

(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
2012 年 6 月 28 日 (28.06.2012)



(10) 国际公布号
WO 2012/083732 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2011/079634
- (22) 国际申请日: 2011 年 9 月 14 日 (14.09.2011)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201010615134.6 2010 年 12 月 22 日 (22.12.2010) CN
- (71) 申请人 (对除美国外的所有指定国): 腾讯科技 (深圳) 有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): 杨谦 (YANG, Qian) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 肖衡 (XIAO, Heng) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 于涛 (YU, Tao) [CN/CN]; 中国广东省深圳

市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。

(74) 代理人: 北京德琦知识产权代理有限公司 (DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路 1 号学院国际大厦 7 层, Beijing 100083 (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, 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, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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,

[见续页]

(54) Title: METHOD AND SYSTEM FOR PERFORMING ENCRYPTION/DECRYPTION WHEN TRANSMITTING DATA IN WEB

(54) 发明名称: 在 WEB 中传输数据时进行加解密的方法及系统

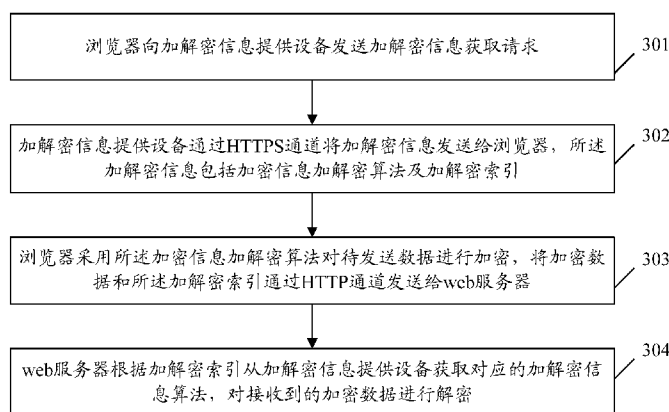


图 3 / FIG. 3

301 A BROWSER SENDS AN ENCRYPTION/DECRYPTION INFORMATION ACQUISITION REQUEST TO AN ENCRYPTION/DECRYPTION INFORMATION PROVIDING DEVICE

302 THE ENCRYPTION/DECRYPTION INFORMATION PROVIDING DEVICE SENDS ENCRYPTION/DECRYPTION INFORMATION TO THE BROWSER THROUGH AN HTTPS CHANNEL, THE ENCRYPTION/DECRYPTION INFORMATION COMPRISING AN ENCRYPTION INFORMATION ENCRYPTION/DECRYPTION ALGORITHM AND AN ENCRYPTION/DECRYPTION INDEX

303 THE BROWSER ADOPTS THE ENCRYPTION INFORMATION ENCRYPTION/DECRYPTION ALGORITHM TO ENCRYPT DATA TO BE SENT, AND SENDS THE ENCRYPTED DATA AND THE ENCRYPTION/DECRYPTION INDEX TO A WEB SERVER THROUGH AN HTTP CHANNEL

304 THE WEB SERVER ACQUIRES THE CORRESPONDING ENCRYPTION/DECRYPTION INFORMATION ALGORITHM FROM THE ENCRYPTION/DECRYPTION INFORMATION PROVIDING DEVICE ACCORDING TO THE ENCRYPTION/DECRYPTION INDEX, SO AS TO DECRYPT THE RECEIVED ENCRYPTED DATA

(57) Abstract: The present invention provides a method and system for performing encryption/decryption when transmitting data in web. The method comprises: a browser sending an encryption/decryption information request to an encryption/decryption information providing device; the encryption/decryption information providing device sending encryption/decryption information to the browser through an HTTPS channel, the encryption/decryption information comprising an encryption/decryption algorithm and an encryption/decryption index; the browser adopting the encryption/decryption algorithm to encrypt data to be sent, and sending the encrypted data and the encryption/decryption index to a web server through an HTTP channel; and the web server acquiring the corresponding encryption/decryption algorithm from the encryption/decryption information providing device according to the encryption/decryption index, so as to decrypt the encrypted data. The solution of the present invention can reduce the load of the HTTPS channel, and improve the overall performance.

[见续页]

WO 2012/083732 A1



SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, 本国际公布:

GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明提供了在 web 中传输数据时进行加解密的方法及系统,其中,该方法包括:浏览器向加解密信息提供设备发送加解密信息获取请求;加解密信息提供设备通过 HTTPS 通道将加解密信息发送给浏览器,所述加解密信息包括加解密算法及加解密索引;浏览器采用所述加解密算法对待发送数据进行加密,将加密数据和所述加解密索引通过 HTTP 通道发送给 web 服务器;web 服务器根据所述加解密索引从加解密信息提供设备获取对应的加解密算法,对所述加密数据进行解密。本发明方案能够减小 HTTPS 通道的负荷,提高了整体性能。

在 web 中传输数据时进行加解密的方法及系统

技术领域

本发明涉及数据传输技术，尤其涉及在 web 中传输数据时进行加解密的方法及系统。

5 发明背景

在 web 应用中，用户终端基于浏览器平台与 web 服务器之间进行数据传输。一般地，采用 AJAX 技术，通过超文件传输协议(HTTP, hypertext transmission protocol) 通道在浏览器与 web 服务器之间进行数据传输，而 Javascript 是解释性语言，代码算法没有秘密，对于收发的数据不便于
10 做加解密处理，导致传输的数据存在泄露的风险。

浏览器与 web 服务器之间的数据传输涉及多种业务，例如即时通讯(IM, Instant Messaging) 业务、在线支付业务、网银业务或证券系统业务等。以 IM 业务中的 webIM 业务为例，该业务特点在于不需要下载和安装客户端，可以在连接网络的 PC 上通过浏览器登录 IMweb 服务器，
15 接入 IM 的服务器集群系统；该业务不像客户端那样可以在 PC 上存储一些用户资料，而是在每次接入集群后，从 IMweb 服务器获取好友列表等资料，而 HTTP 通道采用明文传输的方式，不能对好友列表等资料以及聊天记录等信息进行加解密处理，导致存在信息泄露的风险。

为了提高数据传输的安全性，目前常通过安全超文本传输协议
20 (HTTPS, Hypertext Transfer Protocol over Secure Socket Layer) 通道在浏览器与 web 服务器之间进行数据传输。HTTPS 通道是以安全为目的的通道，简单而言是 HTTP 通道的安全版，具体地，在 HTTP 下加入安

全套接层 (SSL, Secure Socket Layer), HTTPS 的安全基础便是 SSL, 加解密操作需要 SSL 协助完成。在统一资源定位器 (URL, Uniform Resource Locator) 地址中包含 “HTTPS:” 就表明通过 HTTPS 通道进行数据传输, HTTPS 存在不同与 HTTP 的默认端口及一个加密/身份验证层。

5 现有进行加解密数据传输的方案中, 一般都是全程采用 HTTPS 通道来进行数据传输, HTTPS 通道会对在浏览器与 web 服务器之间传输的数据进行加解密处理, 这样, 即使数据在传输过程中被网关或路由器上的抓包工具所截获, 由于抓包工具无法获知加解密算法, 也不会造成数据信息的泄露。图 1 示出了现有在 web 中传输数据时进行加解密的系
10 统结构示意图。

然而, 在浏览器与 web 服务器之间通过 HTTPS 通道进行数据传输存在以下缺点:

HTTPS 对整体构架的使用效率有很大影响, 大致是 HTTP 对整体构架使用效率影响的 10 倍, 如果将 HTTP 全部用 HTTPS 替换, 将导致整
15 体性能下降 90% 左右。也就是, 现有的方案将增大 HTTPS 通道的负荷, 降低整体性能。

发明内容

本发明提供了在 web 中传输数据时进行加解密的方法, 该方法能够减小 HTTPS 通道的负荷。

20 本发明提供了在 web 中传输数据时进行加解密的系统, 该系统能够减小 HTTPS 通道的负荷。

一种在 web 中传输数据时进行加解密的方法, 该方法包括:

浏览器向加解密信息提供设备发送加解密信息获取请求;

加解密信息提供设备通过 HTTPS 通道将加解密信息发送给浏览器,

所述加解密信息包括加解密算法及加解密索引；

浏览器采用所述加解密算法对待发送数据进行加密，将加密数据和所述加解密索引通过 HTTP 通道发送给 web 服务器；

web 服务器根据所述加解密索引从加解密信息提供设备获取对应的
5 加解密算法，对所述加密数据进行解密。

另一种在 web 中传输数据时进行加解密的方法，该方法包括：

web 服务器向加解密信息提供设备发送加解密信息获取请求；

加解密信息提供设备获取包含加解密算法及加解密索引的加解密信息，发送给 web 服务器；

10 web 服务器采用加解密信息中的加解密算法对待发送数据进行加密，将加密数据和加解密信息中的加解密索引通过 HTTP 通道发送给浏览器；

浏览器通过 HTTPS 通道从加解密信息提供设备获取与 web 服务器发送的加解密索引对应的加解密算法，对 web 服务器发送的加密数据进行解密。
15

一种在 web 中传输数据时进行加解密的系统，该系统包括用户终端、web 服务器和加解密信息提供设备；

所述用户终端，基于浏览器向加解密信息提供设备发送加解密信息获取请求，接收所述加解密信息提供设备发送的包含加解密算法和加解密索引的加解密信息，所述浏览器采用所述加解密算法对待发送数据进行加密，将加密数据和所述加解密索引通过 HTTP 通道发送给所述 web 服务器；
20

所述 web 服务器，用于接收所述浏览器发送的加密数据和所述加解密索引，根据所述加解密索引从所述加解密信息提供设备获取对应的加解密算法，对所述加密数据进行解密；
25

所述加解密信息提供设备，用于接收所述浏览器发送的加解密信息获取请求，通过 HTTPS 通道将加解密信息发送给所述浏览器；并根据所述 web 服务器的请求提供与加解密索引对应的加解密算法。

从上述方案可以看出，本发明中，浏览器通过安全性较高的 HTTPS 通道向加解密信息提供设备请求加解密信息，对待发送数据进行加密后通过 HTTP 通道传送给 web 服务器，web 服务器再从加解密信息提供设备获取相应的加解密算法对加密数据进行解密。这样，通过加解密信息提供设备向浏览器和 web 服务器提供加解密信息，实现了在浏览器与 web 服务器之间采用 HTTP 通道进行加密数据的传输，而不用在浏览器和 web 服务器之间采用 HTTPS 通道进行数据传输，减小 HTTPS 通道的负荷，提高了整体性能。

附图简要说明

图 1 为现有技术 in web 中传输数据时进行加解密的系统结构示意图；

图 2 为本发明在 web 中传输数据时进行加解密的系统结构示意图；

图 3 为本发明在 web 中传输数据时进行加解密的方法示意性流程图；

图 4 为本发明在 web 中传输数据时进行加解密的方法流程图实例。

实施本发明的方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明设置加解密信息提供设备，通过加解密信息提供设备向浏览器和 web 服务器提供进行加解密处理时需要的加解密信息，并在浏览器与 web 服务器之间采用 HTTP 通道进行加密数据的传输，这样，无需在

浏览器和 web 服务器之间采用 HTTPS 通道进行数据传输来提高数据安全性，从而，在保证传输数据安全性的基础上，减小了 HTTPS 通道的负荷，提高了整体性能。

参见图 2，为本发明在 web 中传输数据时进行加解密的结构示意图，该系统包括用户终端、web 服务器和加解密信息提供设备；

所述用户终端，基于浏览器向加解密信息提供设备发送加解密信息获取请求，接收所述加解密信息提供设备发送的包含加解密算法和加解密索引的加解密信息，所述浏览器采用所述加解密算法对待发送数据进行加密，将加密数据和所述加解密索引通过 HTTP 通道发送给所述 web 服务器；

所述 web 服务器，用于接收所述浏览器发送的加密数据和所述加解密索引，根据所述加解密索引从所述加解密信息提供设备获取对应的加解密算法，对所述加密数据进行解密；

所述加解密信息提供设备，用于接收所述浏览器发送的加解密信息获取请求，通过 HTTPS 通道将加解密信息发送给所述浏览器；并根据所述 web 服务器的请求提供与加解密索引对应的加解密算法。

为了提高安全性，加解密信息提供设备与用户终端之间通过 HTTPS 通道进行信息交互，通过 HTTPS 通道传输的信息都经过加密，即使在这段传输中有信息被抓包工具所截获，抓包工具也无法进行分析以获知截获的信息。

加解密信息提供设备可以通过一个服务器实现，也可以通过算法服务器和 HTTPS 服务器实现；这里，以加解密信息提供设备通过算法服务器和 HTTPS 服务器实现进行说明：

所述 HTTPS 服务器，用于接收所述浏览器发送的加解密信息获取请求，向所述算法服务器传送加解密信息获取请求；接收所述算法服务

器反馈的加解密信息，通过 HTTPS 通道发送给所述浏览器；

所述算法服务器，用于接收所述 HTTPS 服务器发送的加解密信息获取请求，获取相应的加解密信息，通过内网反馈给所述 HTTPS 服务器。为了提高安全性，算法服务器与 web 服务器之间，以及算法服务器
5 与 HTTPS 服务器，都通过内网进行通信。

可选地，所述加解密信息提供设备还包括管理服务器，用于对算法服务器中的加解密信息进行实时更新。具体地，可以对加解密信息进行更换，或者，对加解密算法、加解密密钥的生成规则进行修改。对算法服务器中的加解密信息进行实时更新，可避免被外界恶意垃圾取或分析以
10 猜测到加解密规律。

进一步地，为了提高 web 服务器向浏览器传输数据的安全性，web 服务器向浏览器进行数据传输时：

所述 web 服务器，还用于从所述加解密信息提供设备获取包含加解密算法及加解密索引的加解密信息，采用加解密信息中的加解密算法对待发送数据进行加密，将加密数据和加解密信息中的加解密索引通过
15 HTTP 通道发送给所述浏览器；

所述用户终端，还基于浏览器通过 HTTPS 通道从所述加解密信息提供设备获取与所述 web 服务器发送的加解密索引对应的加解密算法，对所述 web 服务器发送的加密数据进行解密。

20 本发明还提供了在 web 中传输数据时进行加解密的方法，其流程如图 3 所示，其包括以下步骤：

步骤 301，浏览器向加解密信息提供设备发送加解密信息获取请求。

步骤 302，加解密信息提供设备通过 HTTPS 通道将加解密信息发送给浏览器，所述加解密信息包括加解密算法及加解密索引。

25 步骤 303，浏览器采用所述加解密算法对待发送数据进行加密，将

加密数据和所述加解密索引通过 HTTP 通道发送给 web 服务器。

步骤 304, web 服务器根据加解密索引从加解密信息提供设备获取对应的加解密算法, 对接收到的加密数据进行解密。

5 为了节省 web 服务器的存储空间, 本步骤 web 服务器对所述加密数据
5 据进行解密之后, 可删除从算法服务器获取的加解密算法。

如果加解密信息提供设备由 HTTPS 服务器和算法服务器实现, 则
上述流程步骤 302 所述加解密信息提供设备通过 HTTPS 通道将加解密
信息发送给浏览器包括: 加解密信息提供设备包含的 HTTPS 服务器接
收加解密信息获取请求, 向加解密信息提供设备包含的算法服务器传送
10 加解密信息获取请求; 算法服务器获取相应的加解密信息, 通过内网发
送给 HTTPS 服务器, HTTPS 服务器通过 HTTPS 通道将加解密信息发送
给浏览器; 相应地, 步骤 304 web 服务器根据加解密索引从加解密信息
提供设备获取加解密算法包括: web 服务器根据加解密索引, 通过内网
从算法服务器获取相应的加解密算法。

15 加解密信息提供设备存储了加解密算法和相应的加解密索引, 所述
加解密算法例如包括加解密函数和加解密密钥。接收加解密信息获取请
求后, 加解密信息提供设备可以从存储的加解密信息中随机选择一组提
供给请求方, 还可以, 按照一定的规范提取加解密信息, 例如, 若加解
密信息提供设备对应域名存储了加解密算法和相应的加解密索引, 则加
20 解密信息提供设备接收的加解密信息获取请求中也包含域名, 然后根据
域名提取相应的加解密信息。

可选地, 上述流程还包括: 对算法服务器中的加解密信息进行实时
更新。

进一步地, 为了提高 web 服务器向浏览器传输数据的安全性, 本发
25 明对 web 服务器向浏览器传输的数据也进行加密传输, 具体包括:

web 服务器向加解密信息提供设备发送加解密信息获取请求;

加解密信息提供设备获取包含加解密算法及加解密索引的加解密信息, 发送给 web 服务器;

web 服务器采用加解密信息中的加解密算法对待发送数据进行加密, 将加密数据和加解密信息中的加解密索引通过 HTTP 通道发送给浏览器;

浏览器通过 HTTPS 通道从加解密信息提供设备获取与 web 服务器发送的加解密索引对应的加解密算法, 对 web 服务器发送的加密数据进行解密。

浏览器与 web 服务器之间的数据传输涉及多种业务, 例如 IM 业务、在线支付业务、网银业务或证券系统业务等。下面以 IM 业务中的 IMweb 业务为例, 对本发明在 web 中传输数据时进行加解密的方法进行详细说明, 该方法基于图 3 的系统实现, 其中 web 服务器具体为 IMweb 服务器, 加解密信息提供设备包括算法服务器和 HTTPS 服务器, 该方法包括以下步骤:

步骤 401, 浏览器向 HTTPS 服务器发送加解密信息获取请求。

在业务进行过程中, 若浏览器有数据需要发送给 IMweb 服务器, 则执行步骤 401。

在用户个人计算机 (PC, Personal Computer) 的浏览器平台上, 先从 IMweb 服务器中的静态页面服务器上下载到完整的 JavaScript, 然后, 浏览器采用 JavaScript 向 HTTPS 服务器发起加解密信息获取请求。

步骤 402, HTTPS 服务器接收加解密信息获取请求, 向算法服务器传送加解密信息获取请求。

步骤 403, 算法服务器获取相应的加解密信息, 通过内网发送给 HTTPS 服务器, HTTPS 服务器通过 HTTPS 通道将加解密信息发送给浏

览器。

所述加解密信息包括加解密算法和加解密索引 (Index)，本实例中，所述加解密算法包括解密函数和加解密密钥 (key)。

5 算法服务器负责维护若干加解密函数对 (Fun)，每个加解密函数对包括加密函数 (EnFun) 和解密函数 (DnFun)，并生成加解密 Key；然后将 Fun 和 Key 组合成队列，并给每个队列设置一个 Index。将 Fun 和 Key 进行组合时，Fun 和 Key 可一一对应地进行组合，也可进行交叉组合，组合后的一条队列信息例如为表 1 所示。

索引 (Index)	加 密 函 数 (EnFun)	解密函数 (DeFun)	加 解 密 Key	标志 Flag
------------	--------------------	--------------	--------------	---------

表 1 Fun 和 Key 组合后的队列信息

10 其中索引 (Index) 用来查询对应的函数，EnFun 用来加密需要传输的数据，DeFun 用来解密已经加密的数据，EnFun 和 DeFun 都采用效率比较高的对称加密算法，可以由管理人员进行设定，加解密 Key 可大量生成，而且不重复、不可逆，标志位 Flag 可标识此队算法是否已经使用，是否已经过期等等。如果用户在 WebIM 上下线，则
15 WebIM 服务器会通知算法服务器及时更新此队列信息的 Flag 字段，使其标识为未使用。

浏览器还可以对应加解密索引存储获取的加解密算法，以备多次使用。这样，浏览器无需每次发送数据时都向 HTTPS 服务器请求加解密信息，简化了流程。

20 步骤 404，浏览器用接收到的加解密函数、加解密 key 对待发送数据进行加密，将加密数据和接收到的加解密索引通过 HTTP 通道发送给 IMweb 服务器。

浏览器应用 JavaScript，采用加解密函数、加解密 key 对待发送数据进行加密。

步骤 405, IMweb 服务器根据加解密索引从算法服务器获取对应的加解密算法, 对接收的加密数据进行解密。

IMweb 服务器获取加解密算法后, 可对应加解密索引存储加解密算法, 以备多次使用。这样, IMweb 服务器无需每次发送数据时都向
5 算法服务器请求加解密信息, 简化了流程。

对加密数据进行解密后, 便可对此数据进行相应处理, 例如进行本地计算、向后台服务器发送 UDP 数据包以获得反馈数据等, 得到处理后的数据, 若需要向浏览器返回处理后的数据, 则执行步骤 406。

在业务进行过程中, 若 IMweb 服务器有数据需要发送给浏览器,
10 则执行步骤 406。

步骤 406, IMweb 服务器向算法服务器发送加解密信息获取请求。

步骤 407, 算法服务器获取包含加解密算法及加解密索引的加解密信息, 通过内网发送给 IMweb 服务器。

步骤 408, IMweb 服务器采用加解密信息中的加解密算法对待发
15 送数据进行加密, 将加密数据和加解密信息中的加解密索引通过 HTTP 通道发送给浏览器。

步骤 409, 浏览器接收加密数据和加解密索引后, 向 HTTPS 服务器发送包含加解密索引的加解密信息获取请求。

步骤 410, HTTPS 服务器接收包含加解密索引的加解密信息获取
20 请求, 向算法服务器传送包含加解密索引的加解密信息获取请求。

步骤 411, 算法服务器获取与接收的加解密索引对应的加解密算法, 通过内网发送给 HTTPS 服务器, HTTPS 服务器通过 HTTPS 通道将加解密算法发送给浏览器。

步骤 412, 浏览器采用接收到的加解密算法, 对 IMweb 服务器发
25 送的加密数据进行解密。

如果步骤 403 中浏览器对应加解密索引存储了加解密算法，则浏览器无需再次从 HTTPS 服务器获取，而直接采用之前存储的加解密算法对接收到的加密数据进行解密。

步骤 401 - 405 是对浏览器向 IMweb 服务器传输的数据进行加密传输的流程，步骤 406 - 412 是对 IMweb 服务器向浏览器传输的数据进行加密传输的流程，步骤 401 与 406 可无序执行。

采用图 4 的方法流程后，即使浏览器与 IMweb 服务器之间通过 HTTP 通道传输的数据被抓包工具所截获，由于抓包工具不知道加解密算法和加解密 Key，也就无法获得其中的真实信息。

10 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

权利要求书

1、一种在 web 中传输数据时进行加解密的方法，其特征在于，该方法包括：

浏览器向加解密信息提供设备发送加解密信息获取请求；

5 加解密信息提供设备通过 HTTPS 通道将加解密信息发送给浏览器，所述加解密信息包括加解密算法及加解密索引；

浏览器采用所述加解密算法对待发送数据进行加密，将加密数据和所述加解密索引通过 HTTP 通道发送给 web 服务器；

web 服务器根据所述加解密索引从加解密信息提供设备获取对应的
10 加解密算法，对所述加密数据进行解密。

2、如权利要求 1 所述的方法，其特征在于，所述加解密信息提供设备通过 HTTPS 通道将加解密信息发送给浏览器包括：

加解密信息提供设备包含的 HTTPS 服务器接收加解密信息获取请求，向加解密信息提供设备包含的算法服务器传送加解密信息获取请求；
15 算法服务器获取相应的加解密信息，通过内网发送给 HTTPS 服务器，HTTPS 服务器通过 HTTPS 通道将加解密信息发送给浏览器。

3、如权利要求 2 所述的方法，其特征在于，所述加解密算法包括加解密函数和加解密密钥；

所述 web 服务器对所述加密数据进行解密之后，该方法还包括：
20 web 服务器删除从算法服务器获取的加解密算法。

4、如权利要求 2 所述的方法，其特征在于，该方法还包括：

加解密信息提供设备对算法服务器中的加解密信息进行实时更新。

5、如权利要求 2 所述的方法，其特征在于，所述加解密信息获取请求中包含域名；所述算法服务器获取相应的加解密信息，通过内网发送

给 HTTPS 服务器包括：算法服务器提取与所述域名对应的加解密信息，通过内网发送给 HTTPS 服务器。

6、一种在 web 中传输数据时进行加解密的方法，其特征在于，该方法包括：

5 web 服务器向加解密信息提供设备发送加解密信息获取请求；
 加解密信息提供设备获取包含加解密算法及加解密索引的加解密信息，发送给 web 服务器；

 web 服务器采用加解密信息中的加解密算法对待发送数据进行加密，将加密数据和加解密信息中的加解密索引通过 HTTP 通道发送给浏
10 览器；

 浏览器通过 HTTPS 通道从加解密信息提供设备获取与 web 服务器发送的加解密索引对应的加解密算法，对 web 服务器发送的加密数据进行解密。

7、一种在 web 中传输数据时进行加解密的系统，其特征在于，该
15 系统包括用户终端、web 服务器和加解密信息提供设备；

 所述用户终端，基于浏览器向加解密信息提供设备发送加解密信息获取请求，接收所述加解密信息提供设备发送的包含加解密算法和加解密索引的加解密信息，所述浏览器采用所述加解密算法对待发送数据进行加密，将加密数据和所述加解密索引通过 HTTP 通道发送给所述 web
20 服务器；

 所述 web 服务器，用于接收所述浏览器发送的加密数据和所述加解密索引，根据所述加解密索引从所述加解密信息提供设备获取对应的加解密算法，对所述加密数据进行解密；

 所述加解密信息提供设备，用于接收所述浏览器发送的加解密信息
25 获取请求，通过 HTTPS 通道将加解密信息发送给所述浏览器；并根据

所述 web 服务器的请求提供与加解密索引对应的加解密算法。

8、如权利要求 7 所述的系统，其特征在于，

所述 web 服务器，还用于从所述加解密信息提供设备获取包含加解密算法及加解密索引的加解密信息，采用加解密信息中的加解密算法对待发送数据进行加密，将加密数据和加解密信息中的加解密索引通过 HTTP 通道发送给所述浏览器；

所述用户终端，还基于浏览器通过 HTTPS 通道从所述加解密信息提供设备获取与所述 web 服务器发送的加解密索引对应的加解密算法，对所述 web 服务器发送的加密数据进行解密。

10 9、权利要求 7 所述的系统，其特征在于，所述加解密信息提供设备包括算法服务器和 HTTPS 服务器；

所述 HTTPS 服务器，用于接收所述浏览器发送的加解密信息获取请求，向所述算法服务器传送加解密信息获取请求；接收所述算法服务器反馈的加解密信息，通过 HTTPS 通道发送给所述浏览器；

15 所述算法服务器，用于接收所述 HTTPS 服务器发送的加解密信息获取请求，获取相应的加解密信息，通过内网反馈给所述 HTTPS 服务器。

10、如权利要求 9 所述的系统，其特征在于，所述加解密信息提供设备还包括管理服务器，用于对所述算法服务器中的加解密信息进行实时更新。

1/3

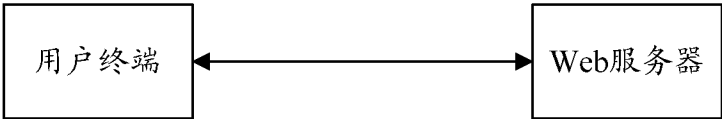


图 1

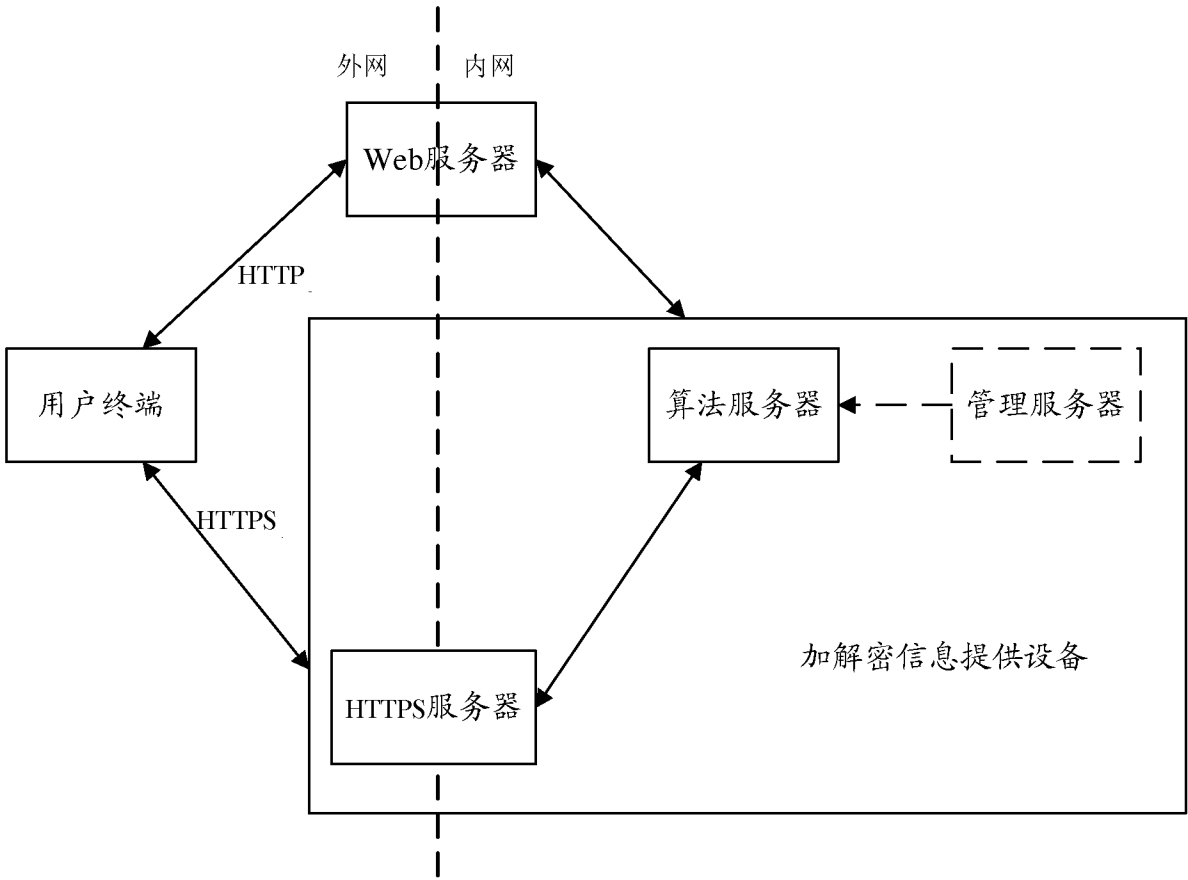


图 2

2/3

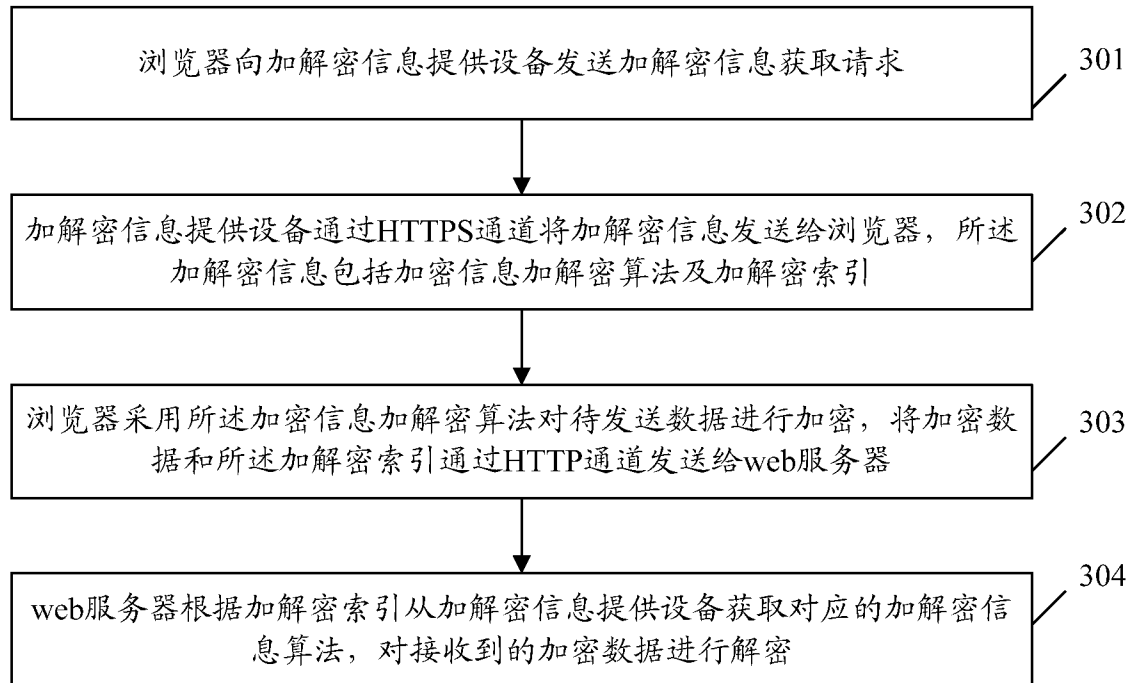


图 3

3/3

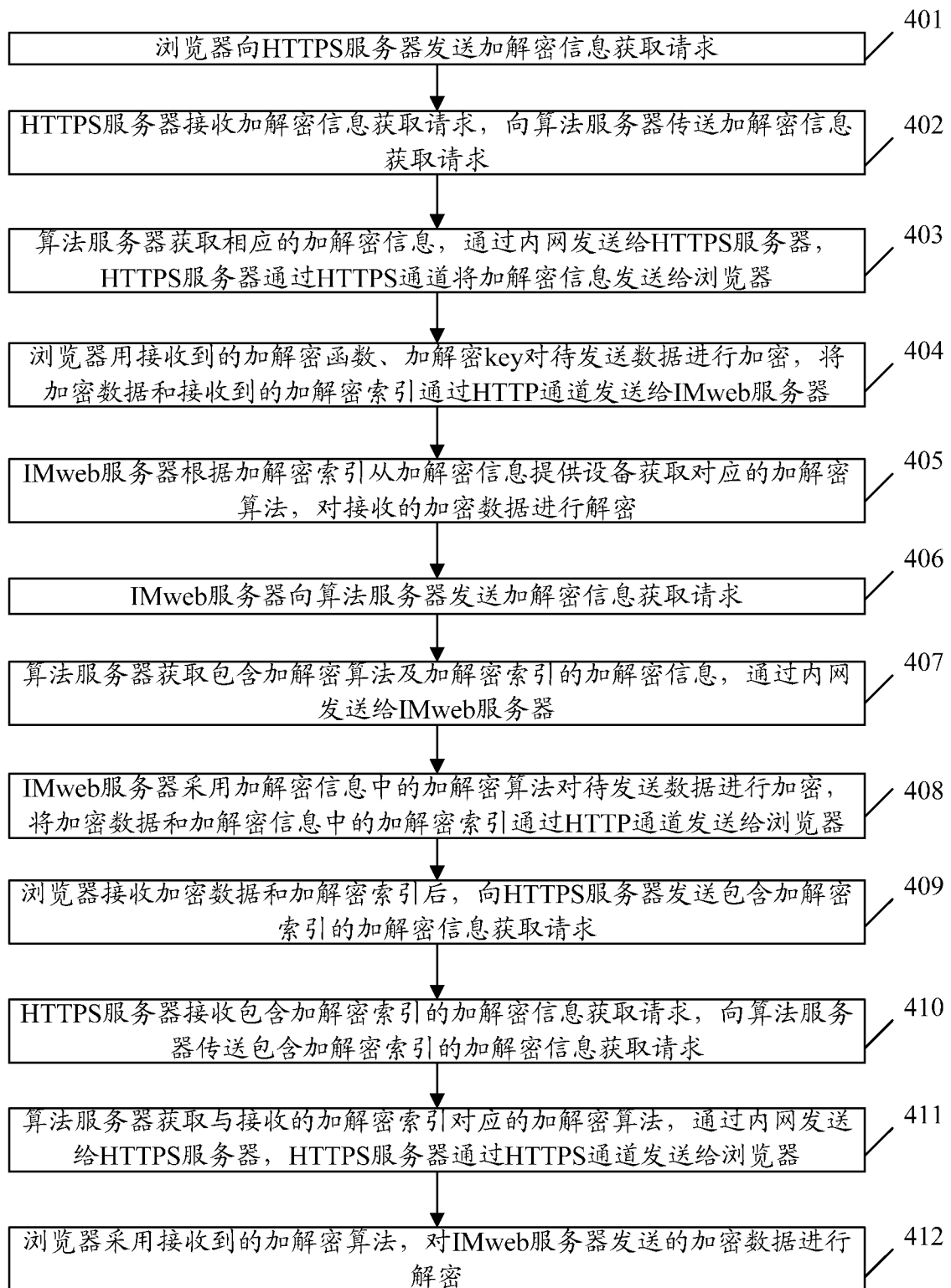


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/079634

A. CLASSIFICATION OF SUBJECT MATTER

See Extra Sheet

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: H04L, G06F

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)

CPRSABS, CNKI, CNTXT, VEN: web, server, encrypt, decrypt, browser, viewer, HTTP, HTTPS, SSL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2009220080A1 (HERNE ET-AL) 03 Sep. 2009(03.09.2009) see abstract, description paragraph 0026	1-10
A	CN101304310A (CHENGDU WEISHITONG INFORMATION IND. CO., LT.) 12 Nov. 2008 (12.11.2008) the whole document	1-10
A	CN101436933A (HUAWEI TECHNOLOGIES CO., LTD.) 20 May 2009 (20.05.2009) the whole document	1-10
A	US2009222888A1 (MICROSOFT CORPORATION ET-AL) 03 Sep. 2009 (03.09.2009) the whole document	1-10

☐ 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
14 Nov. 2011 (14.11.2011)

Date of mailing of the international search report
01 Dec. 2011 (01.12.2011)

Name and mailing address of the ISA/CN
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
WANG Hongli
Telephone No. (86-10) 62411281

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/079634

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2009220080A1	03.09.2009	None	
CN101304310A	12.11.2008	CN101304310B	15.09.2010
CN101436933A	20.05.2009	WO2009062406A1	22.05.2009
		RU2008145038A	20.05.2010
		RU2422893C2	27.06.2011
US2009222888A1	03.09.2009	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2011/079634

Continuation of: A. **CLASSIFICATION OF SUBJECT MATTER**

H04L 29/06 (2006.01)i

H04L 29/08 (2006.01)n

国际检索报告

国际申请号

PCT/CN2011/079634

A. 主题的分类

参见附加页

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)

IPC: H04L, G06F

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))

CPRSABS, CNKI, CNTXT: WEB, 服务器, 加密, 解密, 浏览器, HTTP, HTTPS, SSL, 安全套接

VEN: web, server, encrypt, decrypt, browser, viewer, HTTP, HTTPS, SSL

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
A	US2009220080A1 (HERNE 等) 03.9 月 2009 (03.09.2009) 摘要, 说明书第 0026 段	1-10
A	CN101304310A (成都卫士通信息产业股份有限公司) 12.11 月 2008 (12.11.2008) 全文	1-10
A	CN101436933A (华为技术有限公司) 20.5 月 2009 (20.05.2009) 全文	1-10
A	US2009222888A1 (MICROSOFT CORPORATION 等) 03.9 月 2009 (03.09.2009) 全文	1-10

☐ 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

14.11 月 2011 (14.11.2011)

国际检索报告邮寄日期

01.12 月 2011 (01.12.2011)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

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

王红丽

电话号码: (86-10) **62411281**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/079634

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
US2009220080A1	03.09.2009	无	
CN101304310A	12.11.2008	CN101304310B	15.09.2010
CN101436933A	20.05.2009	WO2009062406A1	22.05.2009
		RU2008145038A	20.05.2010
		RU2422893C2	27.06.2011
US2009222888A1	03.09.2009	无	

续: A. 主题的分类

H04L 29/06 (2006.01) i

H04L 29/08 (2006.01) n