

(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
2016 年 7 月 7 日 (07.07.2016)



(10) 国际公布号
WO 2016/107322 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2015/094851

(22) 国际申请日: 2015 年 11 月 17 日 (17.11.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410849886.7 2014 年 12 月 30 日 (30.12.2014) CN

(71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: 杭程 (HANG, Cheng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。石彦伟 (SHI, Yanwei); 中国北京市朝阳区酒仙桥路 6 号

院 2 号楼, Beijing 100015 (CN)。贾正强 (JIA, Zhengqiang); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: IMPLEMENTATION METHOD FOR SECURE BROWSER, AND SECURE BROWSER DEVICE

(54) 发明名称: 安全浏览器的实现方法和安全浏览器装置

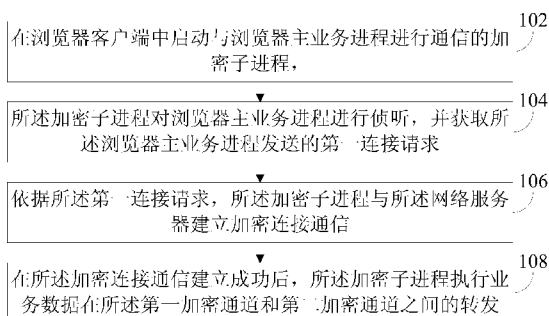


图 1 / FIG.1

102 Encryption sub-process communicating with browser main service process is started up in browser client
104 Encryption sub-process monitors browser main service process, and obtains first connection request sent by browser main service process
106 According to first connection request, encryption sub-process establishes encryption connection communication with network server
108 After encryption connection communication has been successfully established, encryption sub-process executes forwarding of service data between first encryption channel and second encryption channel

(57) Abstract: An implementation method for a secure browser, and a browser device, the method comprising: an encryption sub-process communicating with a browser main service process is started up in a browser client, the encryption sub-process being used for acting as a connection broker to implement a conversion from a first encryption channel to a second encryption channel, and data forwarding; the encryption sub-process monitors the browser main service process, and obtains a first connection request sent by the browser main service process; according to the first connection request, the encryption sub-process establishes encryption connection communication with a network server; after the encryption connection communication has been successfully established, the encryption sub-process executes the forwarding of service data between the first encryption channel and the second encryption channel, the first encryption channel being a secure communication channel of the browser main service process and the encryption sub-process, the second encryption channel being a secure communication channel of the encryption sub-process and the network server.

(57) 摘要:

[见续页]



WO 2016/107322 A1



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))。

一种安全浏览器的实现方法和浏览器装置，该方法包括：在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换及数据转发；加密子进程对浏览器主业务进程进行侦听，并获取浏览器主业务进程发送的第一连接请求；依据所述第一连接请求，加密子进程与网络服务器建立加密连接通信；在所述加密连接通信建立成功后，加密子进程执行业务数据在第一加密通道和第二加密通道之间的转发；其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

安全浏览器的实现方法和安全浏览器装置

技术领域

本发明涉及互联网技术领域，特别是涉及一种安全浏览器的实现方法和一种安全浏览器装置。

5 背景技术

浏览器是指可以显示网页服务器或者文件系统的 HTML (Hyper Text Markup Language, 超级文本标记语言) 文件内容，并让用户与这些文件交互的一种软件。浏览器主要通过 HTTP (HyperText Transfer Protocol, 超文本传送协议) 与网页服务器交互并获取网页，为用户在网页中显示图像、动画、文字、视频、声音以及流媒体等，堪称是应用最为广泛的客户端程序之一。个人电脑上常见的浏览器包括微软的 IE (Internet Explorer)、苹果的 Safari、谷歌的 Chrome、360 安全浏览器、搜狗高速浏览器等。

随着互联网的快速发展，网络应用已经成为一种趋势，越来越多的网络应用可以在浏览器中实现，如网上证券、网上银行、电子政务、电子商务、网上办公等。进而越来越多的信息在网络中流转，但是浏览器中的网络应用认证机制较弱，明文传输等安全隐患严重阻碍了信息化的发展，如何保护这些数据的流转安全是浏览器实现网络应用面临的一个重要问题。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的安全浏览器的实现方法和相应的安全浏览器装置。

依据本发明的一个方面，提供了一种安全浏览器的实现方法，包括：在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；所述加密子进程对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信；在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发；其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

根据本发明的另一方面，提供了一种安全浏览器装置，包括：一处理器，该处理器中运行有一浏览器主业务进程模块和加密子进程模块，其中，所述浏览器主业务进程模块，用于在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程的加密子进

程模块，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；所述加密子进程模块，包括：代理子模块，用于对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；以及在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发；安全连接子模块，用于依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信；其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

根据本发明的另一方面，提供了一种程序，包括可读代码，当所述可读代码在计算设备上运行时，导致所述计算设备执行根据本发明实施例所述的安全浏览器的实现方法。

根据本发明的另一方面，提供了一种可读介质，其中存储了如本发明实施例所述的程序。

本实施例可以通过加密子进程作为代理实现第一加密通道到第二加密通道的转换，以及数据转发，成功在浏览器的主业务进程与网络服务器之间建立了一条安全的加密通道，保证了业务数据的安全传输，可以降低业务数据泄露的风险，提高业务数据传输的安全性和可靠性。而且，由于本实施例通过浏览器实现上述功能，因此在用户使用浏览器客户端的过程中，浏览器客户端可以自动启动加密子进程在主业务进程与网络服务器之间建立安全通道，实现上述功能，提高了浏览器与网络服务器进行数据流转的安全性和可靠性，使得安全浏览器得以实现。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且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，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的一种安全浏览器的实现方法的流程图；

图 2 示出了根据本发明一个实施例的一种安全浏览器的实现方法的流程图；

图 3 示出了根据本发明一个实施例的加密子进程的一种代理机制示意图；

图 4 示出了根据本发明一个实施例的加密子进程和网络服务器的握手过程示意图；

图 5 示出了根据本发明一个实施例的一种安全浏览器装置的结构框图；

图 6 示出了根据本发明一个实施例的一种安全浏览器装置的结构框图；

图 7 示出了根据本发明一个实施例的加密子进程的结构框图；以及

图 8 示出了根据本发明一个实施例的主业务进程的结构框图；

图 9 示出了用于执行根据本发明的安全浏览器的实现方法的计算设备的框图；

图 10 示出了用于保持或者携带实现根据本发明的安全浏览器的实现方法的程序代
5 码的存储单元。

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
10 范围完整的传达给本领域的技术人员。

实施例一：

参照图 1，示出了根据本发明一个实施例的一种安全浏览器的实现方法实施例的步骤
流程图，具体可以包括如下步骤：

步骤 102，在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，
15 所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据
转发。

对于一些网站，如银行网站、支付宝网站等涉及金融业务的网站需要通过以安全为
目标的 HTTP (Hyper Text Transfer Protocol, 超文本传送协议) 通道进行加密数据的传输，
但是有时浏览器主业务进程与网络服务器采用不同的加密协议或算法，导致两者无法直
20 接通信，无法对该网络服务器的网页进行访问。

本实施例中，提供了一种安全浏览器客户端，其在浏览器中还设置了与浏览器主业
务进程进行通信的加密子进程。为了使得安全浏览器能够实现，需要首先在浏览器客户
端中启动与浏览器主业务进程进行通信的加密子进程。所述加密子进程的主要功能是作
为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发。即采用加密子进
25 程作为主业务进程的代理，其既能与浏览器主业务进程进行加密的安全通行，也能够与
网络服务器进行加密的安全通信，如对于浏览器主业务进程的业务数据通过第一加密通
道发送给加密子进程，该加密子进程将业务数据通过第二加密通道传输给网络服务器，
实现数据转发以及两个加密通道的连通。

需要说明的是，通常情况下，浏览器的主业务进程与网络服务器直接进行通信，但
30 是，在以安全为目标的 HTTP 通道进行通信时，若主业务进程无法对网络服务器反馈的
数据信息进行解析，启动所述加密子进程作为代理连接，即所述加密子进程作为所述主

业务进程与所述网络服务器之间的代理。本实施例中上述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和网络服务器的安全通信通道。因此所述加密子进程通过将加密子进程与所述主业务进程的第一加密通道，转换为加密子进程与网络服务器的第二加密通道，来实现所述主业务进程与
5 所述网络服务器之间的连接代理。当然对于主业务进程通过所述第一加密通道发送给加密子进程的业务数据，加密子进程可以将所述业务数据通过第二加密通道发送给网络服务器。

步骤 104，所述加密子进程对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求。

10 加密子进程对浏览器主业务进程进行侦听，是为了第一时间获取浏览器主业务进程发送的第一连接请求。具体实现时，加密子进程可以通过服务端口对所述浏览器主业务进程进行侦听。当加密子进程侦听到第一连接请求到来时，加密子进程接收所述主业务进程发送的第一连接请求。所述浏览器主业务进程发送的第一连接请求，具体可以包括业务数据。

15 步骤 106，依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信。

加密子进程接收到主业务进程发送来的第一连接请求之后，所述加密子进程依据所述第一连接请求，与所述网络服务器建立加密连接通信。所述加密子进程与所述网络服务器建立加密连接通信，即所述加密子进程和所述网络服务器进行安全认证，以确认是
20 安全、合法的通信方，从而建立安全通信的通道。

需要说明的是，所述加密子进程与所述网络服务器建立加密连接通信，结合加密子进程与主业务进程也可以进行通信，因此加密子进程分别与主业务进程和网络服务器这两端建立了相应连接，加密连接通信可以作为所述两端进行数据交换的桥梁。

步骤 108，在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第
25 一加密通道和第二加密通道之间的转发。

本实施例中所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

所述加密子进程与所述网络服务器成功建立加密连接通信，意味着加密子进程与网络服务器之间能够相互发送数据，并且这些数据经加密处理，可以保证数据流转的安全
30 可靠。加密子进程可以将接收到的所述第一连接请求中的业务数据发送给网络服务器，具体地，加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发，即加密子进程可以通过所述第一加密通道接收业务数据，进行解密后，再采用第二加密通

道约定的加密方法对业务数据进行加密后，发送给所述网络服务器。这样所述业务数据就从第一加密通道转发至第二加密通道，代表业务数据从主业务进程转发至网络服务器了。

本实施例首先在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；然后所述加密子进程对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；接着依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信；最后在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发；其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。本实施例可以通过加密子进程作为代理实现第一加密通道到第二加密通道的转换，以及数据转发，成功在浏览器的主业务进程与网络服务器之间建立了一条安全的加密通道，保证了业务数据的安全传输，可以降低业务数据泄露的风险，提高业务数据传输的安全性和可靠性。而且，由于本实施例通过浏览器实现上述功能，因此在用户使用浏览器客户端的过程中，浏览器客户端可以自动启动加密子进程在主业务进程与网络服务器之间建立安全通道，实现上述功能，提高了浏览器与网络服务器进行数据流转的安全性和可靠性，使得安全浏览器得以实现。

实施例二：

在上述实施例的基础上，本实施例继续论述安全浏览器的实现方法。

参照图 2，示出了根据本发明一个实施例的一种安全浏览器的实现方法实施例的步骤流程图，具体可以包括如下步骤：

步骤 202，在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发。

本实施例中在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，可以由浏览器自动启动，具体地，当浏览器主业务进程与网络服务器通信失败时，浏览器自动启动所述加密子进程，所述加密子进程接收主业务进程的第一连接请求，根据所述第一连接请求中包含的业务数据进行相应处理，形成浏览器主业务进程的代理连接。

本实施例中上述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和网络服务器的安全通信通道。因此所述加密子进程通过将加密子进程与所述主业务进程的第一加密通道，转换为加密子进程与网络服务器的第二加密通道，来实现所述主业务进程与所述网络服务器之间的连接代理。

当然对于主业务进程通过所述第一加密通道发送给加密子进程的业务数据，加密子进程可以将所述业务数据通过第二加密通道发送给网络服务器。

本实施例中，浏览器主业务进程与加密子进程采用代理及 IPC（Inter-Process Communication，进程间通信）两种通信方式，从而加密子进程可以作为连接代理，负责和浏览器主业务进程第一加密通道，到和网络服务器的第二加密通道的通道转换及数据转发，而 IPC 通信方式负责进程间数据传递。本实施例中，加密子进程代理实现机制如图 3 所示，具体可以包括如下结构：

主线程：读取各类配置，创建监听线程、主业务线程，以及浏览器主进程 IPC 通。

侦听线程：用于监听服务端口，当有主业务进程存在连接请求并接收（accept）成功执行相应的代理操作。

业务处理线程：与主业务进程和网络服务器两端分别建立相应加密通道连接并维持，从而作为桥梁进行两端的数据交换。

步骤 204，所述加密子进程对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求。

所述加密子进程对浏览器主业务进程进行侦听，具体可以通过以下方式来实现：所述加密子进程创建侦听线程；所述侦听线程通过服务端口对所述浏览器主业务进程进行侦听。当侦听线程侦听到第一连接请求到来时，接收所述主业务进程发送的第一连接请求。所述浏览器主业务进程发送的第一连接请求，具体可以包括业务数据。加密子进程对浏览器主业务进程进行侦听，是为了第一时间获取浏览器主业务进程发送的第一连接请求。

步骤 206，依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信。

本实施例中依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信，具体可以包括以下子步骤：

子步骤一，在确认所述第一连接请求接收成功后，所述加密子进程与所述网络服务器依次进行加密数据协商和证书认证。

子步骤二，在加密数据协商完毕且证书认证通过后，建立所述浏览器客户端与网络服务器的加密连接通信。

需要说明的是，所述子步骤一中加密子进程与所述网络服务器进行加密数据协商的步骤，具体可以通过以下方式来实现：首先，所述加密子进程向所述网络服务器发送客户端问候消息，其中，所述客户端问候消息包括所述浏览器客户端的第一加密数据，所述第一加密数据包括若干协议版本号；其次，所述网络服务器向所述加密子进程反馈服

务端问候消息，其中，所述服务端问候消息包括所述服务器客户端的第二加密数据，所述第二加密数据包括：从所述第一加密数据中选定的协议版本号。需要说明的是，上述客户端问候消息和服务端问候消息用于确定双方的安全传输能力，包括若干协议版本号、会话标识、密码套件等属性，并且产生和交换随机数。

5 客户端问候消息 (ClientHello 消息) 作为浏览器客户端和网络服务器握手协议的第一条消息，所述加密子进程向所述网络服务器发送客户端问候消息之后，等待网络服务器返回服务器问候消息。客户端问题消息结构定义：

1、Clie_vision 表示客户端在这个会话中使用的协议版本。如协议版本号是 1.1。

2、Radom 是客户端产生的随机信息，其内容包括始终和随机数。

10 3、session_id 是客户端在连接中使用的会话标识。session_id 是一个可变长字段，其值由服务器决定。如果没有可重用的会话标识或希望协商安全参数，该字段为空，则表示客户端希望重用该会话。这个会话标识可能是之前的连接标识，当前连接标识，或其他处于连接状态的连接标识。会话标识生成后应一致保持到被超时删除或与这个会话相关的连接遇到致命错误被关闭。一个会话失效或被关闭时则与其相关的连接都应被强
15 制关闭。

4、cipher_suites 是客户端所支持的密码套件列表，客户端应按照密码套件使用的优先级顺序排列，优先级最高的密码套件应排在首位。如果会话标识字段不为空，本字段应至少包含将重用的会话所使用的密码套件。每个密码套件包括一个密钥交换算法，一个加密算法和一个校验算法。服务器将在密码套件列表选择一个与之匹配的密码套件，
20 如果没有可匹配的密码套件，应返回握手失败报警消息并且关闭连接。

5、compression_methods 是客户端所支持的压缩算法列表，客户端应该按照压缩算法使用的优先级顺序排列，优先级最高的压缩算法排在首位。服务器将在压缩算法列表选择一个与之匹配的压缩算法，列表中必须包含空压缩算法，这样客户端和服务端总能协商出一致的压缩算法。

25 需要说明的是，服务器如果能从客户端问候消息中找到匹配的密码套件，服务器发送所述服务端问候消息 (Server Hello 消息) 作为对客户端问候消息的回复。如果找不到匹配的密码套件，服务器将回应报警消息。

需要说明的是，所述子步骤一中加密子进程与所述网络服务器依次进行证书认证的步骤，具体可以包括：所述加密子进程对所述网络服务器进行单向证书认证；或，所述
30 加密子进程和所述网络服务器进行双向证书认证。

本发明一个可选实施例中，在进行数字证书的双向认证时，所述加密子进程弹出证书选择框，并在所述证书选择框中显示所述浏览器所在终端中加载的各用户证书的信息；

通过所述证书选择框接收用户选择的用户证书。。

还包括：所述加密子进程显示口令输入消息，所述口令输入消息用于提示用户输入所述用户证书对应的保护口令；所述加密子进程接收用户输入的保护口令，并对所述保护口令进行验证，在确认所述保护口令确认所述用户具有所述用户证书的使用权限。

- 5 本实施例中，为了保证访问网站和用户的安全，CA (Certificate Authority, 认证中心) 机构为不同的网站颁布不同的站点证书，同时为不同网站的不同用户颁布不同的用户证书。其中，数字证书中包括站点或用户的公钥，站点或用户的信息，以及数字签名等内容。

- 10 在双向认证过程中，所述加密子进程可以在浏览器客户端中弹出证书选择框，并在所述证书选择框中显示所述浏览器所在终端中加载的各用户证书的信息；通过所述证书选择框接收用户选择的用户证书，用户在对用户证书进行选择后，所述加密子进程显示口令输入消息，所述口令输入消息用于提示用户输入所述用户证书对应的保护口令，如输入个人识别码 (Personal Identification Number, PIN)，所述加密子进程接收用户输入的保护口令，并对所述保护口令进行验证，即通过保护口令可以对用户身份进行认证，确
15 认用户是否具有该用户证书的使用权项，从而在保护口令输入正确后确认所述用户具有所述用户证书的使用权限。并且，上述用户证书和保护口令可以作为用户证书认证过程中的认证数据发送给网络服务器。

- 可选的，还包括：所述加密子进程通过提示信息提示用户插入安全密钥存储硬件，所述安全密钥存储硬件中存储有用户证书；所述加密子进程调用驱动程序检测所述安全
20 密钥存储硬件；当检测到所述安全密钥存储硬件后，所述加密子进程获取所述安全密钥存储硬件中存储的用户证书的信息。

- 浏览器客户端加载用户证书时，首先所述加密子进程通过提示信息提示用户插入安全密钥存储硬件，该安全密钥存储硬件即 USB Key，它是一种 USB (Universal Serial Bus, 通用串行总线) 接口的硬件设备，内置单片机或智能卡芯片，有一定的存储空间，可以
25 存储用户的私钥以及数字证书，利用 USB Key 内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。

- 所述加密子进程通过驱动识别安全密钥存储硬件，并依据所述硬件证书载体在双向证书认证过程中进行加密运算。例如，SSL (Secure Sockets Layer, 安全套接层) 连接建立过程中如果需要双向认证，所述加密子进程会提示用户插入安全密钥存储硬件，即
30 USBKey 设备。在用户插入安全密钥存储硬件后能够自动识别并弹出证书选择对话框，提示用户选择证书。所述加密子进程自动识别安全密钥存储硬件需要依赖 CSP

(Cryptographic Service Provider, 加密服务提供) 注册表项中的两个关键信息:
SKFImagePath: 指定 SKF 动态库的路径和 TokenVidPid: 字符串格式。

KEY 设备的 VendorID 和 ProductID, 采用的格式类似 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB 中的格式, 也即 VID_XXXX&PID_XXXX。浏览器会通过 USBKey 设备的 vendorid、productid 关联到相应驱动, 完成相关操作。浏览器不会存储用户输入的 pin 密码, 也不会存储 USBKey 中的私钥信息。具体流程如下: 首先连接到 USBKey 设备; 然后打开相应应用 (Application), Application 由用户选择决定; 然后打开相应容器 (Container), Container 由用户选择决定; 接着校验 PIN 码 (个人身份识别码), 验证错误后会提示重新输入; 然后获取签名证书信息; 接着获取加密证书信息; 最后关闭设备、断开连接。

1、单向认证

在本发明实施例的一种可选示例中, 所述加密子进程对所述网络服务器进行单向证书认证, 具体可以通过以下方式来实现: 首先, 所述加密子进程接收所述网络服务器发送的服务端证书消息, 所述服务端证书消息包括所述网络服务器的站点签名证书; 其次, 所述加密子进程对所述网络服务器的站点签名证书进行认证。下面对服务端证书消息 (Server Certificate 消息) 进行说明, 网络服务器需要发送一个服务端证书消息给客户端, 该消息总是紧跟在服务端问候消息之后, 当选中的密码套件使用 RSA 或 ECC 或 ECDHE 算法时, 所述服务端证书消息的内容为服务端标识和 IBC 公共参数, 用于客户端与服务器协商 IBC 公开参数。密钥交换算法与证书密钥类型的关系如表 1 所示。

密钥交换算法	证书密钥类型
RSA	RSA 公钥, 必须使用加密证书中的公钥
IBC	服务端标识和 IBC 公共参数
IBSDH	服务端标识和 IBC 公共参数
ECC	ECC 公钥, 必须使用加密证书中的公钥
ECDHE	ECC 公钥, 必须使用加密证书中的公钥

表 1, 密钥交换算法与证书密钥类型关系表

2、双向认证

在本发明实施例的一种可选示例中, 所述加密子进程和所述网络服务器进行双向证书认证, 具体可以通过以下方式来实现:

1) 所述加密子进程接收所述网络服务器发送的服务端证书消息, 所述服务端证书消息包括所述网络服务器的站点签名证书;

2) 所述加密子进程接收所述网络服务器发送的证书认证请求消息, 所述证书认证请

求消息用于指示进行客户端的证书认证;

3) 所述加密子进程接收所述网络服务器发送的服务端密钥交换消息, 包括密钥交换参数;

4) 所述加密子进程接收所述网络服务器发送的服务端问候完结消息;

5) 所述加密子进程对所述站点签名证书进行认证;

6) 当所述站点签名证书认证通过后, 所述加密子进程向所述网络服务器发送客户端证书消息, 所述客户端证书消息包括所述浏览器客户端的签名证书, 以使所述网络服务器对所述签名证书进行认证。

在本发明实施例的一种可选示例中, 所述的方法还包括密钥交换的步骤: 所述加密子进程依据所述密钥交换参数随机产生预主密钥, 其中, 所述预主密钥是采用所述网络服务器的加密公钥通过椭圆曲线密码算法 SM2 进行加密计算得到的; 所述加密子进程采用所述预主密钥生成客户端密钥交换消息, 并发送给网络服务器, 以使所述网络服务器获取所述预主密钥。

在本发明实施例一种可选示例中, 所述的方法还包括验证证书签名的步骤, 具体包括: 所述加密子进程获取依据站点签名证书计算的签名校验参数, 并生成客户端证书校验消息发送给所述网络服务器; 所述加密子进程向所述网络服务器发送客户端密码规格变更消息, 以表征加密数据的协商完成; 所述加密子进程向所述网络服务器发送客户端握手结束消息; 所述加密子进程接收所述网络服务器发送的服务端密码规格变更消息, 以表征认可该加密数据的协商; 所述加密子进程接收所述网络服务器发送的服务端握手结束消息。需要说明的是, 国密 SSL 连接过程的每次 SSL 握手处理中, 都对服务器证书进行了严格的验证。

本实施例中, 上述加密数据协商、证书认证、密钥交换以及签名认证都是在安全浏览器客户端的加密子进程和网络服务器的握手过程中执行的。本实施例中, 双向认证采用了双证书机制, 证书的非对称算法采用 SM2 算法, 使用签名证书基于 ECDSA 签名实现身份认证, 使用加密证书基于 ECDH 实现密钥协商。使用的 SM4 算法对数据进行加密, 使用 SM3 算法对数据进行摘要。

其中, SM2 算法 (SM2 algorithm) 是一种椭圆曲线公钥密码算法, 其密钥长度为 256 比特。SM3 算法 (SM3 algorithm) 是一种密码杂凑算法, 其密钥长度为 128 比特, SM4 算法 (SM4 algorithm) 是一种分组密码算法, 分组长度为 128 比特, 密钥长度为 128 比特。

如图 4 所示, 加密子进程和网络服务器的握手过程包括:

4.02、加密子进程发送客户端问候消息 ClientHello 给网络服务器。

4.04、网络服务器发送服务端问候消息 SeverHello 给所述安全安全浏览器客户端的加密子进程。

其中，网络服务器从 ClientHello 消息中找到匹配的密码套件，发送 SeverHello 作为回复，若找不到匹配的密码套件，则发送报警消息。该 SeverHello 中，Sever_vision，表示服务器支持的版本号，如 1.1；Radom 服务器端产生的随机数；session_id 服务端使用的会话标识；cipher_suites 服务端从 ClientHello 消息中选取的密码套件；compression_methods 服务端从 ClientHello 消息中选取的压缩算法。

4.06、网络服务器发送服务端证书消息 Certificate 给加密子进程。

即 SeverCertificate 本消息内容为签名证书和加密证书。如服务端的站点签名证书（X.509 序列）

4.08、网络服务器发送证书认证请求消息 SeverRequest 给加密子进程。

通过 SeverRequest 消息要求客户端提供证书。同时指明了认证类型（ECDSA）

4.10、网络服务器发送服务端密钥交换消息 SeverKeyExchange 给加密子进程。

SeverKeyExchange 用于客户端计算产生 48 字节的预主密钥。公钥可以直接从服务器端的加密证书中获取。如客户端随机产生预主密钥 pre_master_secret 密钥，并使用服务器证书的公钥进行 ECDH 运算

4.12、网络服务器发送问候完结消息 SeverHelloDone 给加密子进程。

SeverHelloDone 表征握手过程的 hello 消息阶段完成，然后等待客户端的响应消息。

4.14、加密子进程发送客户密钥交换消息 Certificate 给网络服务器。

即 ClientCertificate 消息是 hello 消息阶段完成后的第一条消息，如包括客户的签名证书（X.509 序列）。

4.16、加密子进程发送客户密钥交换消息 ClientKeyExchange 给网络服务器。

ClientKeyExchange 消息中网络服务器的公钥加密预主密钥。

4.18、加密子进程发送证书校验消息 CertificateVerify 给网络服务器。

CertificateVerify 消息用于鉴别客户端是够为证书的合法持有者。本实施例中，提示用户插入 USBKey 后可以提示用户输入保护口令，该保护口令即携带在该消息中验证用户是否合法。如，客户端使用签名证书的 ECC 私钥对握手信息的摘要进行 ESDSA 签名。

4.20、加密子进程发送客户端密码规格变更消息 ChangeCipherSpec 给网络服务器。

即 ClientChangeCipherSpec 消息向服务端表明算法及密钥协商完成。

4.22、加密子进程发送客户端握手结束消息 Finished 给网络服务器。

本实施例中，加密子进程根据客户端的随机数、服务端的随机数、pre_master_secret 使用密钥算法计算 master_secret，然后再使用随机数和 master_secret 计算真正的数据加

密密钥，然后将所有握手消息摘要后加密形成 ClientFinished 消息向服务端发送。

4.24、网络服务器发送服务端密码规格变更消息 ChangeCipherSpec 给加密子进程。

4.26、网络服务器发送服务端握手结束消息 Finished 给加密子进程。

5 服务端验证客户端证书，使用客户端的签名证书验证客户端的签名。服务使用自身的加密私钥和进行 ECDH 运算，获得 pre_master_secret，采用客户端同样的算法计算 master_secret 和数据加密密钥，验证 ServerFinished 消息的正确性，向客户端发送 ServerChangeCipherSpec 消息，表示认可算法及密钥协商。

通过上述握手过程完成了浏览器客户端和网络服务器双方的认证、密钥协商等过程，从而加密子进程和网络服务端可以分别使用协商计算出的密钥加密应用数据。

10 步骤 208，在所述加密连接通信建立成功后，建立为所述加密子进程和所述网络服务器进行安全通信的第二加密通道。

所述加密子进程和所述网络服务器在第二加密通道中进行加密通信。具体地，可以将第二加密通道中进行通信的数据采用对称加密算法 SM4 对业务数据进行加密。

15 步骤 210，所述加密子进程创建业务处理线程；所述业务处理线程分别与所述第一加密通道和所述第二加密通道建立连接。

所述加密子进程创建的业务处理线程，与所述加密子进程与主业务进程之间的第一加密通道，和所述加密子进程与网络服务器之间的第二加密通道都建立连接。所述业务处理线程具体作为所述主业务进程和所述网络服务器之间的桥梁进行两端的数据交换。

20 步骤 212，在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发。

本实施例中所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发，具体可以通过以下方式来实现：所述业务处理线程通过所述第一加密通道接收所述浏览器主业务进程发送的第一业务数据；所述业务处理线程采用第一对称算法对所述第一业务数据进行解密处理，获取原始业务数据；所述业务处理线程采用第二对称算法对所述原始业务数据进行加密处理，获取所述第二业务数据；所述业务处理线程采用
25 通过所述第二加密通道间所述第二业务数据发送给所述网络服务器。需要说明的是，上述过程是数据通信过程中加密子进程分别对两个通道数据转换的过程。

在本发明实施例的一种可选示例中，所述加密子进程和所述浏览器主业务进程通过握手过程建立加密连接通信，并在加密连接通信成功后，建立为所述浏览器主业务进程
30 和所述加密子进程进行安全通信的第一加密通道；其中，所述握手过程中执行通过第一非对称算法执行所述加密子进程和所述浏览器主业务进程之间的双向证书认证、密钥交换，以及执行证书认证；所述密钥交换过程中生成对称密钥。需要说明的是，第一非对

称算法具体可以是 RSA 算法。

在本发明实施例的一种可选示例中，所述安全浏览器的实现方法还包括：所述业务处理线程将第一连接请求通过第二对称算法进行加密处理得到第二连接请求；所述业务处理线程将所述第二连接请求发送给所述网络服务器；所述业务处理线程接收所述网络服务器基于所述第二连接请求反馈的第二连接应答；第二连接请求将所述第二连接应答通过第二对称算法进行解密处理得到第一连接应答，并反馈给所述浏览器主业务进程。

需要说明的是，业务处理线程的具体流程如下：（1）接收代理数据，具体接收代理连接的 http request 数据。（2）与网络服务器进行 SSL 连接，具体包括 SSL 连接的建立，SSL 协议协商，算法协商，客户端证书验证（CRL 检查或 OCSP 认证）（3）与 web 服务器交互。具体将代理连接 http request 数据经由国密 SSL 通道发给 Web 服务器，获取 Web 服务器的 http response。（4）发送网络服务器返回数据给代理连接。具体将网络服务器的 http response 转给代理连接。（5）关闭连接。业务处理流程中如果发生错误，则关闭连接，同时给代理连接返回错误页面。需要说明的是，所述第二对称算法具体可以是国密算法。

需要说明的是，采用 SSL 的安全技术解决网络应用身份认证以及数据保密性得到广泛的认可，主流的浏览器和网络服务器中也内置了 SSL 模块，专业的 SSL 硬件产品也广泛使用。但当前 SSL 产品还都存在一定局限性：

（1）当前 SSL 产品普遍采用单证书机制。而双证书机制是当前 PKI（Public Key Infrastructure，公钥基础设施）体系建设的主流模式。本实施例使用签名证书进行身份认证，使用加密证书进行密钥的交换和保护，发挥了 PKI 技术非对称密钥的优势。

（2）当前的 SSL 产品中普遍采用国外公开的对称算法，不符合保密要求，具有一定风险性。本实施例中密码产品对称算法采用 SM1 算法或 SM4 算法。

（3）当前的证书非对称算法采用 RSA 算法，而本实施例采用的椭圆曲线密码（ECC）是一种比 RSA 具有更高安全性、更高效率的公钥密码，具有加密/解密、数字签名和密钥协商等重要的密码功能，可以安全且方便地满足各种信息网络中的用户身份识别、电子信息的真伪鉴别和保密传输等重要的信息安全需求，是信息安全领域的核心技术，并已逐渐被诸多国际和国家标准组织采纳为公钥密码标准（IEEE P1363、ANSI X9、ISO/IEC 和 IETF 等），将会成为信息安全产业界使用的主流密码技术之一。可以将该 ECC（ECDSA+ECDH）算法命名为 SM2。

本实施例提供的安全浏览器的实现方法，可以实现符合该 PKI 机制和密码产品管理政策的网络安全浏览器，对国内安全产品的管理的规范性和网络应用的快速增长都起到积极的推动作用。

对于方法实施例，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，本发明实施例并不受所描述的动作顺序的限制，因为依据本发明实施例，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，所涉及的动作并不一定是本发明实施例所必须的。

5 实施例三：

在上述实施例的基础上，本实施例还公开了一种浏览器装置。

参照图 5，示出了根据本发明一个实施例的一种安全浏览器装置实施例的结构框图，具体可以包括：一处理器 50，该处理器中运行有一浏览器主业务进程模块 502 和加密子进程模块 504，

10 其中，所述浏览器主业务进程模块 502，用于在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程的加密子进程模块，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发。

在本发明实施例的如图 6 所示的一种可选示例中，所述加密子进程模块 504，包括：代理子模块 5042 和安全连接子模块 5044，其中：代理子模块 5042，用于对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；以及在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发。安全连接子模块 5044，用于依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信。其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

在本发明实施例的一种可选示例中，所述代理子模块，用于所述加密子进程创建侦听线程；所述侦听线程通过服务端口对所述浏览器主业务进程进行侦听。

在本发明实施例的一种可选示例中，所述安全连接子模块，用于在确认所述第一连接请求接收成功后，所述加密子进程与所述网络服务器依次进行加密数据协商和证书认证；在加密数据协商完毕且证书认证通过后，建立所述浏览器客户端与网络服务器的加密连接通信。

在本发明实施例的一种可选示例中，所述安全连接子模块，用于所述加密子进程向所述网络服务器发送客户端问候消息，其中，所述客户端问候消息包括所述浏览器客户端的第一加密数据，所述第一加密数据包括若干协议版本号；所述网络服务器向所述加密子进程反馈服务端问候消息，其中，所述服务端问候消息包括所述服务器客户端的第二加密数据，所述第二加密数据包括：从所述第一加密数据中选定的协议版本号。

在本发明实施例的一种可选示例中，所述安全连接子模块，用于对所述网络服务器

进行单向证书认证；或，所述加密子进程和所述网络服务器进行双向证书认证。

在本发明实施例的一种可选示例中，所述代理子模块，还用于创建业务处理线程；所述业务处理线程分别与所述第一加密通道和所述第二加密通道建立连接。

在本发明实施例的一种可选示例中，所述代理子模块，用于采用所述业务处理线程
5 通过所述第一加密通道接收所述浏览器主业务进程发送的第一业务数据；所述业务处理线程采用第一对称算法对所述第一业务数据进行解密处理，获取原始业务数据；所述业务处理线程采用第二对称算法对所述原始业务数据进行加密处理，获取所述第二业务数据；所述业务处理线程采用通过所述第二加密通道向所述第二业务数据发送给所述网络服务器。

10 在本发明实施例的一种可选示例中，所述安全连接子模块，用于接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书；所述加密子进程对所述网络服务器的站点签名证书进行认证。

在本发明实施例的一种可选示例中，所述安全连接子模块，用于所述加密子进程接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的
15 站点签名证书；所述加密子进程接收所述网络服务器发送的证书认证请求消息，所述证书认证请求消息用于指示进行客户端的证书认证；所述加密子进程接收所述网络服务器发送的服务端密钥交换消息，包括密钥交换参数；所述加密子进程接收所述网络服务器发送的服务端问候完结消息；所述加密子进程对所述站点签名证书进行认证；当所述站点签名证书认证通过后，所述加密子进程向所述网络服务器发送客户端证书消息，所述
20 客户端证书消息包括所述浏览器客户端的签名证书，以使所述网络服务器对所述签名证书进行认证。

在本发明实施例的一种可选示例中，所述安全连接子模块，还用于依据所述密钥交换参数随机产生预主密钥，其中，所述预主密钥是采用所述网络服务器的加密公钥通过
25 椭圆曲线密码算法 SM2 进行加密计算得到的；所述加密子进程采用所述预主密钥生成客户端密钥交换消息，并发送给网络服务器，以使所述网络服务器获取所述预主密钥。

在本发明实施例的一种可选示例中，所述安全连接子模块，还用于获取依据站点签名证书计算的签名校验参数，并生成客户端证书校验消息发送给所述网络服务器；所述
加密子进程向所述网络服务器发送客户端密码规格变更消息，以表征加密数据的协商完成；所述加密子进程向所述网络服务器发送客户端握手结束消息；所述加密子进程接收
30 所述网络服务器发送的服务端密码规格变更消息，以表征认可该加密数据的协商；所述加密子进程接收所述网络服务器发送的服务端握手结束消息。

在本发明实施例的一种可选示例中，所述安全连接子模块，还用于在所述加密连接

通信建立成功后，建立为所述加密子进程和所述网络服务器进行安全通信的第二加密通道。

在本发明实施例的一种可选示例中，所述代理子模块，还用于采用所述加密子进程和所述浏览器主业务进程通过握手过程建立加密连接通信，并在加密连接通信成功后，
5 建立为所述浏览器主业务进程和所述加密子进程进行安全通信的第一加密通道；其中，所述握手过程中执行通过第一非对称算法执行所述加密子进程和所述浏览器主业务进程之间的双向证书认证、密钥交换，以及执行证书认证；所述密钥交换过程中生成对称密钥。

在本发明实施例的一种可选示例中，所述代理子模块，还用于所述业务处理线程将
10 第一连接请求通过第二对称算法进行加密处理得到第二连接请求；所述业务处理线程将所述第二连接请求发送给所述网络服务器；所述业务处理线程接收所述网络服务器基于所述第二连接请求反馈的第二连接应答；第二连接请求将所述第二连接应答通过第二对称算法进行解密处理得到第一连接应答，并反馈给所述浏览器主业务进程。

所述加密子进程模块还包括：硬件管理子模块 5046 和证书验证子模块 5048，其中，
15 所述硬件管理模块，用于加密子进程通过驱动识别安全密钥存储硬件。所述证书验证模块，用于依据所述硬件证书载体在双向证书认证过程中进行加密运算。

需要说明的是，可以参照图 7 所示的加密子进程的结构框图对加密子进程进行理解，如图 7 所示，加密子进程包括：配置模块 702、代理模块 704、CTL 管理模块 706、CRL 管理模块 708、Session 管理模块 710、证书验证模块 712、SSL 连接模块 714、USBKey
20 操作模块 716。其中，代理模块接受浏览器主业务进程连接，根据浏览器主业务进程连接的类型进行相应处理，形成浏览器主业务进程的连接代理。CTL 模块用于管理信任根证书列表。CRL 管理模块用于获取 CRL 列表，管理本地 CRL 列表。Session 管理模块管理代理进程与 web 服务器的 session 连接。SSL 连接模块负责建立与 web 服务器的安全连接。USBKey 管理模块负责操作 USBKey 设备。配置模块负责读取、存储客户端的相关配置。

25 其中，对于 CTL 管理模块 706，其工作原理如下：CTL 描述的是浏览器信任根证书列表，用于验证服务器端证书。安全浏览器客户端中，支持的信任根证书为 PEM 编码方式，同时支持两种证书添加方式：1) 程序内部添加信任根证书；2) 配置文件添加信任根证书，配置文件采用 des 加密保存。其中，CTL 可以配置为不支持导入导出功能。

对于 CRL 管理模块 708，其工作原理如下：CRL 描述的是证书颁发机构 CA 的证书
30 撤销列表，其本质是证书序列号，证书序列号以 ASN.1 编码的 Integer 表示。X509v3 证书中的一个扩展项 (OID 为 2.5.29.31) 用于指定该证书的 CRL 发布点。本实施例的安全浏览器中装置对 CRL 进行了本地缓存，同时 CRL 查找根据 CA 进行一级索引。对 CRL

的验证操作的步骤如下：(1) 获取证书中的 Issuer 项，定位对应的 CA 节点，如果 Issuer 项不存在或者找不到对应的 CA 项，则认为是非法证书。(2) 使用二分法搜索该 CA 下所有的 CRL 项。

对于 Session 管理模块 710，SSL 连接需要在 TCP 3 次握手的基础上增加 4 次握手，连接建立过程是比较耗时的，因此保存 Session、复用之前的连接可以有效优化连接性能。本实施例的安全浏览器装置中在一次 SSL 连接建立完成之后，会建立 host+port 到 session 的内存索引，后续操作会复用之前的 session，如 session 有效期为 1 小时。浏览器关闭、USBKey 设备拔出时会清空之前的 session。

对于证书验证模块 612，SSL 连接建立过程中如果需要双向认证，所述加密子进程会提示用户插入安全密钥存储硬件，即 USBKey 设备。在用户插入安全密钥存储硬件后能够自动识别并弹出证书选择对话框，提示用户选择证书。所述加密子进程自动识别安全密钥存储硬件需要依赖 CSP 注册表项中的两个关键信息：SKFImagePath：指定 SKF 动态库的路径和 TokenVidPid：字符串格式。KEY 设备的 VendorID 和 ProductID，采用的格式类似 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB 中的格式，也即 VID_XXXX&PID_XXXX。浏览器会通过 USBKey 设备的 vendorid、productid 关联到相应驱动，完成相关操作。浏览器不会存储用户输入的 pin 密码，也不会存储 USBKey 中的私钥信息。具体流程如下：首先连接到 USBKey 设备；然后打开相应应用 (Application)，Application 由用户选择决定；然后打开相应容器 (Container)，Container 由用户选择决定；接着校验 PIN 码 (个人身份识别码)，验证错误后会提示重新输入；然后获取签名证书信息；接着获取加密证书信息；最后关闭设备、断开连接。

本实施例中，针对上述方法实施例的证书验证过程，对服务器端的证书验证发生在握手协议过程中，浏览器收到 ServerHelloDone 消息之后，发送 Certificate 消息之前。证书验证主要确保服务器的合理性，验证过程依赖于 CTL，CRL 模块，具体过程在子进程证书验证线程池中进行。检查步骤如下：初始化受信任根证书列表；检查是否是自签名证书；检查证书扩展信息；检查证书信任关系；检查 CRL 列表；检查证书签名；检查证书时间有效性；检查证书是否在黑名单中。

需要说明的是，可以参照图 8 所示的主业务进程的结构框图对主业务进程进行理解，如图 8 所示，主业务进程包括：证书显示模块 802、白名单管理模块 804、网络服务器证书存储模块 806、代理设置模块 808。其中证书显示模块 802 负责显示数字证书。白名单管理模块 804 负责管理支持本实施例的加密算法的 web 服务器列表。网络服务器证书存储模块 806 用于存储负责管理网络服务器的证书。代理设置模块 808 代理设置负责设置与加密子进程的代理。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所述的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

例如，图 9 示出了可以实现根据本发明的安全浏览器的实现方法的计算设备。该计算设备传统上包括处理器 910 和以存储器 920 形式的程序产品或者可读介质。存储器 920 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM 或者 ROM 之类的

电子存储器。存储器 920 具有用于执行上述方法中的任何方法步骤的程序代码 931 的存储空间 930。例如，用于程序代码的存储空间 930 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 931。这些程序代码可以从一个或者多个程序产品中读出或者写入到这一个或者多个程序产品中。这些程序产品包括诸如存储卡之类的程序代码载体。

5 这样的程序产品通常为如参考图 10 所述的便携式或者固定存储单元。该存储单元可以具有与图 9 的计算设备中的存储器 920 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括可读代码 931'，即可以由例如诸如 910 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

10 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的安全浏览器的实现方法和安全浏览器装置设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计
15 算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，
20 不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将
25 这些单词解释为名称。

权 利 要 求 书

1、一种安全浏览器的实现方法，包括：

在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；

5 所述加密子进程对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；

依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信；

在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发；

10 其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

2、如权利要求 1 所述的方法，其特征在于，所述加密子进程对浏览器主业务进程进行侦听，包括：

所述加密子进程创建侦听线程；

所述侦听线程通过服务端口对所述浏览器主业务进程进行侦听。

15 3、如权利要求 1 所述的方法，其特征在于，依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信，包括：

在确认所述第一连接请求接收成功后，所述加密子进程与所述网络服务器依次进行加密数据协商和证书认证；

20 在加密数据协商完毕且证书认证通过后，建立所述浏览器客户端与网络服务器的加密连接通信。

4、如权利要求 3 所述的方法，其特征在于，所述加密子进程与所述网络服务器进行加密数据协商的步骤，包括：

所述加密子进程向所述网络服务器发送客户端问候消息，其中，所述客户端问候消息包括所述浏览器客户端的第一加密数据，所述第一加密数据包括若干协议版本号；

25 所述网络服务器向所述加密子进程反馈服务端问候消息，其中，所述服务端问候消息包括所述服务器客户端的第二加密数据，所述第二加密数据包括：从所述第一加密数据中选定的协议版本号。

5、如权利要求 3 所述的方法，其特征在于，所述加密子进程与所述网络服务器依次进行证书认证的步骤，包括：

30 所述加密子进程对所述网络服务器进行单向证书认证；

或，所述加密子进程和所述网络服务器进行双向证书认证。

6、如权利要求 1 所述的方法，其特征在于，所述加密子进程执行业务数据在所述第

一加密通道和第二加密通道之间的转发之前，还包括：

所述加密子进程创建业务处理线程；

所述业务处理线程分别与所述第一加密通道和所述第二加密通道建立连接。

5 7、如权利要求 6 所述的方法，其特征在于，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发，包括：

所述业务处理线程通过所述第一加密通道接收所述浏览器主业务进程发送的第一业务数据；

所述业务处理线程采用第一对称算法对所述第一业务数据进行解密处理，获取原始业务数据；

10 所述业务处理线程采用第二对称算法对所述原始业务数据进行加密处理，获取所述第二业务数据；

所述业务处理线程采用通过所述第二加密通道向所述第二业务数据发送给所述网络服务器。

15 8、如权利要求 5 所述的方法，其特征在于，所述加密子进程对所述网络服务器进行单向证书认证，包括：

所述加密子进程接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书；

所述加密子进程对所述网络服务器的站点签名证书进行认证。

20 9、如权利要求 5 所述的方法，其特征在于，所述加密子进程和所述网络服务器进行双向证书认证，包括：

所述加密子进程接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书；

所述加密子进程接收所述网络服务器发送的证书认证请求消息，所述证书认证请求消息用于指示进行客户端的证书认证；

25 所述加密子进程接收所述网络服务器发送的服务端密钥交换消息，包括密钥交换参数；

所述加密子进程接收所述网络服务器发送的服务端问候完结消息；

所述加密子进程对所述站点签名证书进行认证；

30 当所述站点签名证书认证通过后，所述加密子进程向所述网络服务器发送客户端证书消息，所述客户端证书消息包括所述浏览器客户端的签名证书，以使所述网络服务器对所述签名证书进行认证。

10、如权利要求 9 所述的方法，其特征在于，所述的方法还包括密钥交换的步骤：

所述加密子进程依据所述密钥交换参数随机产生预主密钥，其中，所述预主密钥是采用所述网络服务器的加密公钥通过椭圆曲线密码算法 SM2 进行加密计算得到的；

所述加密子进程采用所述预主密钥生成客户端密钥交换消息，并发送给网络服务器，以使所述网络服务器获取所述预主密钥。

- 5 11、如权利要求 9 所述的方法，其特征在于，所述的方法还包括验证证书签名的步骤：

所述加密子进程获取依据站点签名证书计算的签名校验参数，并生成客户端证书校验消息发送给所述网络服务器；

- 10 所述加密子进程向所述网络服务器发送客户端密码规格变更消息，以表征加密数据的协商完成；

所述加密子进程向所述网络服务器发送客户端握手结束消息；

所述加密子进程接收所述网络服务器发送的服务端密码规格变更消息，以表征认可该加密数据的协商；

所述加密子进程接收所述网络服务器发送的服务端握手结束消息。

- 15 12、如权利要求 11 所述的方法，其特征在于，还包括：

在所述加密连接通信建立成功后，建立为所述加密子进程和所述网络服务器进行安全通信的第二加密通道。

13、如权利要求 7 所述的方法，其特征在于，还包括：

- 20 所述加密子进程和所述浏览器主业务进程通过握手过程建立加密连接通信，并在加密连接通信成功后，建立为所述浏览器主业务进程和所述加密子进程进行安全通信的第一加密通道；

其中，所述握手过程中执行通过第一非对称算法执行所述加密子进程和所述浏览器主业务进程之间的双向证书认证、密钥交换，以及执行证书认证；所述密钥交换过程中生成对称密钥。

- 25 14、如权利要求 7 所述的方法，其特征在于，还包括：

所述业务处理线程将第一连接请求通过第二对称算法进行加密处理得到第二连接请求；

所述业务处理线程将所述第二连接请求发送给所述网络服务器；

- 30 所述业务处理线程接收所述网络服务器基于所述第二连接请求反馈的第二连接应答；

第二连接请求将所述第二连接应答通过第二对称算法进行解密处理得到第一连接应答，并反馈给所述浏览器主业务进程。

15、如权利要求 5 所述的方法，其特征在于，还包括：

加密子进程通过驱动识别安全密钥存储硬件，并依据所述硬件证书载体在双向证书认证过程中进行加密运算。

16、一种安全浏览器装置，包括：一处理器，该处理器中运行有一浏览器主业务进程模块和加密子进程模块，

其中，所述浏览器主业务进程模块，用于在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程的加密子进程模块，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；

所述加密子进程模块，包括：

10 代理子模块，用于对浏览器主业务进程进行侦听，并获取所述浏览器主业务进程发送的第一连接请求；以及在所述加密连接通信建立成功后，所述加密子进程执行业务数据在所述第一加密通道和第二加密通道之间的转发；

安全连接子模块，用于依据所述第一连接请求，所述加密子进程与所述网络服务器建立加密连接通信；

15 其中，所述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和所述网络服务器的安全通信通道。

17、如权利要求 16 所述的装置，其特征在于：

所述代理子模块，用于所述加密子进程创建侦听线程；所述侦听线程通过服务端口对所述浏览器主业务进程进行侦听。

20 18、如权利要求 16 所述的装置，其特征在于：

所述安全连接子模块，用于在确认所述第一连接请求接收成功后，所述加密子进程与所述网络服务器依次进行加密数据协商和证书认证；在加密数据协商完毕且证书认证通过后，建立所述浏览器客户端与网络服务器的加密连接通信。

19、如权利要求 18 所述的装置，其特征在于：

25 所述安全连接子模块，用于所述加密子进程向所述网络服务器发送客户端问候消息，其中，所述客户端问候消息包括所述浏览器客户端的第一加密数据，所述第一加密数据包括若干协议版本号；所述网络服务器向所述加密子进程反馈服务端问候消息，其中，所述服务端问候消息包括所述服务器客户端的第二加密数据，所述第二加密数据包括：从所述第一加密数据中选定的协议版本号。

30 20、如权利要求 18 所述的装置，其特征在于：

所述安全连接子模块，用于对所述网络服务器进行单向证书认证；或，所述加密子进程和所述网络服务器进行双向证书认证。

21、如权利要求 16 所述的装置，其特征在于：

所述代理子模块，还用于创建业务处理线程；所述业务处理线程分别与所述第一加密通道和所述第二加密通道建立连接。

22、如权利要求 21 所述的装置，其特征在于：

5 所述代理子模块，用于采用所述业务处理线程通过所述第一加密通道接收所述浏览器主业务进程发送的第一业务数据；所述业务处理线程采用第一对称算法对所述第一业务数据进行解密处理，获取原始业务数据；所述业务处理线程采用第二对称算法对所述原始业务数据进行加密处理，获取所述第二业务数据；所述业务处理线程采用通过所述第二加密通道向所述第二业务数据发送给所述网络服务器。

10 23、如权利要求 20 所述的装置，其特征在于：

所述安全连接子模块，用于接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书；所述加密子进程对所述网络服务器的站点签名证书进行认证。

24、如权利要求 20 所述的装置，其特征在于：

15 所述安全连接子模块，用于所述加密子进程接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书；所述加密子进程接收所述网络服务器发送的证书认证请求消息，所述证书认证请求消息用于指示进行客户端的证书认证；所述加密子进程接收所述网络服务器发送的服务端密钥交换消息，包括密钥交换参数；所述加密子进程接收所述网络服务器发送的服务端问候完结消息；所述加
20 密子进程对所述站点签名证书进行认证；当所述站点签名证书认证通过后，所述加密子进程向所述网络服务器发送客户端证书消息，所述客户端证书消息包括所述浏览器客户端的签名证书，以使所述网络服务器对所述签名证书进行认证。

25、如权利要求 24 所述的装置，其特征在于：

所述安全连接子模块，还用于依据所述密钥交换参数随机产生预主密钥，其中，所
25 述预主密钥是采用所述网络服务器的加密公钥通过椭圆曲线密码算法 SM2 进行加密计算得到的；所述加密子进程采用所述预主密钥生成客户端密钥交换消息，并发送给网络服务器，以使所述网络服务器获取所述预主密钥。

26、如权利要求 24 所述的装置，其特征在于：

所述安全连接子模块，还用于获取依据站点签名证书计算的签名校验参数，并生成
30 客户端证书校验消息发送给所述网络服务器；所述加密子进程向所述网络服务器发送客户端密码规格变更消息，以表征加密数据的协商完成；所述加密子进程向所述网络服务器发送客户端握手结束消息；所述加密子进程接收所述网络服务器发送的服务端密码规

格变更消息，以表征认可该加密数据的协商；所述加密子进程接收所述网络服务器发送的服务端握手结束消息。

27、如权利要求 26 所述的装置，其特征在于，还包括：

所述安全连接子模块，还用于在所述加密连接通信建立成功后，建立为所述加密子
5 进程和所述网络服务器进行安全通信的第二加密通道。

28、如权利要求 22 所述的装置，其特征在于：

所述代理子模块，还用于采用所述加密子进程和所述浏览器主业务进程通过握手过
程建立加密连接通信，并在加密连接通信成功后，建立为所述浏览器主业务进程和所述
加密子进程进行安全通信的第一加密通道；其中，所述握手过程中执行通过第一非对称
10 算法执行所述加密子进程和所述浏览器主业务进程之间的双向证书认证、密钥交换，以
及执行证书认证；所述密钥交换过程中生成对称密钥。

29、如权利要求 22 所述的装置，其特征在于：

所述代理子模块，还用于所述业务处理线程将第一连接请求通过第二对称算法进行
加密处理得到第二连接请求；所述业务处理线程将所述第二连接请求发送给所述网络服
15 务器；所述业务处理线程接收所述网络服务器基于所述第二连接请求反馈的第二连接应
答；第二连接请求将所述第二连接应答通过第二对称算法进行解密处理得到第一连接应
答，并反馈给所述浏览器主业务进程。

30、如权利要求 20 所述的装置，其特征在于，所述加密子进程模块，还包括：

所述硬件管理子模块，用于加密子进程通过驱动识别安全密钥存储硬件；

20 所述证书验证子模块，用于依据所述硬件证书载体在双向证书认证过程中进行加密
运算。

31、一种程序，包括可读代码，当所述可读代码在计算设备上运行时，导致所述计
算设备执行根据权利要求 1-15 中的任一个所述的安全浏览器的实现方法。

32、一种可读介质，其中存储了如权利要求 31 所述的程序。

说明书附图

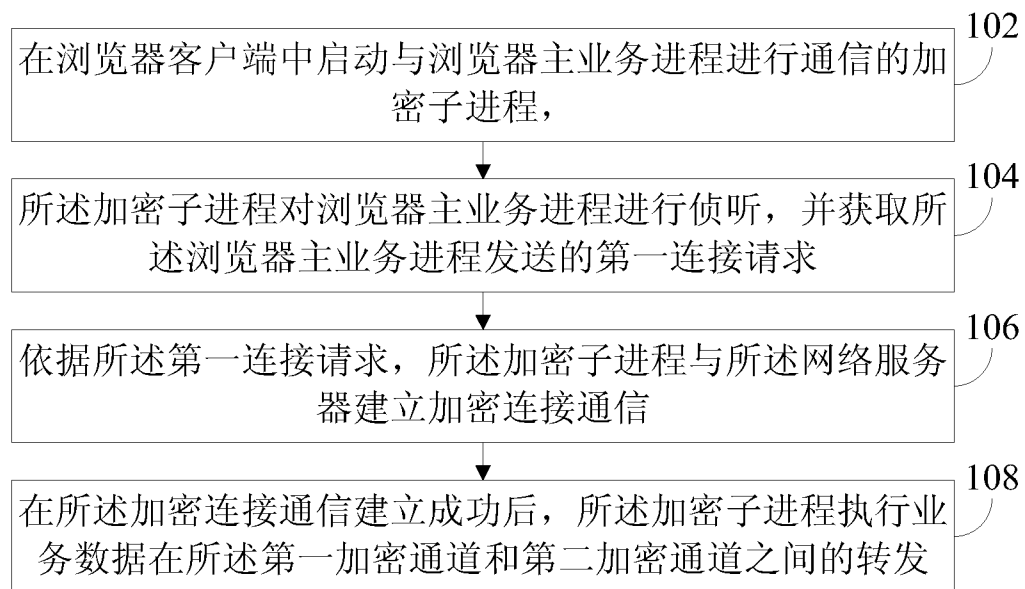


图 1

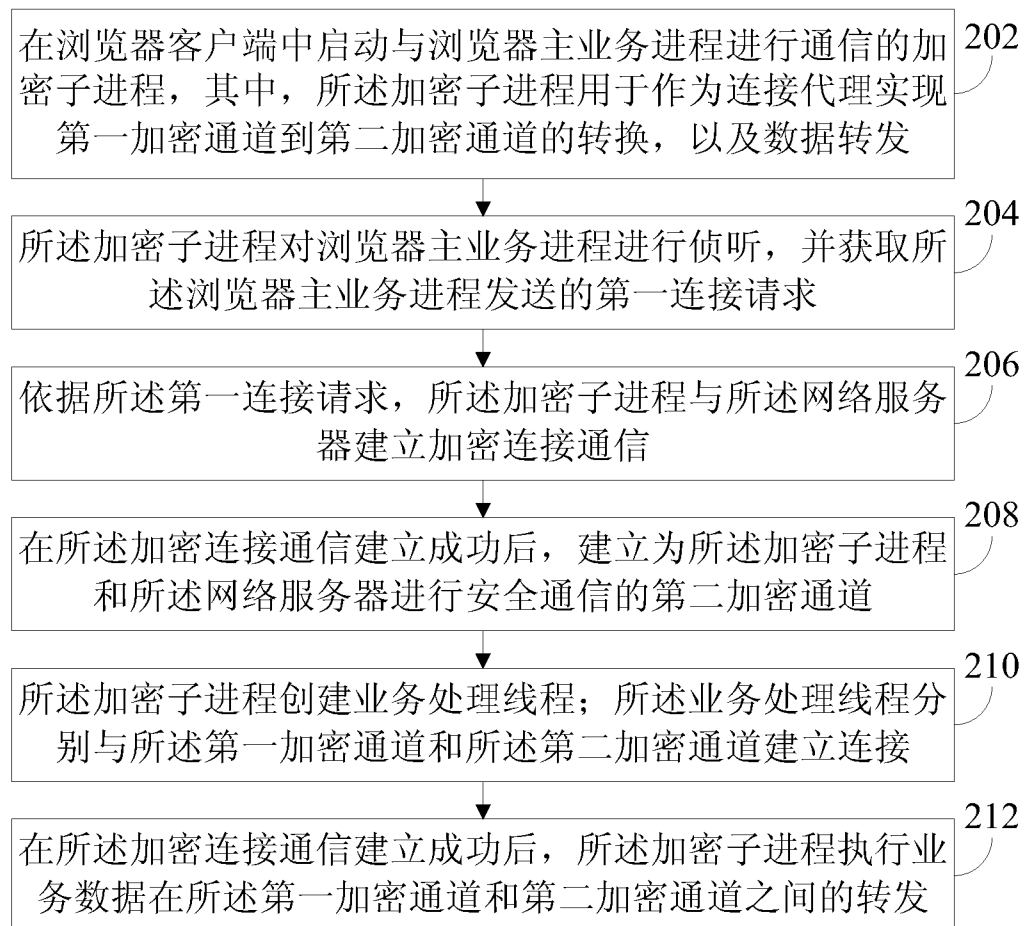


图 2

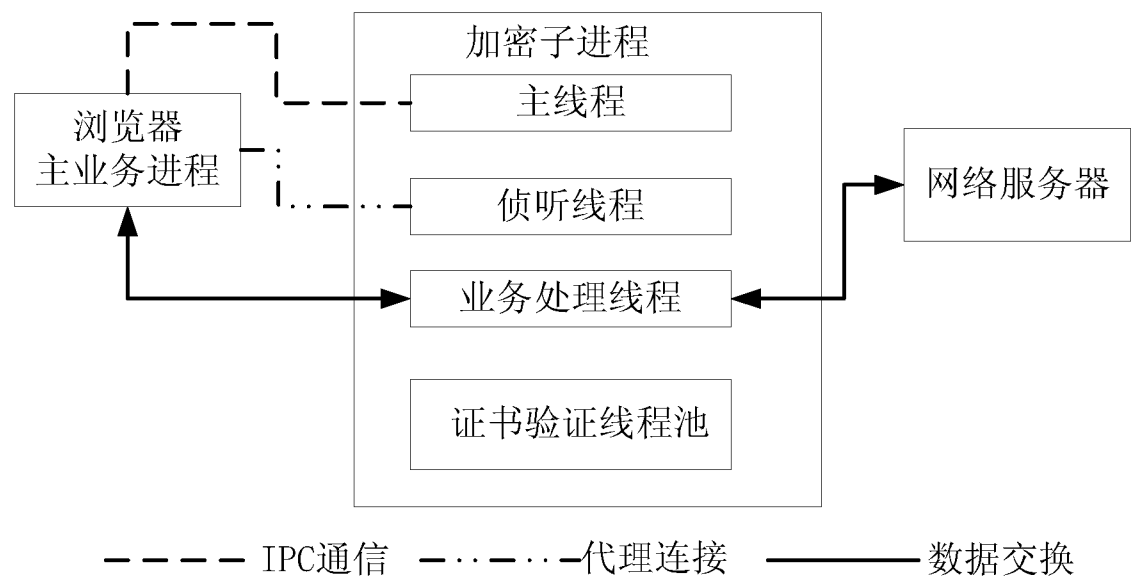


图 3

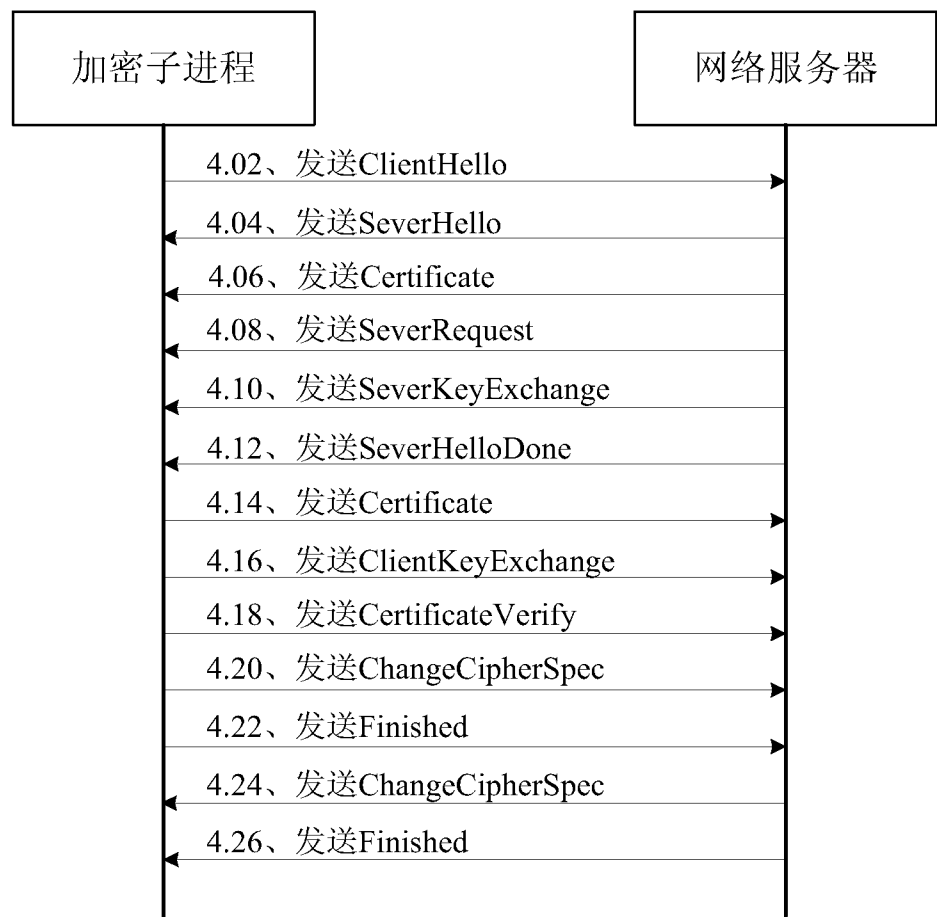


图 4

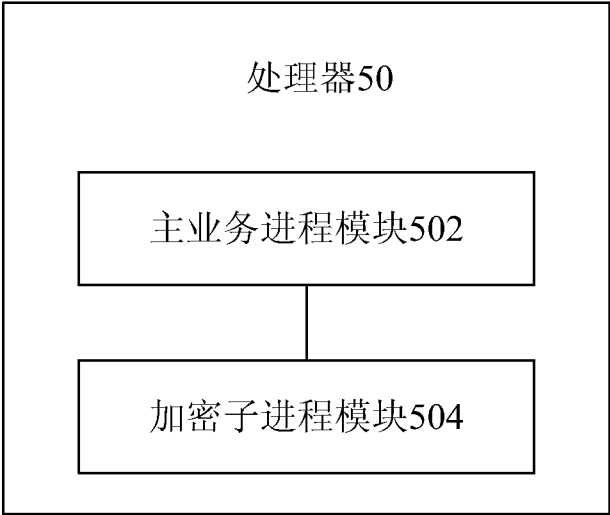


图 5

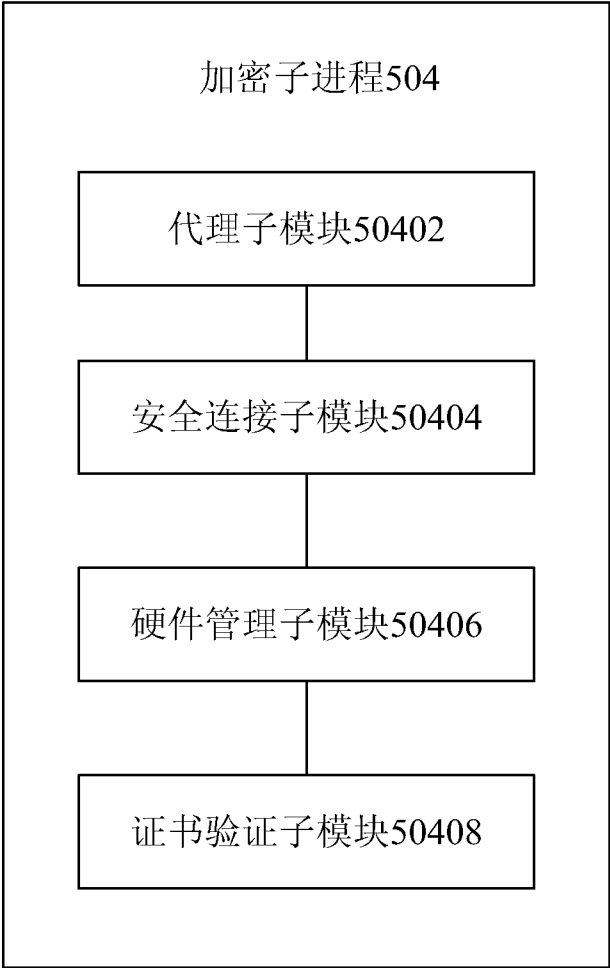


图 6

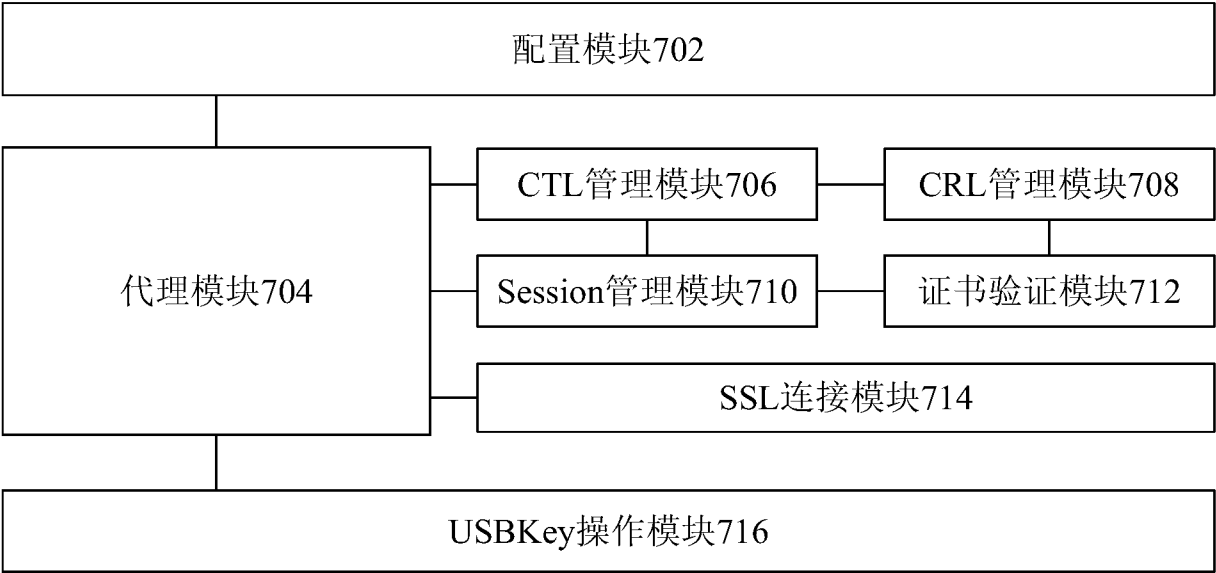


图 7

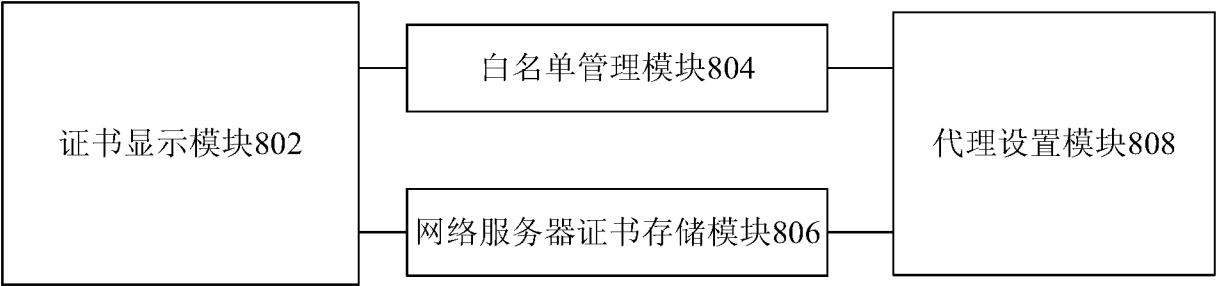


图 8

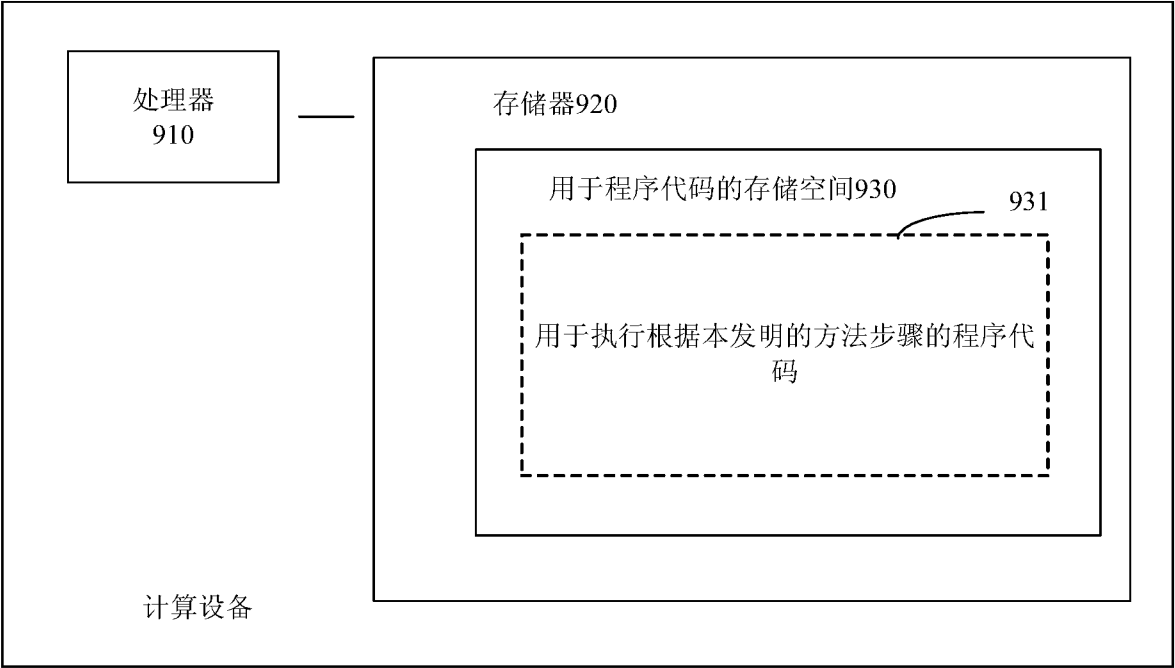


图 9

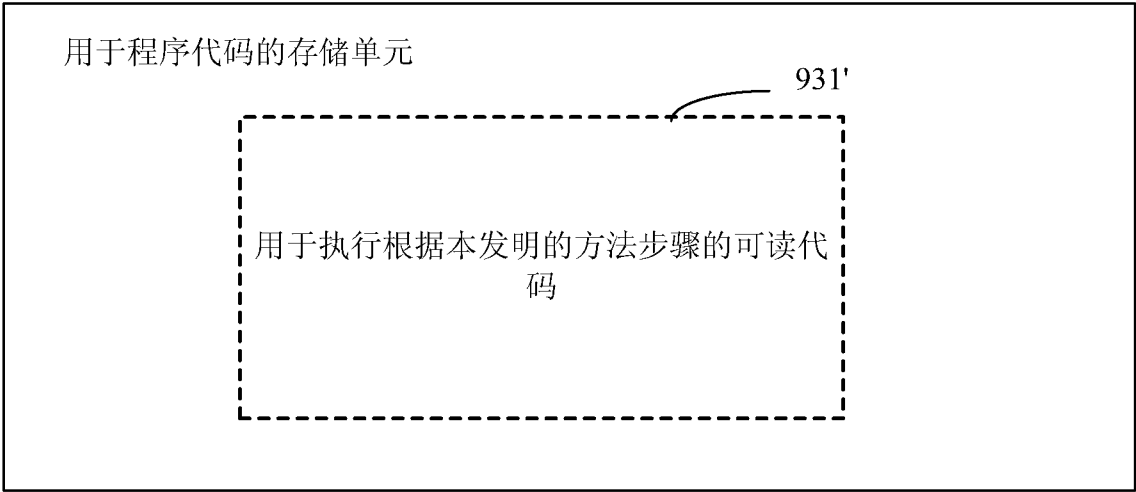


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/094851

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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, SIPOABS, VEN, CNKI: secure+, encrypt+, channel, tunnel, convert, agent, browser, explorer, forward, monitor, intercept

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104580190 A (BEIJING QIHOO SCI & TECHNOLOGY CO., LTD. et al.) 29 April 2015 (29.04.2015) claims 1-10, description, paragraphs [0020] to [0151]	1-32
PX	CN 104580189 A (BEIJING QIHOO SCI & TECHNOLOGY CO., LTD. et al.) 29 April 2015 (29.04.2015) claims 1-10, description, paragraphs [0019] to [0164]	1-32
X	CN 103188074 A (SHANGHAI KOAL SOFTWARE CO., LTD.) 03 July 2013 (03.07.2013) description, paragraphs [0035] to [0073]	1-32
A	CN 101436933 A (HUAWEI TECHNOLOGIES CO., LTD.) 20 May 2009 (20.05.2009) the whole document	1-32
A	CN 103763308 A (BEIJING WONDER SOFT CO., LTD.) 30 April 2014 (30.04.2014) the whole document	1-32
A	US 2011231652 A1 (F5 NETWORKS INC.) 22 September 2011 (22.09.2011) the whole document	1-32

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 03 February 2016	Date of mailing of the international search report 14 February 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer PENG, Yuan Telephone No. (86-10) 62411268

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/094851

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104580190 A	29 April 2015	None	
CN 104580189 A	29 April 2015	None	
CN 103188074 A	03 July 2013	None	
CN 101436933 A	20 May 2009	RU 2008145038 A	20 May 2010
		RU 2422893 C2	27 June 2011
		CN 101436933 B	01 February 2012
		WO 2009062406 A1	22 May 2009
CN 103763308 A	30 April 2014	None	
US 2011231652 A1	22 September 2011	JP 5744172 B2	01 July 2015
		EP 2548332 A2	23 January 2013
		US 2011231651 A1	22 September 2011
		EP 2548332 A4	15 July 2015
		US 2011231649 A1	22 September 2011
		CN 202206418 U	25 April 2012
		US 2011231653 A1	22 September 2011
		US 8700892 B2	15 April 2014
		US 9210131 B2	08 December 2015
		WO 2011116342 A2	22 September 2011
		JP 2013523050 A	13 June 2013
		CN 102195878 B	22 July 2015
		US 2011231655 A1	22 September 2011
		CN 102195878 A	21 September 2011
		WO 2011116342 A3	22 December 2011
		US 9166955 B2	20 October 2015
		US 9172682 B2	27 October 2015
		US 9178706 B1	03 November 2015
		US 9100370 B2	04 August 2015
		US 2011231923 A1	22 September 2011

A. 主题的分类 H04L 29/06 (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, SIPOABS, VEN, CNKI: 安全, 加密, 信道, 通道, 转换, 代理, 浏览器, 转发, 监听, 侦听, secur+, encrypt+, channel, tunnel, convert, agent, browser, explorer, forward, monitor, intercept		
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
PX	CN 104580190 A (北京奇虎科技有限公司等) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1-10, 说明书第[0020]-[0151]段	1-32
PX	CN 104580189 A (北京奇虎科技有限公司等) 2015年 4月 29日 (2015 - 04 - 29) 权利要求1-10, 说明书第[0019]-[0164]段	1-32
X	CN 103188074 A (上海格尔软件股份有限公司) 2013年 7月 3日 (2013 - 07 - 03) 说明书第[0035]-[0073]段	1-32
A	CN 101436933 A (华为技术有限公司) 2009年 5月 20日 (2009 - 05 - 20) 全文	1-32
A	CN 103763308 A (北京明朝万达科技有限公司) 2014年 4月 30日 (2014 - 04 - 30) 全文	1-32
A	US 2011231652 A1 (F5 NETWORKS INC) 2011年 9月 22日 (2011 - 09 - 22) 全文	1-32
☐ 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 2016年 2月 3日		国际检索报告邮寄日期 2016年 2月 14日
ISA/CN的名称和邮寄地址 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		授权官员 彭媛 电话号码 (86-10) 62411268

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/094851

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	104580190	A	2015年 4月 29日	无			
CN	104580189	A	2015年 4月 29日	无			
CN	103188074	A	2013年 7月 3日	无			
CN	101436933	A	2009年 5月 20日	RU	2008145038	A	2010年 5月 20日
				RU	2422893	C2	2011年 6月 27日
				CN	101436933	B	2012年 2月 1日
				WO	2009062406	A1	2009年 5月 22日
CN	103763308	A	2014年 4月 30日	无			
US	2011231652	A1	2011年 9月 22日	JP	5744172	B2	2015年 7月 1日
				EP	2548332	A2	2013年 1月 23日
				US	2011231651	A1	2011年 9月 22日
				EP	2548332	A4	2015年 7月 15日
				US	2011231649	A1	2011年 9月 22日
				CN	202206418	U	2012年 4月 25日
				US	2011231653	A1	2011年 9月 22日
				US	8700892	B2	2014年 4月 15日
				US	9210131	B2	2015年 12月 8日
				WO	2011116342	A2	2011年 9月 22日
				JP	2013523050	A	2013年 6月 13日
				CN	102195878	B	2015年 7月 22日
				US	2011231655	A1	2011年 9月 22日
				CN	102195878	A	2011年 9月 21日
				WO	2011116342	A3	2011年 12月 22日
				US	9166955	B2	2015年 10月 20日
				US	9172682	B2	2015年 10月 27日
				US	9178706	B1	2015年 11月 3日
				US	9100370	B2	2015年 8月 4日
				US	2011231923	A1	2011年 9月 22日

表 PCT/ISA/210 (同族专利附件) (2009年7月)