤 103 中服务器不用发送 ServerKeyExchange 消息，即用 ServerHelloDone 来表示服务器握手消息的结束，服务器通过这种方式表明默认使用预共享的公开参数；相应地，上述步骤 105 中，客户端在 ClientKeyExchange 消息中不用包含公开参数的相关信息（确认使用了默认的预共享的公开参数），只用包含一项内容即通过该 ClientKeyExchange 消息直接将使用预共享公开参数和服务器标识加密的预主密钥发送至服务器。

（二）如果客户端和服务器预共享唯一的一套公开参数，服务器使用 ServerKeyExchange 消息通知客户端使用预共享的公开参数，客户端使用 ClientKeyExchange 消息响应；

其中，具体实现时，上述步骤 103 中服务器可以通过 ServerKeyExchange 发送一个预设标识，用于通告客户端使用预共享的公开参数，而不需要携带任何有关于公开参数的实质内容；相应地，上述步骤 105 中，客户端对使用预共享参数进行确认，通过 ClientKeyExchange 传递预设标识，用于确认使用了预共享的公开参数，而不需要公开参数的实质内容。

其中，上述唯一的一套公开参数是事先客户端和服务器分别向 PKG 获取后，进行保存的。

（三）如果客户端和服务器共享了多套公开参数，服务器使用 ServerKeyExchange 消息通知客户端它建议使用的公开参数的对应标识，客户端使用 ClientKeyExchange 消息响应；

其中，具体实现时，上述步骤 103 中服务器根据具体的系统部署策略，从共享的多套公开参数中，选择至少一套公开参数，其中，每套公开参数可以对应于唯一的标识，参见表 1，提供了一种公开参数和标识的对应表，通过 ServerKeyExchange 将选择出的公开参数的对应的标识发送到客户端；

表 1

标识	公开参数
1	第一套公开参数
2	第二套公开参数
3	第三套公开参数

相应地，由于多套公开参数为客户端和服务器所共享，所以相应的代表每套公开参数的标识也是一致，在步骤 104 中，客户端根据服务器提供的标识获取到对应的一套公开参数，然后通过发送 ClientKeyExchange 携带该套公开参数对应的标识响应服务器。

进一步地，当服务器向客户端发送的公开参数标识为多个时，客户端根据服务器提供的多个标识，根据自身的选择策略选择出一个后，客户端使用该选择的标识对应的公开参数。

进一步，客户端收到服务器发送的公开参数标识后，还可以根据自身的选择策略选择不使用服务器发送的公开参数标识对应的公开参数，而根据自身的策略，选择出使用的一套公开参数，并相应地，通过 ClientKeyExchange 携带该套确定的公开参数对应的标识响应服务器。

其中，上述多套公开参数是事先客户端和服务器分别向 PKG 获取后，进行保存的。

（四）如果客户端和服务器未预先共享公开参数，则服务器使用 ServerKeyExchange

消息将加密需要使用的一套公开参数发送给客户端；或者服务器使用 ServerKeyExchange 消息将多套公开参数发送给客户端；相应地，客户端从收到的多套公开参数中，选择出一套使用的公开参数后，通过 ClientKeyExchange 消息响应服务器选择使用的公开参数。

其中，在具体实现时，服务器可以采用通过 ServerKeyExchange 消息发送公开参数以及其对应标识的形式；相应地，客户端在使用 ClientKeyExchange 消息响应服务器时，可以仅通过携带标识的形式实现。

（五）如果采用远程获取的方式获取公开参数，则服务器使用 ServerKeyExchange 消息将产生公开参数的 PKG 的地址（或域名）等用于定位公开参数的标识发送给客户端，相应地，当客户端收到该 ServerKeyExchange 消息后，根据其中携带的定位公开参数的标识信息，去 PKG 获取公开参数后，使用 ClientKeyExchange 通告服务器其选择的公开参数。

进一步地，服务器使用 ServerKeyExchange 消息发送用于定位公开参数的标识时，可以发送多个 PKG 的标识，相应地，客户端根据自身的策略（如出于安全、方便等角度出发制定策略），从多个标识中选择出一个 PKG 标识，向该 PKG 获取公开参数。参见图 3，为该情况下通信场景，服务器向客户端发送 PKG1、PKG2 和 PKG3 地址标识，客户端收到后，根据自身的策略配置，从中选择出 PKG2，向 PKG2 获取公开参数。

（六）如果采用远程获取的方式获取公开参数，并且预设了用于存储多套公开参数的公开参数服务器（其中，该公开参数服务器做为一个功能实体既可以单独存在也可以集成在现有的 PKG 设备中），则服务器使用 ServerKeyExchange 消息将公开参数在公开参数服务器中的保存的地址发送给客户端，参见表 2，提供了一种公开参数和地址的对应关系表；相应地，当客户端收到该 ServerKeyExchange 消息后，根据携带的地址信息向公开参数服务器获取公开参数后，通过 ClientKeyExchange 通告服务器其选择的公开参数的地址。

表 2

公开参数	地址
第一套公开参数	A
第二套公开参数	B
第三套公开参数	C

进一步地，服务器使用 ServerKeyExchange 消息将向客户端发送地址时，还可以发送多个地址，由客户端根据自身的策略从中选择出一个做为获取公开参数的地址。

进一步，参见表 3，还可以为公开参数以及地址配置标识的形式，相应地，服务器使用 ServerKeyExchange 消息将公开参数的标识发送给客户端，客户端根据收到的标识向对应的地址获取公开参数后，通过 ClientKeyExchange 通告服务器其选择的公开参数的标识。

表 3

标识	公开参数	地址
1	第一套公开参数	A
2	第二套公开参数	B
3	第三套公开参数	C

综上，上述第五种方式和第六种方式中，由于客户端需要从第三方（PKG 或者公开参数服务器）获取公开参数，因此客户端应该根据服务器提供的可选项中，根据自身制定的安全选择策略，选择出自己信任的第三方来申请公开参数，防止可能出现的中间人攻击。客户端需要维护一个可信任第三方的列表。

本领域技术人员可以获知 SSL/TLS VPN 在 SSL/TLS 通信的过程中多数情况下扮演服务器的角色，但也能成为客户端（如在 SSL/TLS VPN 在建立站点到站点的隧道的情况下），因此，参见图 4，SSL/TLS VPN 必须具备以下功能模块才能满足支持对 IBE 的支持，其中，支持 IBE 的 SSL/TLS 通信模块完成 SSL/TLS 握手。在握手过程中如果 IBE 需要获得加密和解密的公开参数：如果使用上述第一种、第二种和第三种协商方式，则调用预共享公开参数管理模块从本地获得公开参数；如果使用上述第四种、第五种和第六种协商方式，则调用远程公开参数获取模块从远程获得公开参数。

综上所述，本发明实施例提供的获取密钥的方法，通过将 IBE 技术与 SSL/TLS 技术结合，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的，并且 SSL/TLS 客户端和服务器通过上述六种方式的任意一种，可以唯一确定了加密和解密运算过程中使用的公开参数，实现了预主密钥的安全传输。

实施例 2

参见图 5，本发明实施例提供了一种获取密钥的系统，包括：系统包括客户端 201 和服务器 202；

客户端 201，用于和服务器 202 进行基于标识加密的安全认证 IBE 的协商后，获取用于 IBE 的公开参数（可以和服务器 202 协商获取该公开参数）；并利用获取的服务器标识和获取的公开参数，生成并发送 IBE 加密的预主密钥；

服务器 202，用于和客户端 201 进行基于标识加密的安全认证 IBE 的协商后，获取用于 IBE 的公开参数（可以和客户端 201 协商获取该用于 IBE 的公开参数）；并用于接收客户端 201 发送的 IBE 加密的预主密钥，利用获取的私钥进行解密后获取预主密钥的明文。

（一）本发明实施例提供的获取密钥的系统中的客户端 201 包括：

IBE 协商模块，用于向服务器 202 发送客户端请求消息，客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；并接收服务器 202 返回的 IBE 确认消息；

公开参数获取模块，用于获取用于进行 IBE 的公开参数；

服务器标识获取模块，用于获取服务器标识；

处理模块，用于利用公开参数获取模块获取的公开参数，和服务器标识获取模块获取的服务器标识，生成并发送 IBE 加密的预主密钥。

其中，该客户端 201 的公开参数获取模块包括：

（a）公开参数保存单元，用于保存一套公开参数；公开参数选择单元，用于获取公开参数保存单元中保存的公开参数。该情况即对应着当客户端 201 和服务器 202 进行了 IBE 认证协商后，默认使用了该套预共享的公开参数。

或者；

（b）公开参数保存单元，用于保存至少一套公开参数；公开参数选择单元，用于根据服务器 202 的通知，从公开参数保存单元中选择一套公开参数；响应单元，用于当公开参数选择单元选择了一套公开参数后，响应服务器 202 选择的公开参数。

或者；

（c）公开参数获取单元，用于获取服务器 202 发送的至少一套公开参数；公开参数选择单元，用于从公开参数获取单元中获取的公开参数中，选择出一套公开参数；响应单元，用于当公开参数选择单元选择了一套公开参数后，通知服务器 202 选择的公开参数。

或者；

（d）当系统还包括：至少一个私钥生成器 PKG 时，其中 PKG 用于提供公开参数；相应地，公开参数获取模块包括：PKG 标识获取单元，用于获取服务器 202 发送的至少一个私钥生成器 PKG 标识；PKG 标识选择单元，用于从 PKG 标识获取单元获取的 PKG 标识中，选择一个 PKG 标识；公开参数获取单元，用于根据 PKG 标识选择单元选择的 PKG 标识，向选择的 PKG 标识对应的 PKG 获取公开参数；通知单元，用于当 PKG 标识选择单元选择了 PKG 标识后，通知服务器 202 选择的 PKG 标识。

或者；

（e）当系统还包括：能够提供至少一套公开参数的公开参数服务器时，相应地，公开参数获取模块包括：

地址标识获取单元，用于获取服务器 202 发送的公开参数服务器中保存的至少一个公开参数的地址标识；地址标识选择单元，用于根据地址标识获取单元获取的地址标识中，

选择一个地址标识；公开参数获取单元，用于根据地址标识选择单元选择的地址标识，根据选择的地址标识向公开参数服务器获取公开参数；通知单元，用于当地址标识选择单元选择了地址标识后，通知服务器 202 选择的地址标识。

（二）本发明实施例提供的获取密钥的系统中的服务器 202 包括：

IBE 协商模块，用于接收客户端 201 发送的客户端请求消息，客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；判断支持 IBE 认证后，向客户端 201 返回确认消息；

公开参数获取模块，用于和客户端 201 协商用于进行 IBE 的公开参数；

私钥获取模块，用于获取私钥，私钥用于解密 IBE 加密的预主密钥；

处理模块，用于接收客户端 201 发送的 IBE 加密的预主密钥，利用私钥获取模块获取的私钥进行解密后，获取预主密钥的明文。

其中，该服务器 202 的公开参数获取模块包括：

(a)公开参数保存单元，用于保存一套公开参数；公开参数选择单元，用于获取公开参数保存单元中保存的公开参数。该情况即对应着当客户端 201 和服务器 202 进行了 IBE 认证协商后，默认使用了该套预共享的公开参数。

(b)公开参数保存单元，用于保存至少一套公开参数；通知单元，用于根据公开参数保存单元保存的公开参数，向客户端 201 发送通知；接收单元，用于接收客户端 201 返回的选择的公开参数的响应。

(c)发送单元，用于向客户端 201 发送至少一套公开参数；接收单元，用于接收客户端 201 返回的选择的公开参数的响应。

(d)当系统还包括：至少一个私钥生成器 PKG 时，其中 PKG 用于提供公开参数；相应地，公开参数获取模块包括：

PKG 标识发送单元，用于向客户端 201 发送至少一个私钥生成器 PKG 标识；接收单元，用于接收客户端 201 返回的选择的 PKG 标识; 获取单元，用于接收单元接收的 PKG 标识，获取一套用于 IBE 的公开参数。

（e）当系统还包括：能够提供至少一套公开参数的公开参数服务器时，相应地，公开参数获取模块包括：

地址标识发送单元，用于向客户端 201 发送公开参数服务器中保存的至少一个公开参数的地址标识；接收单元，用于接收客户端 201 返回的选择的地址标识。获取单元，用于接收单元接收的地址标识，获取一套用于 IBE 的公开参数。

综上所述，本发明实施例提供的获取密钥的系统，通过将 IBE 技术与 SSL/TLS 技术结

合，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的，并且 SSL/TLS 客户端和服务器多种公开参数协商模式中的任意一种，可以唯一确定了加密和解密运算过程中使用的公开参数，实现了预主密钥的安全传输。

实施例 3

参见图 6，本发明实施例提供了一种客户端，所述客户端包括：

IBE 协商模块 301，用于和服务器进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块 302，用于获取用于 IBE 的公开参数（可以和服务器协商获取该用于 IBE 的公开参数）；

服务器标识获取模块 303，用于获取服务器标识；

处理模块 304，用于根据服务器标识获取模块 303 获取的服务器标识和公开参数获取模块 302 获取的公开参数，生成并发送 IBE 加密的预主密钥；

其中，IBE 协商模块 301 具体用于向服务器发送客户端请求消息，客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；并接收服务器返回的 IBE 确认消息；

其中，公开参数获取模块 302 包括：

公开参数保存单元，用于保存一套公开参数；公开参数选择单元，用于获取公开参数保存单元中保存的公开参数。该情况即对应着当客户端和服务器进行了 IBE 认证协商后，默认使用了该套预共享的公开参数。

或者包括：

公开参数保存单元，用于保存至少一套公开参数；

公开参数选择单元，用于根据服务器的通知，从公开参数保存单元中选择一套公开参数；

响应单元，用于当公开参数选择单元选择了一套公开参数后，响应服务器选择的公开参数；

或者包括：

公开参数获取单元，用于获取服务器发送的至少一套公开参数；

公开参数选择单元，用于从公开参数获取单元中获取的公开参数中，选择出一套公开参数；

响应单元，用于当公开参数选择单元选择了一套公开参数后，通知服务器选择的公开参数；

或者包括：

PKG 标识获取单元，用于获取服务器发送的至少一个私钥生成器 PKG 标识；

PKG 标识选择单元，用于从 PKG 标识获取单元获取的 PKG 标识中，选择一个 PKG 标识；

公开参数获取单元，用于根据 PKG 标识选择单元选择的 PKG 标识，向选择的 PKG 标识对应的 PKG 获取公开参数；

通知单元，用于当 PKG 标识选择单元选择了 PKG 标识后，通知服务器选择的 PKG 标识。

或者包括：

地址标识获取单元，用于获取服务器发送的公开参数服务器中保存的至少一个公开参数的地址标识；

地址标识选择单元，用于根据地址标识获取单元获取的地址标识中，选择一个地址标识；

公开参数获取单元，用于根据地址标识选择单元选择的地址标识，根据选择的地址标识向公开参数服务器获取公开参数；

通知单元，用于当地址标识选择单元选择了地址标识后，通知服务器选择的地址标识。

综上所述，本发明实施例提供的客户端，通过将 IBE 技术与 SSL/TLS 技术结合，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的，并且 SSL/TLS 客户端和服务器多种公开参数协商模式中的任意一种，可以唯一确定了加密和解密运算过程中使用的公开参数，实现了预主密钥的安全传输。

实施例 4

参见图 7，本发明实施例提供了一种服务器，包括：

IBE 协商模块 401，用于和客户端进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块 402，用于获取用于 IBE 的公开参数（具体可以为和客户端协商获取该用于进行 IBE 的公开参数）；

私钥获取模块 403，用于获取私钥，私钥用于解密 IBE 加密的预主密钥；

处理模块 404，用于接收客户端发送的 IBE 加密的预主密钥，利用私钥获取模块 403 获取的私钥和公开参数获取模块 402 获取的公开参数对 IBE 加密的预主密钥进行解密后，获取预主密钥的明文。

其中，IBE 协商模块 401 具体用于接收客户端发送的客户端请求消息，客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；判断支持 IBE 认证后，向客户端返回确认消息。

其中，公开参数获取模块 402 包括：

公开参数保存单元，用于保存一套公开参数；公开参数选择单元，用于获取公开参数保存单元中保存的公开参数。该情况即对应着当客户端和服务器进行了 IBE 认证协商后，默认使用了该套预共享的公开参数。

或者包括：

公开参数保存单元，用于保存至少一套公开参数；

通知单元，用于根据公开参数保存单元保存的公开参数，向客户端发送通知；

接收单元，用于接收客户端返回的选择的公开参数响应；

获取单元，用于根据接收单元接收的响应，获取公开参数保存单元中保存的公开参数。

或者包括：

发送单元，用于向客户端发送至少一套公开参数；

接收单元，用于接收客户端返回的选择的公开参数响应；

获取单元，用于根据接收单元接收的响应，获取一套公开参数。

或者包括：

PKG 标识发送单元，用于向客户端发送至少一个私钥生成器 PKG 标识；

接收单元，用于接收客户端返回的选择的 PKG 标识；

获取单元，用于接收单元接收的 PKG 标识，获取一套用于 IBE 的公开参数。

或者包括：

地址标识发送单元，用于向客户端发送公开参数服务器中保存的至少一个公开参数的地址标识；

接收单元，用于接收客户端返回的选择的地址标识；

获取单元，用于接收单元接收的地址标识，获取一套用于 IBE 的公开参数。

综上所述，本发明实施例提供的服务器，通过将 IBE 技术与 SSL/TLS 技术结合，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的，并且 SSL/TLS 客户端和服务器多种公开参数协商模式中的任意一种，可以唯一确定了加密和解密运算过程中使用的公开参数，实现了预主密钥的安全传输。

实施例 5

本发明实施例提供了一种提供设备，该提供设备用于在服务器和客户端在基于 IBE 的安全套接层 SSL/TLS 协议的协商认证过程中，提供用于 IBE 的公开参数（可以为根据服务器和客户端的协商结果提供该用于 IBE 的公开参数），其中，该公开参数用于客户端根据公开参数和服务器标识生成 IBE 加密的预主密钥；相应地，服务器根据该公开参数和获取的

私钥，获取 IBE 加密的预主密钥的明文。

其中，本领域技术人员可以获知使用 IBE 进行认证时，需要获取用于 IBE 的公开参数，其中，该公开参数通常为一套数据包含一系列的参数，例如根据系统的需要配置的安全曲线、算法等等。具体实现时，可以为每套公开参数设置对应的标识，通过查看标识便可以知道具体使用了哪套对应的公开参数。

进一步地，本发明实施例提供的能够提供公开参数的提供设备，还可以用于向服务器提供私钥，其中，该私钥用于当获取到 IBE 解密后的预主密钥后，对该预主密钥进行解密，从而获取到该预主密钥的明文。

本发明实施例涉及的提供设备在具体实施时，可以通过现有的 PKG 设备来实现，通过 PKG 设备实现提供公开参数的实体功能，每个 PKG 设备中配置的公开参数不同，相应地，在系统配置时，需要提供多个 PKG 设备来支持提供多套公开参数的目的，优选地，还可以通过单独设置公开参数服务器来实现提供至少一套公开参数的实体功能，事先将至少一套公开参数配置在该公开参数服务器中，对应与每套公开参数还可以为其配置对应的标识，本发明实施例不限制在具体实施时的具体的实现形式。

综上所述，本发明实施例提供的技术方案，通过将 IBE 技术与 SSL/TLS 技术结合，丰富现有的 SSL/TLS 协议中预主密钥的加密形式，实现了充分扩展了现有的 SSL/TLS 协议的使用范围的目的，并且 SSL/TLS 客户端和服务器多种公开参数协商模式中的任意一种，可以唯一确定了加密和解密运算过程中使用的公开参数，实现了预主密钥的安全传输。本领域技术人员可以获知，当服务器获取到预主密钥之后的 SSL/TLS 协商和通信过程和现有的标准 SSL/TLS 一致。本发明实施例还可以应用于使用 IBE 的其他技术方案中。

本发明实施例中的部分步骤，可以利用软件实现，相应的软件程序可以存储在可读取的存储介质中，如光盘或硬盘等。

以上所述仅为本发明的具体实施例，并不用以限制本发明，对于本技术领域的普通技术人员来说，凡在不脱离本发明原理的前提下，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种获取密钥的方法，其特征在于，所述方法包括：

服务器确认支持基于标识加密的安全认证 IBE；

获取用于所述 IBE 的公开参数和私钥；

所述服务器接收 IBE 加密的预主密钥，根据所述公开参数和私钥获取所述预主密钥的明文。

2. 如权利要求 1 所述的获取密钥的方法，其特征在于，所述服务器确认支持基于标识加密的安全认证 IBE，包括：

所述服务器接收客户端请求消息，所述客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件，判断支持所述 IBE 认证后，向所述客户端返回确认消息。

3. 如权利要求 1 所述的获取密钥的方法，其特征在于，当客户端和所述服务器预共享了一套公开参数时，所述获取用于所述 IBE 的公开参数，包括：

所述服务器使用所述预共享的公开参数。

4. 如权利要求 1 所述的获取密钥的方法，其特征在于，当客户端和所述服务器预共享了至少一套公开参数时，所述获取用于所述 IBE 的公开参数，包括：

所述服务器通知所述客户端使用所述预共享的公开参数；

所述客户端响应所述服务器的通知，

所述服务器根据所述通知，获取一套用于所述 IBE 的公开参数。

5. 如权利要求 4 所述的获取密钥的方法，其特征在于，当所述客户端和所述服务器预共享了多套公开参数时，所述服务器通知所述客户端使用所述预共享的公开参数；包括：

所述服务器通知所述客户端至少一套公开参数对应的标识；

相应地，所述客户端响应所述服务器的通知，具体为：

所述客户端从所述预共享的多套公开参数中选择出一套公开参数后，响应所述服务器所述选择的公开参数的标识。

6. 如权利要求 1 所述的获取密钥的方法，其特征在于，所述获取用于所述 IBE 的公开参数，包括：

所述服务器向客户端发送至少一套公开参数；

所述客户端从接收的所述服务器发送的至少一套公开参数中，选择出一套公开参数后，通知所述服务器所述选择的公开参数；

所述服务器根据所述通知，获取一套用于所述 IBE 的公开参数。

7. 如权利要求 1 所述的获取密钥的方法，其特征在于，所述获取用于所述 IBE 的公开

参数，包括：

所述服务器向客户端发送至少一个用于获取公开参数的私钥生成器 PKG 的标识；

所述客户端从接收的至少一个 PKG 标识中，选择一个 PKG 标识后，向所述选择的 PKG 标识对应的 PKG 获取公开参数；并通知所述服务器所述选择的 PKG 标识；

所述服务器根据所述通知，获取一套用于所述 IBE 的公开参数。

8. 如权利要求 1 所述的获取密钥的方法，其特征在于，所述获取用于所述 IBE 的公开参数，包括：

所述服务器向客户端发送公开参数服务器中保存的至少一个公开参数的地址标识；

所述客户端从接收到的所述服务器发送的至少一个地址标识中，选择一个地址标识后，根据所述选择的地址标识向所述公开参数服务器获取公开参数；并通知所述服务器所述选择的地址标识；

所述服务器根据所述通知，获取一套用于所述 IBE 的公开参数。

9. 一种获取密钥的系统，其特征在于，所述系统包括客户端和服务器；

所述客户端，用于和所述服务器进行基于标识加密的安全认证 IBE 的协商后，获取用于所述 IBE 的公开参数；并利用获取的所述服务器标识和所述获取的公开参数，生成并发送所述 IBE 加密的预主密钥；

所述服务器，用于和所述客户端进行基于标识加密的安全认证 IBE 的协商后，获取用于所述 IBE 的公开参数；并用于接收所述客户端发送的所述 IBE 加密的预主密钥，利用获取的公开参数和获取的私钥对所述 IBE 加密的预主密钥进行解密后，获取所述预主密钥的明文。

10. 如权利要求 9 所述的获取密钥的系统，其特征在于，所述客户端具体包括：

IBE 协商模块，用于向服务器发送客户端请求消息，所述客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；并接收所述服务器返回的 IBE 确认消息；

公开参数获取模块，用于获取用于进行 IBE 的公开参数；

服务器标识获取模块，用于获取所述服务器标识；

处理模块，用于利用所述公开参数获取模块获取的公开参数，和所述服务器标识获取模块获取的服务器标识，生成并发送所述 IBE 加密的预主密钥；

相应地，

所述服务器具体包括：

IBE 协商模块，用于接收所述客户端发送的客户端请求消息，所述客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；判断支持所述 IBE 认证后，向所述

客户端返回确认消息；

公开参数获取模块，用于获取用于进行 IBE 的公开参数；

私钥获取模块，用于获取私钥，所述私钥用于解密 IBE 加密的预主密钥；

处理模块，用于接收所述客户端发送的 IBE 加密的预主密钥，利用所述私钥获取模块获取的私钥和所述服务器的公开参数获取模块获取的公开参数进行解密后，获取所述预主密钥的明文。

11．如权利要求 10 所述的获取密钥的系统，其特征在于，所述系统还包括：

私钥生成器 PKG，用于提供公开参数；所述 PKG 至少一个；

相应地，所述客户端的公开参数获取模块具体包括：

PKG 标识获取单元，用于获取所述服务器发送的至少一个所述私钥生成器 PKG 标识；

PKG 标识选择单元，用于从所述 PKG 标识获取单元获取的 PKG 标识中，选择一个 PKG 标识；

公开参数获取单元，用于根据所述 PKG 标识选择单元选择的 PKG 标识，向所述选择的 PKG 标识对应的 PKG 获取公开参数；

通知单元，用于当所述 PKG 标识选择单元选择了 PKG 标识后，通知所述服务器所述选择的 PKG 标识；

相应地，所述服务器的公开参数获取模块具体包括：

PKG 标识发送单元，用于向所述客户端发送至少一个所述私钥生成器 PKG 标识；

接收单元，用于接收所述客户端返回的选择的 PKG 标识；

获取单元，用于所述接收单元接收的 PKG 标识，获取一套用于所述 IBE 的公开参数。

12．如权利要求 10 所述的获取密钥的系统，其特征在于，所述系统还包括：

公开参数服务器，用于提供至少一个公开参数；相应地，

所述客户端的公开参数获取模块具体包括：

地址标识获取单元，用于获取所述服务器发送的所述公开参数服务器中保存的至少一个公开参数的地址标识；

地址标识选择单元，用于根据所述地址标识获取单元获取的地址标识中，选择一个地址标识；

公开参数获取单元，用于根据所述地址标识选择单元选择的地址标识，根据所述选择的地址标识向所述公开参数服务器获取公开参数；

通知单元，用于当所述地址标识选择单元选择了地址标识后，通知所述服务器所述选择的地址标识；

相应地，所述服务器的公开参数获取模块具体包括：

地址标识发送单元，用于向所述客户端发送所述公开参数服务器中保存的至少一个公开参数的地址标识；

接收单元，用于接收所述客户端返回的选择的地址标识；

获取单元，用于所述接收单元接收的地址标识，获取一套用于所述 IBE 的公开参数。

13．一种客户端，其特征在于，所述客户端包括：

IBE 协商模块，用于和服务器进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块，用于获取用于所述 IBE 的公开参数；

服务器标识获取模块，用于获取所述服务器标识；

处理模块，用于根据所述服务器标识获取模块获取的服务器标识和所述公开参数获取模块协商获取的公开参数，生成并发送所述 IBE 加密的预主密钥。

14．如权利要求 13 所述的客户端，其特征在于，所述 IBE 协商模块具体用于向所述服务器发送客户端请求消息，所述客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；并接收所述服务器返回的 IBE 确认消息；

15．如权利要求 13 所述的客户端，其特征在于，所述公开参数获取模块具体包括：

公开参数保存单元，用于保存一套公开参数；

公开参数选择单元，用于获取所述公开参数保存单元中保存的公开参数。

16．如权利要求 13 所述的客户端，其特征在于，所述公开参数获取模块具体包括：

公开参数保存单元，用于保存至少一套公开参数；

公开参数选择单元，用于根据所述服务器的通知，从所述公开参数保存单元中选择一套公开参数；

响应单元，用于当所述公开参数选择单元选择了一套公开参数后，响应所述服务器所述选择的公开参数。

17．如权利要求 13 所述的客户端，其特征在于，所述公开参数获取模块具体包括：

公开参数获取单元，用于获取所述服务器发送的至少一套公开参数；

公开参数选择单元，用于从所述公开参数获取单元中获取的公开参数中，选择出一套公开参数；

响应单元，用于当所述公开参数选择单元选择了一套公开参数后，通知所述服务器所述选择的公开参数。

18．如权利要求 13 所述的客户端，其特征在于，所述公开参数获取模块具体包括：

PKG 标识获取单元，用于获取所述服务器发送的至少一个所述私钥生成器 PKG 标识；

PKG 标识选择单元，用于从所述 PKG 标识获取单元获取的 PKG 标识中，选择一个 PKG 标识；

公开参数获取单元，用于根据所述 PKG 标识选择单元选择的 PKG 标识，向所述选择的 PKG 标识对应的 PKG 获取公开参数；

通知单元，用于当所述 PKG 标识选择单元选择了 PKG 标识后，通知所述服务器所述选择的 PKG 标识。

19．如权利要求 13 所述的客户端，其特征在于，所述公开参数获取模块具体包括：

地址标识获取单元，用于获取所述服务器发送的公开参数服务器中保存的至少一个公开参数的地址标识；

地址标识选择单元，用于根据所述地址标识获取单元获取的地址标识中，选择一个地址标识；

公开参数获取单元，用于根据所述地址标识选择单元选择的地址标识，根据所述选择的地址标识向所述公开参数服务器获取公开参数；

通知单元，用于当所述地址标识选择单元选择了地址标识后，通知所述服务器所述选择的地址标识。

20．一种服务器，其特征在于，所述服务器包括：

IBE 协商模块，用于和客户端进行基于标识加密的安全认证 IBE 的协商；

公开参数获取模块，用于获取用于进行 IBE 的公开参数；

私钥获取模块，用于获取私钥，所述私钥用于解密 IBE 加密的预主密钥；

处理模块，用于接收所述客户端发送的 IBE 加密的预主密钥，利用所述私钥获取模块获取的私钥和所述公开参数获取模块获取的公开参数对所述 IBE 加密的预主密钥进行解密后，获取所述预主密钥的明文。

21．如权利要求 20 所述的服务器，其特征在于，所述 IBE 协商模块具体用于接收所述客户端发送的客户端请求消息，所述客户端请求消息中携带用于进行基于标识加密的安全认证 IBE 的密码套件；判断支持所述 IBE 认证后，向所述客户端返回确认消息。

22．如权利要求 20 所述服务器，其特征在于，所述公开参数获取模块具体包括：

公开参数保存单元，用于保存一套公开参数；

公开参数选择单元，用于获取所述公开参数保存单元中保存的公开参数。

23．如权利要求 20 所述服务器，其特征在于，所述公开参数获取模块具体包括：

公开参数保存单元，用于保存至少一套公开参数；

通知单元，用于根据所述公开参数保存单元保存的公开参数，向所述客户端发送通知；

接收单元，用于接收所述客户端返回的选择的公开参数的响应；

获取单元，用于根据所述接收单元接收的响应，获取所述公开参数保存单元中保存的公开参数。

24．如权利要求 20 所述服务器，其特征在于，所述公开参数获取模块具体包括：

发送单元，用于向所述客户端发送至少一套公开参数；

接收单元，用于接收所述客户端返回的选择的公开参数的响应；

获取单元，用于根据所述接收单元接收的响应，获取一套公开参数。

25．如权利要求 20 所述服务器，其特征在于，所述公开参数获取模块具体包括：

PKG 标识发送单元，用于向所述客户端发送至少一个私钥生成器 PKG 标识；

接收单元，用于接收所述客户端返回的选择的 PKG 标识；

获取单元，用于所述接收单元接收的 PKG 标识，获取一套用于所述 IBE 的公开参数。

26．如权利要求 20 所述服务器，其特征在于，所述公开参数获取模块具体包括：

地址标识发送单元，用于向所述客户端发送所述公开参数服务器中保存的至少一个公开参数的地址标识；

接收单元，用于接收所述客户端返回的选择的地址标识；

获取单元，用于所述接收单元接收的地址标识，获取一套用于所述 IBE 的公开参数。

27．一种提供设备，其特征在于，所述提供设备用于在服务器和客户端在基于 IBE 的安全套接层 SSL/TLS 协议的协商认证过程中，提供用于 IBE 的公开参数，其中，所述公开参数用于所述客户端根据所述公开参数和服务器标识生成 IBE 加密的预主密钥；相应地，所述服务器根据所述公开参数和获取的私钥，获取所述 IBE 加密的预主密钥的明文。

28．如权利要求 27 所述的提供设备，其特征在于，所述提供设备还用于向服务器提供私钥，所述私钥用于解密 IBE 加密的预主密钥。

说 明 书 附 图

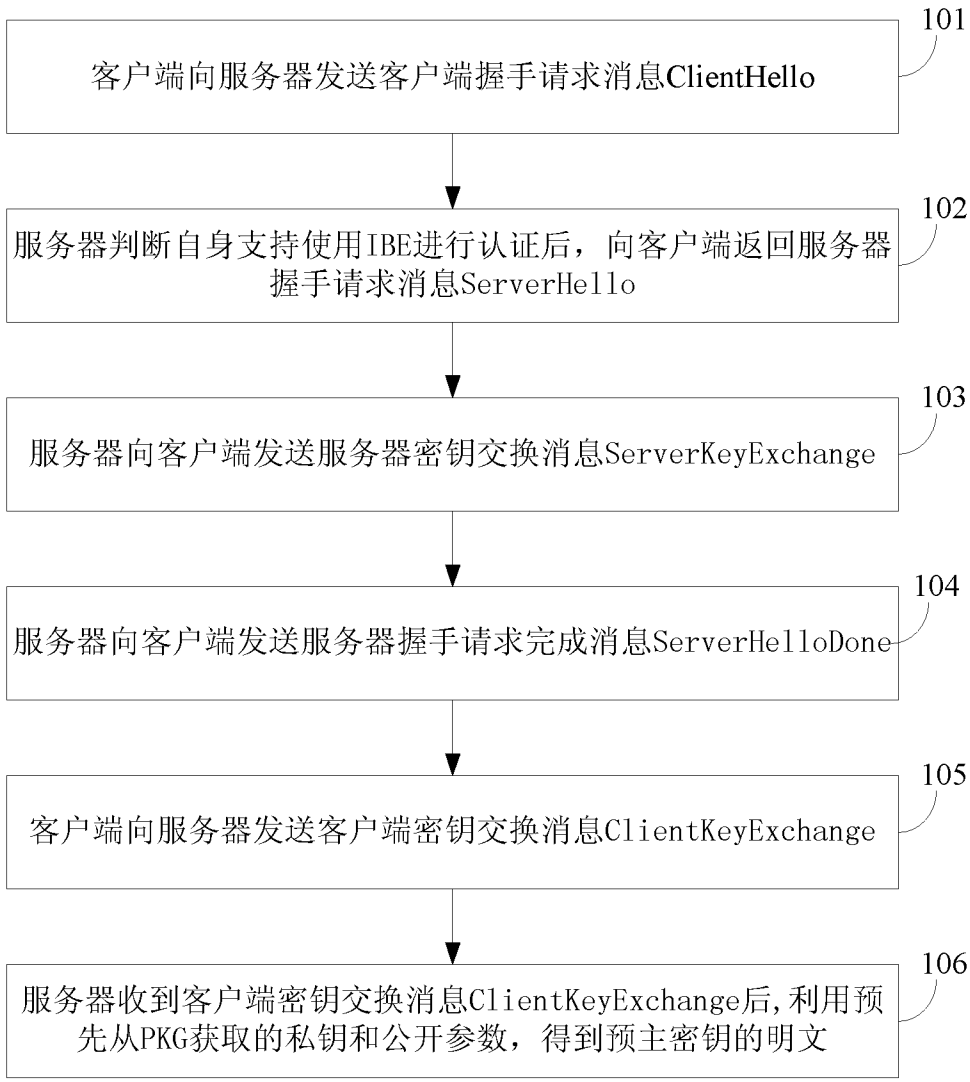
101
客户端向服务器发送客户端握手请求消息ClientHello
102
服务器判断自身支持使用IBE进行认证后，向客户端返回服务器握手请求消息ServerHello
103
服务器向客户端发送服务器密钥交换消息ServerKeyExchange
104
服务器向客户端发送服务器握手请求完成消息ServerHelloDone
105
客户端向服务器发送客户端密钥交换消息ClientKeyExchange
106
服务器收到客户端密钥交换消息ClientKeyExchange后,利用预先从PKG获取的私钥和公开参数，得到预主密钥的明文

图 1

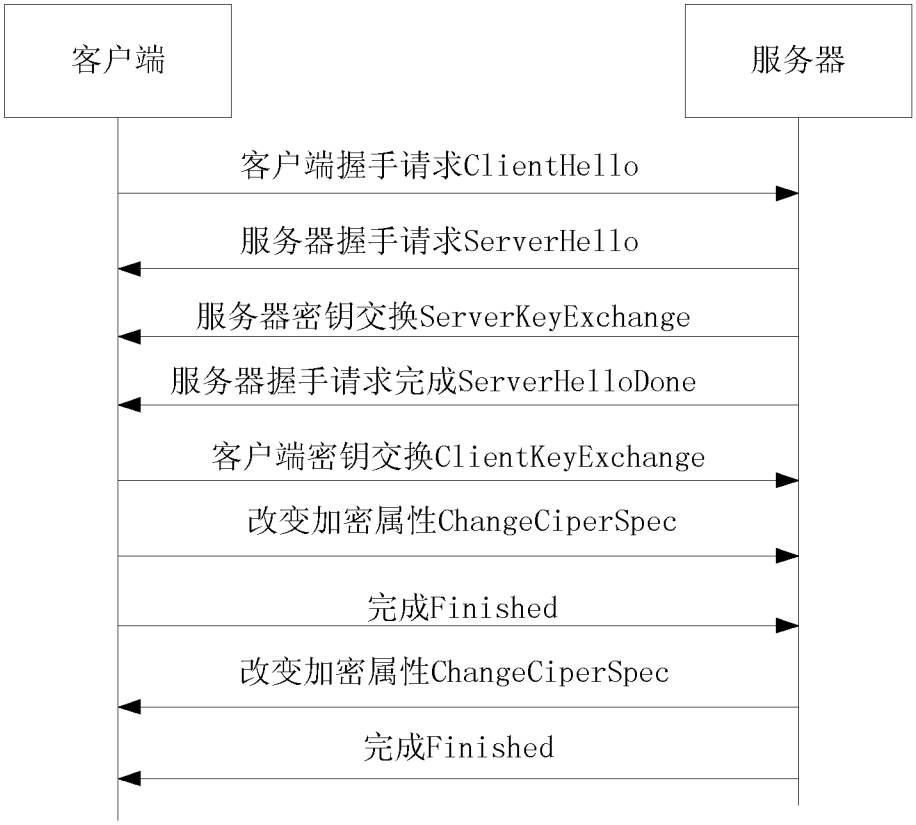
客户端
服务器
客户端握手请求ClientHello
服务器握手请求ServerHello
服务器密钥交换ServerKeyExchange
服务器握手请求完成ServerHelloDone
客户端密钥交换ClientKeyExchange
改变加密属性ChangeCiperSpec
完成Finished
改变加密属性ChangeCiperSpec
完成Finished

图 2

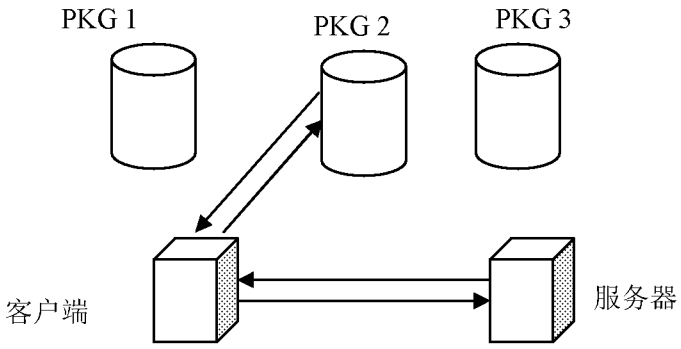
PKG 1
PKG 2
PKG 3
客户端
服务器

图 3


远程公开参数获取模块
支持 IBE 的 SSL/TLS 通信模块
预共享公开参数管理模块

图 4


客户端201
服务器202

图 5

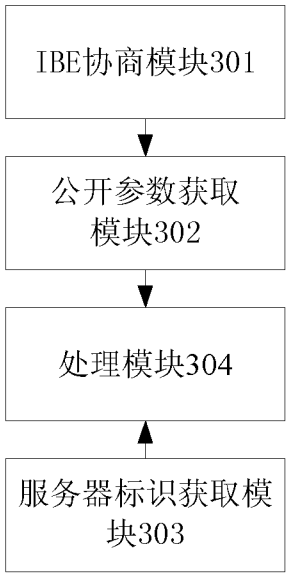
IBE协商模块301
公开参数获取模块302
处理模块304
服务器标识获取模块303

图 6

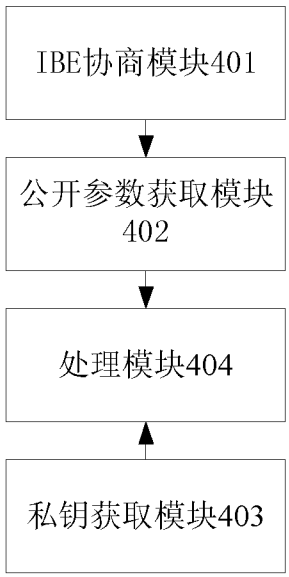
IBE协商模块401
公开参数获取模块402
处理模块404
私钥获取模块403

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/071371

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/28(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)

IPC:H04L9/-

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,PAJ: identi+, encrypt+, public, privat+, key, handshak+, negotiat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US2004179684A1 (IDENTICRYPT INC)16 Sep. 2004 (16.09.2004) See the description paragraphs 61-62,66-67,71-72,79,88-97,figure 7	1-28
A	US6886096B2 (IDENTICRYPT INC) 26 Apr. 2005 (26.04.2005) See the whole document	1-28
A	CN1633071 A (BEIJING E-HENXEN AUTHENTICATION TECHNOLO et al) 29 Jun. 2005 (29.06.2005) see the whole document	1-28

☐ 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
10 Jun. 2009(10.06.2009)	**16 Jul. 2009 (16.07.2009)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer CUI Xianli Telephone No. (86-10)62411431

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/071371

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2004179684A1	16.09.2004	WO2005010732A2	03.02.2005
		EP1604484A2	14.12.2005
		JP2006528874T	21.12.2006
US6886096B2	26.04.2005	US2004098589A1	20.05.2004
		WO2004047352A2	03.06.2004
		AU2003297271A1	15.06.2004
		EP1579625A2	28.09.2005
		JP2006506908T	23.02.2006
		AU2003297271B2	14.02.2008
		AU2003297271B8	06.03.2008
		CA2505865A1	03.06.2004
		JP2009044763A	26.02.2009
		US2009034742A1	05.02.2009
		US2008148047A1	19.06.2008
		US7424614B2	09.09.2008
CN1633071A	29.06.2005	WO2006074611A1	20.07.2006
		CN1262087C	28.06.2006
		EP1843509A1	10.10.2007
		AU2006205987A1	20.07.2006
		KR20070096014A	01.10.2007
		JP2008527866T	24.07.2008
		CA2593414A1	20.07.2006
		JP2008527866T	24.07.2008
		US2008267394A1	30.10.2008

国际检索报告

国际申请号
PCT/CN2009/071371

A. 主题的分类

H04L9/28(2006.01)i

按照国际专利分类表(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)

IPC:H04L9/-

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：标识，加密，公开，参数，私钥，握手，协商

WPI，EPDOC，PAJ：identi+，encrypt+，public，privat+，key，handshak+，negotiat+

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	US2004179684A1（IDENTICRYPT INC）16.9 月 2004（16.09.2004）参见说明书第 61-62，66-67，71-72，79，88-97 段，附图 7	1-28
A	US6886096B2（IDENTICRYPT INC）26.4 月 2005（26.04.2005）参见全文	1-28
A	CN1633071 A（北京易恒信认证科技有限公司等） 29.6 月 2005（29.06.2005）参见全文	1-28

☐ 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

"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
10.6 月 2009（10.06.2009）	**16.7 月 2009 (16.07.2009)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 崔宪丽 电话号码：(86-10) **62411431**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2009/071371

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2004179684A1	16.09.2004	WO2005010732A2	03.02.2005
		EP1604484A2	14.12.2005
		JP2006528874T	21.12.2006
US6886096B2	26.04.2005	US2004098589A1	20.05.2004
		WO2004047352A2	03.06.2004
		AU2003297271A1	15.06.2004
		EP1579625A2	28.09.2005
		JP2006506908T	23.02.2006
		AU2003297271B2	14.02.2008
		AU2003297271B8	06.03.2008
		CA2505865A1	03.06.2004
		JP2009044763A	26.02.2009
		US2009034742A1	05.02.2009
		US2008148047A1	19.06.2008
		US7424614B2	09.09.2008
CN1633071A	29.06.2005	WO2006074611A1	20.07.2006
		CN1262087C	28.06.2006
		EP1843509A1	10.10.2007
		AU2006205987A1	20.07.2006
		KR20070096014A	01.10.2007
		JP2008527866T	24.07.2008
		CA2593414A1	20.07.2006
		JP2008527866T	24.07.2008
		US2008267394A1	30.10.2008