

(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
2020 年 11 月 5 日 (05.11.2020)



(10) 国际公布号
WO 2020/220833 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *G06F 8/65* (2018.01)
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2020/078395

(22) 国际申请日: 2020 年 3 月 9 日 (09.03.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910359100.6 2019年4月28日 (28.04.2019) CN

(71) 申请人: 深圳前海微众银行股份有限公司
(WEBANK CO., LTD) [CN/CN]; 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。

(72) 发明人: 冯冬(FENG, Dong); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 万磊(WAN, Lei); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 李毅(LI, Yi); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 王志远(WANG, Zhiyuan); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 王文博(WANG, Wenbo); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所(CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区西丽街

(54) Title: SECURE SOCKETS LAYER ACCELERATION METHOD, APPARATUS AND DEVICE, AND READABLE STORAGE MEDIUM

(54) 发明名称: 安全套接层加速方法、装置、设备及可读存储介质

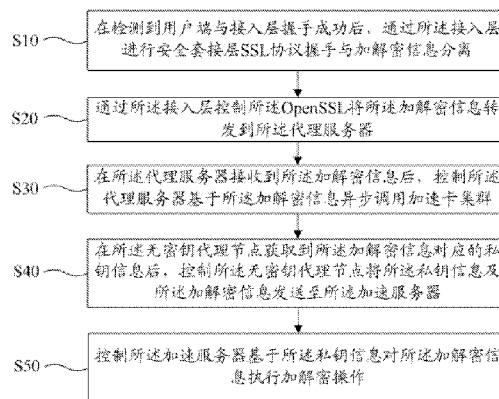


图 2

S10 After detecting successful handshake between a client and an access layer, separate secure sockets layer (SSL) protocol handshake from encryption and decryption information by means of the access layer

S20 Control, by means of the access layer, OpenSSL to forward the encryption and decryption information to a proxy server

S30 After the proxy server receives the encryption and decryption information, control the proxy server to asynchronously call an accelerator card cluster on the basis of the encryption and decryption information

S40 After a keyless proxy node obtains private key information corresponding to the encryption and decryption information, control the keyless proxy node to send the private key information and the encryption and decryption information to an acceleration server

S50 Control the acceleration server to perform encryption and decryption operations on the encryption and decryption information on the basis of the private key information

(57) Abstract: Disclosed is a secure sockets layer (SSL) acceleration method, comprising: after detecting successful handshake between a client and an access layer, separating SSL protocol handshake from encryption and decryption information by means of the access layer; controlling, by means of the access layer, OpenSSL to forward the encryption and decryption information to a proxy server; after the proxy server receives the encryption and decryption information, controlling the proxy server to asynchronously call an accelerator card cluster on the basis of the encryption and decryption information; after a keyless proxy node obtains corresponding private key

道松坪山社区松坪山路3号奥特迅电力大厦201, Guangdong 518052 (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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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))。

information on the basis of the encryption and decryption information, controlling the keyless proxy node to send the private key information and the encryption and decryption information to an acceleration server; and controlling the acceleration server to perform encryption and decryption operations on the encryption and decryption information on the basis of the private key information. Also disclosed are an SSL acceleration apparatus and device, and a readable storage medium. In the present application, the acceleration server is disposed in a blockchain or the accelerator card cluster other than the access layer of another service, so that OpenSSL and the acceleration server are completely decoupled without affecting each other, and service management and version upgrade are facilitated.

(57) 摘要: 本申请公开了一种安全套接层加速方法, 包括: 在检测到用户端与接入层握手成功后, 通过接入层进行SSL协议握手与加解密信息分离; 通过接入层控制OpenSSL将加解密信息转发到代理服务器; 在代理服务器接收到加解密信息后, 控制代理服务器基于加解密信息异步调用加速卡集群; 在无密钥代理节点基于加解密信息获取对应的私钥信息后, 控制无密钥代理节点将私钥信息及加解密信息发送至加速服务器; 控制加速服务器基于私钥信息对加解密信息执行加解密操作。本申请还公开了一种安全套接层加速装置、设备和存储介质。本申请通过将加速服务器设置在区块链或其他服务的接入层之外的加速卡集群中, 使得OpenSSL与加速服务器之间完全解耦, 互不影响, 便于服务管理以版本升级。

安全套接层加速方法、装置、设备及可读存储介质

[0001] 本申请要求于2019年4月28日提交中国专利局、申请号为201910359100.6、发明名称为“安全套接层加速方法、装置、设备及可读存储介质”的中国专利申请优先权，其全部内容通过引用结合在申请中。

技术领域

[0002] 本申请涉及金融科技（Fintech）技术领域，尤其涉及金融行业的安全套接层加速方法、装置、设备及可读存储介质。

背景技术

[0003] 随着计算机技术的发展，越来越多的技术（如分布式、区块链Blockchain、人工智能等）应用在金融领域，传统金融业正在逐步向金融科技（Fintech）转变，越来越多的技术应用于金融行业。现在网站为了安全起见，大部分都使用HTTPS。HTTPS协议相比HTTP协议增加了安全套接层SSL，所有的 HTTP 请求和响应数据在发送到网络之前，都要进行加密。安全和性能不可兼得，增加的加解密计算消耗转发服务器的大量CPU资源，导致转发性能下降。通用解决方案是使用专用的硬件卸载CPU密集型运算。

[0004] 目前业界较为普遍使用的是Intel QAT加速卡以及其提供的Nginx的适配方案，该方案利用OpenSSL的TSL异步模式，并对Nginx HTTPS模块进行异步模式适配，最终实现了整个HTTPS请求处理的异步化。

[0005] 然而，现有技术中，Nginx、OpenSSL和加速服务QAT耦合度高，各自版本升级成本较大，请求状态和问题排查难度大。

发明概述

技术问题

问题的解决方案

技术解决方案

[0006] 本申请的主要目的在于提出一种安全套接层加速方法、装置、设备及可读存储介质，旨在解决现有技术中使用Intel QAT加速卡及其提供的Nginx的适配方案

时，由于Nginx、OpenSSL和加速卡之间耦合度过高而引起各自版本更新升级成本大的问题。

[0007] 为实现上述目的，本申请提供一种安全套接层加速方法，所述安全套接层加速方法包括如下步骤：

[0008] 在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；

[0009] 通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；

[0010] 在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；

[0011] 在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；

[0012] 控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。

[0013] 此外，为实现上述目的，本申请还提供一种安全套接层加速装置，所述安全套接层加速装置包括：

[0014] 分离模块，用于在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；

[0015] 转发模块，用于通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；

[0016] 调用模块，用于在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；

[0017] 发送模块，用于在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；

[0018] 执行模块，用于控制所述加速服务器基于所述私钥信息对所述加解密信息执行

加解密操作。

[0019] 此外，为实现上述目的，本申请还提供一种安全套接层加速设备，所述安全套接层加速设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的安全套接层加速程序，所述安全套接层加速程序被所述处理器执行时实现如上所述的安全套接层加速方法的步骤。

[0020] 此外，为实现上述目的，本申请还提供一种可读存储介质，所述可读存储介质上存储有安全套接层加速程序，所述安全套接层加速程序被处理器执行时实现如上所述的安全套接层加速方法的步骤。

[0021] 本申请提出的安全套接层加速方法，首先，在检测到用户端与接入层握手成功后，通过接入层进行安全套接层SSL协议握手与加解密信息分解，从而产生异步任务；再者，软件库包OpenSSL仅仅将加解密信息转发到代理服务器，通过代理服务器进行调用无密钥代理节点，并且，通过无密钥代理节点配合加速服务器，实现加速服务器的加解密操作，由于将协议握手和加解密信息分解开，且增加了代理服务器，使得整个请求处理过程都是异步进行的；并且，将加速服务器设置在接入层之外的加速卡集群中，使得软件库包OpenSSL以及加速服务器之间完全解耦，互不影响，且保证高并发，方便服务的管理以及版本的升级。

发明的有益效果

对附图的简要说明

附图说明

[0022] 图1是本申请实施例方案涉及的硬件运行环境的设备结构示意图；

[0023] 图2为本申请安全套接层加速方法第一实施例的流程示意图；

[0024] 图3为本申请安全套接层加速方法第一实施例的的结构示意图。

[0025] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

发明实施例

本发明的实施方式

[0026] 应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0027] 如图1所示，图1是本申请实施例方案涉及的硬件运行环境的设备结构示意图。

[0028] 本申请实施例安全套接层加速设备可以是PC机或服务器设备。

[0029] 如图1所示，该安全套接层加速设备可以包括：处理器1001，例如CPU，网络接口1004，用户接口1003，存储器1005，通信总线1002。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏（Display）、输入单元比如键盘（Keyboard），可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口（如WIFI接口）。存储器1005可以是高速RAM存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0030] 本领域技术人员可以理解，图1中示出的设备结构并不构成对设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0031] 如图1所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及安全套接层加速程序。

[0032] 在图1所示的设备中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端（用户端），与客户端进行数据通信；而处理器1001可以用于调用存储器1005中存储的安全套接层加速程序，并执行下述安全套接层加速方法各个实施例中的操作。

[0033] 基于上述硬件结构，提出本申请安全套接层加速方法实施例。

[0034] 参照图2，图2为本申请安全套接层加速方法第一实施例的流程示意图，所述方法包括：

[0035] 步骤S10，在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；

[0036] 本实施例中，安全套接层（Secure Sockets Layer，SSL），是为网络通信提供安全及数据完整性的一种安全协议。SSL协议是Web浏览器与Web服务器之间安全交换信息的协议，提供两个基本的安全服务：鉴别与保密。

[0037] 本实施例的安全套接层加速方法在检测到用户端与接入层握手成功后，通过接

入层进行安全套接层SSL协议握手与加解密信息分离。如图3所示，接入层Access layer设置有Nginx服务器、软件库包OpenSSL和代理服务器Keyless-Agent，其中，NginxNginx是由伊戈尔·赛索耶夫为俄罗斯访问量第二的Rambler.ru站点开发的，是一个高性能的HTTP和反向代理web服务器；OpenSSL是一个开放源代码的软件库包，应用程序可以使用这个包来进行安全通信；代理服务器Keyless-Agent是增加了一个代理服务器，在软件库包OpenSSL将SSL协议握手和加解密信息分离后，将加解密信息转发出去。

[0038] 用户端与接入层的握手过程为：首先，在检测到用户端发起的HTTPS请求时，Nginx服务器基于HTTPS请求与用户端建立TCP连接，并生成安全套接层SSL；其次，Nginx服务器基于安全套接层SSL将SSL握手请求发送至所述OpenSSL处理得到处理结果，其中，SSL握手请求包括SSL协议握手及加解密信息；再者，软件库包OpenSSL基于处理结果判断与用户端是否握手成功，若是，则软件库包OpenSSL进行SSL协议握手与加解密信息分离。

[0039] 通过将SSL协议握手与加解密信息分离开，以便于加解密信息单独转发至加速卡集群，并且，由于OpenSSL和加速卡集群分属不同服务，因此，二者之间的耦合度较低。

[0040] 步骤S20，通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；

[0041] 该步骤中，在软件库包OpenSSL内部，将SSL协议握手与加解密信息分离开后，接入层中的软件库包OpenSSL将加解密信息单独转发到代理服务器Keyless-Agent中，以便于代理服务器Keyless-Agent能够基于该加解密信息调用处于另一个服务的加速卡集群。

[0042] 由于用户端与接入层握手时，用户端与Nginx服务器交互的内容通常包括加解密信息、SSL协议握手、版本以及证书等信息，如果将所有的交互内容都转发到代理服务器，那么将会占用大量的CPU资源，因此，仅仅将加解密信息转发出去，有效节约资源。

[0043] 步骤S30，在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥

代理节点及加速服务器；

[0044] 该步骤中，在代理服务器Keyless-Agent接收到用户端与Nginx服务器交互产生的加解密信息后，代理服务器Keyless-Agent基于加解密信息进行异步调用加速卡集群。

[0045] 异步调用的方式可以是远程过程调用RPC，RPC是一种通过网络从远程计算机程序上请求服务，而不需要了解底层网络技术的协议。RPC协议假定某些传输协议的存在，如TCP或UDP，为通信程序之间携带信息数据。在OSI网络通信模型中，RPC跨越了传输层和应用层。RPC使得开发包括网络分布式多程序在内的应用程序更加容易。

[0046] 由于代理服务器Keyless-Agent与加速卡集群之间采用的是异步调用的方式，因此，能够有效释放占用的线程等资源，避免阻塞，等到结果产生再重新获取线程处理，从而有效提高效率；并且，由于调用的加速卡集群设置于另一个服务中，有效降低加速卡集群与接入层之间的耦合度。

[0047] 步骤S40，在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器。

[0048] 该步骤中，代理服务器Keyless-Agent通过异步调用加速卡集群中的无密钥代理节点Keyless-Proxy，无密钥代理节点Keyless-Proxy从加速卡集群中的第二数据库DB中获取该请求域名对应的私钥信息，其中，私钥信息与加解密信息对应，为真实的密码，用于加解密，再将私钥信息和加解密信息都交给加速服务器Keyless-Accelerate进行异步处理。

[0049] 由于私钥信息只存在于加速卡集群中，接入层只有加解密信息，并且，只有虚拟的密码，因此，保证了接入层的安全。

[0050] 步骤S50，控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。

[0051] 该步骤中，在加速服务器Keyless-Accelerate接收到私钥信息及所述加解密信息后，利用其高性能的硬件加速卡执行加解密操作，从而实现对加解密的加速处理。

[0052] 当然，本案的用户端在与接入层握手成功后，与业务RS集群进行正常交互。

[0053] 本申请提出的安全套接层加速方法，首先，在检测到用户端与接入层握手成功后，通过接入层进行安全套接层SSL协议握手与加解密信息分解，从而产生异步任务；再者，软件库包OpenSSL仅仅将加解密信息转发到代理服务器，通过代理服务器进行调用无密钥代理节点，并且，通过无密钥代理节点配合加速服务器，实现加速服务器的加解密操作，由于将协议握手和加解密信息分解开，且增加了代理服务器，使得整个请求处理过程都是异步进行的；并且，将加速服务器设置在接入层之外的加速卡集群中，使得软件库包OpenSSL以及加速服务器之间完全解耦，互不影响，且保证高并发，方便服务的管理以及版本的升级。

[0054] 进一步地，基于本申请安全套接层加速方法第一实施例，所述接入层还设有Nginx服务器；提出本申请安全套接层加速方法第二实施例。

[0055] 在本实施例中，上述步骤S10可以包括：

[0056] 在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；

[0057] 控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；

[0058] 控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制所述OpenSSL基于所述处理结果判断与所述用户端是否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。

[0059] 具体地，用户端发起HTTPS请求，Nginx服务器接收请求并与用户端建立TCP连接；Nginx服务器将安全套接层SSL握手请求发给软件库包OpenSSL处理，软件库包OpenSSL与用户端交互SSL协议握手、加密算法、版本以及证书等信息，软件库包OpenSSL根据处理结果判定与用户端之间握手成功后，将SSL协议握手与所述加解密信息分离。

[0060] 通过将SSL协议握手与加解密信息分离开，以便于加解密信息单独转发至加速卡集群，并且，由于Nginx服务器、OpenSSL和加速卡集群分属不同服务，因此，二者之间的耦合度较低。

[0061] 进一步地，所述接入层还包括第一数据库，上述步骤S10还可以包括：控制所

述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；

[0062] 控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。

[0063] 在本实施例中，接入层的第一数据库DB用于提供配置信息、虚拟密码等；安全套接层SSL，是为网络通信提供安全及数据完整性的一种安全协议。在所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。

[0064] 由于接入层只有加解密信息，并且，只有虚拟的密码，因此，保证了接入层的安全。

[0065] 进一步地，步骤S30可以包括：在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息，通过远程过程调用RPC进行异步调用所述无密钥代理节点。

[0066] 在本实施例中，异步调用的方式可以是远程过程调用RPC，RPC是一种通过网络从远程计算机程序上请求服务，而不需要了解底层网络技术的协议。RPC协议假定某些传输协议的存在，如TCP或UDP，为通信程序之间携带信息数据。在OSI网络通信模型中，RPC跨越了传输层和应用层。RPC使得开发包括网络分布式多程序在内的应用程序更加容易。

[0067] 由于代理服务器Keyless-Agent与加速卡集群之间采用的是异步调用的方式，因此，能够有效释放占用的线程等资源，避免阻塞，等到结果产生再重新获取线程处理，从而有效提高效率；并且，由于调用的加速卡集群设置于另一个服务中，有效降低加速卡集群与接入层之间的耦合度。

[0068] 进一步地，步骤S30还可以包括：

[0069] 控制所述无密钥代理节点基于所述代理服务器调用所述无密钥代理节点对应的调用信息，生成调用请求信息；

[0070] 控制所述无密钥代理节点将所述调用请求信息实时上传至所述OpenSSL。

[0071] 在本实施例中，在所述代理服务器基于所述加解密信息异步调用加速卡集群的同时，无密钥代理节点基于所述代理服务器调用所述无密钥代理节点对应的调用信息生成调用请求信息；并且，无密钥代理节点将所述调用请求信息实时上

传至所述OpenSSL。

[0072] 通过调用请求信息上传至软件库包OpenSSL，使得接入层能够监控和统计代理服务器与加速卡集群之间的异步调用情况。

[0073] 进一步地，所述加速卡集群还包括第二数据库；步骤40可以包括：

[0074] 控制所述无密钥代理节点基于所述加解密信息，从所述第二数据库获取所述私钥信息；

[0075] 控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器。

[0076] 本实施例中，第二数据库DB用于提供用户端去请求域名对应的私钥信息，代理服务器Keyless-Agent通过异步调用加速卡集群中的无密钥代理节点Keyless-Proxy，无密钥代理节点Keyless-Proxy从加速卡集群中的第二数据库DB中获取该请求域名对应的私钥信息，其中，私钥信息与加解密信息对应，为真实的密码，用于加解密，再将私钥信息和加解密信息都交给加速服务器Keyless-Accelerate进行异步处理。

[0077] 由于私钥信息只存在于加速卡集群中，接入层只有加解密信息，并且，只有虚拟的密码，因此，保证了接入层的安全。

[0078] 进一步地，步骤S50之后，本申请的安全套接层加速方法还可以包括：

[0079] 通过所述加速服务器基于所述加解密操作得到操作结果；

[0080] 控制所述加速服务器将所述操作结果返回至所述无密钥代理节点。

[0081] 在本实施例中，在加速服务器Keyless-Accelerate利用其高性能的硬件加速卡进行加解密操作后，得到操作结果，并且，加速服务器Keyless-Accelerate将操作结果返回至无密钥代理节点Keyless-Proxy，使得无密钥代理节点Keyless-Proxy能够将操作结果上传至接入层。

[0082] 通过加速服务器Keyless-Accelerate将操作结果返回至无密钥代理节点Keyless-Proxy，进而使得无密钥代理节点Keyless-Proxy能够将操作结果上传至接入层，使得接入层的软件库包OpenSSL能够得到操作结果，实现操作结果回传。

[0083] 本申请还提供一种安全套接层加速装置。本申请所述安全套接层加速装置包括：

- [0084] 分离模块，用于在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；
- [0085] 转发模块，用于通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；
- [0086] 调用模块，用于在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；
- [0087] 发送模块，用于在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；
- [0088] 执行模块，用于控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。
- [0089] 进一步地，所述接入层还设有Nginx服务器；所述分离模块包括：
- [0090] 请求单元，用于在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；
- [0091] 处理单元，用于控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；
- [0092] 判断单元，用于控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制所述OpenSSL基于所述处理结果判断与所述用户端是否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。
- [0093] 进一步地，所述接入层还包括第一数据库，所述处理单元还用于：
- [0094] 控制所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；
- [0095] 控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。
- [0096] 进一步地，所述调用模块还用于：
- [0097] 在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息，通过远程过程调用RPC进行异步调用所述无密钥代理节点。

- [0098] 进一步地，所述调用模块还用于：
- [0099] 控制所述无密钥代理节点基于所述代理服务器调用所述无密钥代理节点对应的调用信息，生成调用请求信息；
- [0100] 控制所述无密钥代理节点将所述调用请求信息实时上传至所述OpenSSL。
- [0101] 进一步地，所述加速卡集群还包括第二数据库；所述发送模块还用于：
- [0102] 控制所述无密钥代理节点基于所述加解密信息，从所述第二数据库获取所述私钥信息；
- [0103] 控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器。
- [0104] 本申请还提供一种计算机可读存储介质。
- [0105] 本申请计算机可读存储介质上存储有安全套接层加速程序，所述安全套接层加速程序被处理器执行时实现如上所述的安全套接层加速方法的步骤。
- [0106] 其中，在所述处理器上运行的安全套接层加速程序被执行时所实现的方法可参照本申请安全套接层加速方法各个实施例，此处不再赘述。
- [0107] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。
- [0108] 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。
- [0109] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台安全套接层加速设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

[0110] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权利要求书

- [权利要求 1] 一种安全套接层加速方法，其中，所述安全套接层加速方法包括如下步骤：
- 在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；
- 通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；
- 在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；
- 在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；
- 控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。
- [权利要求 2] 如权利要求1所述的安全套接层加速方法，其中，所述接入层还设有Nginx服务器；所述在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离的步骤包括：
- 在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；
- 控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；
- 控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制所述OpenSSL基于所述处理结果判断与所述用户端是否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。
- [权利要求 3] 如权利要求2所述的安全套接层加速方法，其中，所述接入层还包括

第一数据库，所述控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL的步骤包括：

控制所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；

控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。

[权利要求 4] 如权利要求1所述的安全套接层加速方法，其中，所述在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群的步骤包括：

在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息，通过远程过程调用RPC进行异步调用所述无密钥代理节点。

[权利要求 5] 如权利要求1所述的安全套接层加速方法，其中，所述在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群的步骤还包括：

控制所述无密钥代理节点基于所述代理服务器调用所述无密钥代理节点对应的调用信息，生成调用请求信息；

控制所述无密钥代理节点将所述调用请求信息实时上传至所述OpenSSL。

[权利要求 6] 如权利要求1所述的安全套接层加速方法，其中，所述加速卡集群还包括第二数据库；所述在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器的步骤包括：

控制所述无密钥代理节点基于所述加解密信息，从所述第二数据库获取所述私钥信息；

控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器。

[权利要求 7] 如权利要求1所述的安全套接层加速方法，其中，所述控制所述加速

服务器基于所述私钥信息对所述加解密信息执行加解密操作的步骤之后，所述安全套接层加速方法还包括：

通过所述加速服务器基于所述加解密操作得到操作结果；

控制所述加速服务器将所述操作结果返回至所述无密钥代理节点。

[权利要求 8]

一种安全套接层加速装置，其中，所述安全套接层加速装置包括：

分离模块，用于在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；

转发模块，用于通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；

调用模块，用于在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；

发送模块，用于在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；

执行模块，用于控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。

[权利要求 9]

如权利要求8所述的安全套接层加速装置，其中，所述接入层还设有Nginx服务器；所述分离模块包括：

请求单元，用于在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；

处理单元，用于控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；

判断单元，用于控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制所述OpenSSL基于所述处理结果判断与所述用户端是

否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。

[权利要求 10] 如权利要求9所述的安全套接层加速装置，其中，所述接入层还包括第一数据库，所述处理单元还用于：
控制所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；
控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。

[权利要求 11] 如权利要求8所述的安全套接层加速装置，其中，所述调用模块还用于：
在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息，通过远程过程调用RPC进行异步调用所述无密钥代理节点。

[权利要求 12] 如权利要求8所述的安全套接层加速装置，其中，所述调用模块还用于：
控制所述无密钥代理节点基于所述代理服务器调用所述无密钥代理节点对应的调用信息，生成调用请求信息；
控制所述无密钥代理节点将所述调用请求信息实时上传至所述OpenSSL。

[权利要求 13] 如权利要求8所述的安全套接层加速装置，其中，所述加速卡集群还包括第二数据库；所述发送模块还用于：
控制所述无密钥代理节点基于所述加解密信息，从所述第二数据库获取所述私钥信息；
控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器。

[权利要求 14] 如权利要求8所述的安全套接层加速装置，其中，所述安全套接层加速装置还包括返回模块，所述返回模块用于：
通过所述加速服务器基于所述加解密操作得到操作结果；

控制所述加速服务器将所述操作结果返回至所述无密钥代理节点。

- [权利要求 15] 一种安全套接层加速设备，其中，所述安全套接层加速设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的安全套接层加速程序，所述安全套接层加速程序被所述处理器执行时实现如下步骤：
- 在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；
- 通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；
- 在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；
- 在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；
- 控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。

- [权利要求 16] 如权利15所述的安全套接层加速设备，其中，所述安全套接层加速程序被所述处理器执行时还实现如下步骤：
- 在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；
- 控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；
- 控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制所述OpenSSL基于所述处理结果判断与所述用户端是否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。

- [权利要求 17] 如权利要求16所述的安全套接层加速设备，其中，所述安全套接层加速程序被所述处理器执行时还实现如下步骤：
控制所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；
控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。
- [权利要求 18] 一种可读存储介质，其中，所述可读存储介质上存储有安全套接层加速程序，所述安全套接层加速程序被处理器执行时实现如下步骤：
在检测到用户端与接入层握手成功后，通过所述接入层进行安全套接层SSL协议握手与加解密信息分离，其中，所述接入层设有软件库包OpenSSL及代理服务器；
通过所述接入层控制所述OpenSSL将所述加解密信息转发到所述代理服务器；
在所述代理服务器接收到所述加解密信息后，控制所述代理服务器基于所述加解密信息异步调用加速卡集群，其中，所述加速卡集群包括无密钥代理节点及加速服务器；
在所述无密钥代理节点获取到所述加解密信息对应的私钥信息后，控制所述无密钥代理节点将所述私钥信息及所述加解密信息发送至所述加速服务器；
控制所述加速服务器基于所述私钥信息对所述加解密信息执行加解密操作。
- [权利要求 19] 如权利要求18所述的可读存储介质，其中，所述安全套接层加速程序被处理器执行时还实现如下步骤：
在检测到用户端发起的HTTPS请求时，控制所述Nginx服务器基于所述HTTPS请求与所述用户端建立TCP连接，并生成安全套接层SSL；
控制所述Nginx服务器基于所述SSL将SSL握手请求发送至所述OpenSSL，其中，所述SSL握手请求包括所述SSL协议握手及所述加解密信息；
控制所述OpenSSL对所述SSL握手请求进行处理得到处理结果，并控制

所述OpenSSL基于所述处理结果判断与所述用户端是否握手成功，其中，若是，则控制所述OpenSSL进行所述SSL协议握手与所述加解密信息分离。

[权利要求 20] 如权利要求19所述的可读存储介质，其中，所述安全套接层加速程序被处理器执行时还实现如下步骤：
控制所述Nginx服务器基于所述SSL，从所述第一数据库获取虚拟密码；
控制所述Nginx服务器基于所述虚拟密码将所述SSL握手请求发送至所述OpenSSL处理。

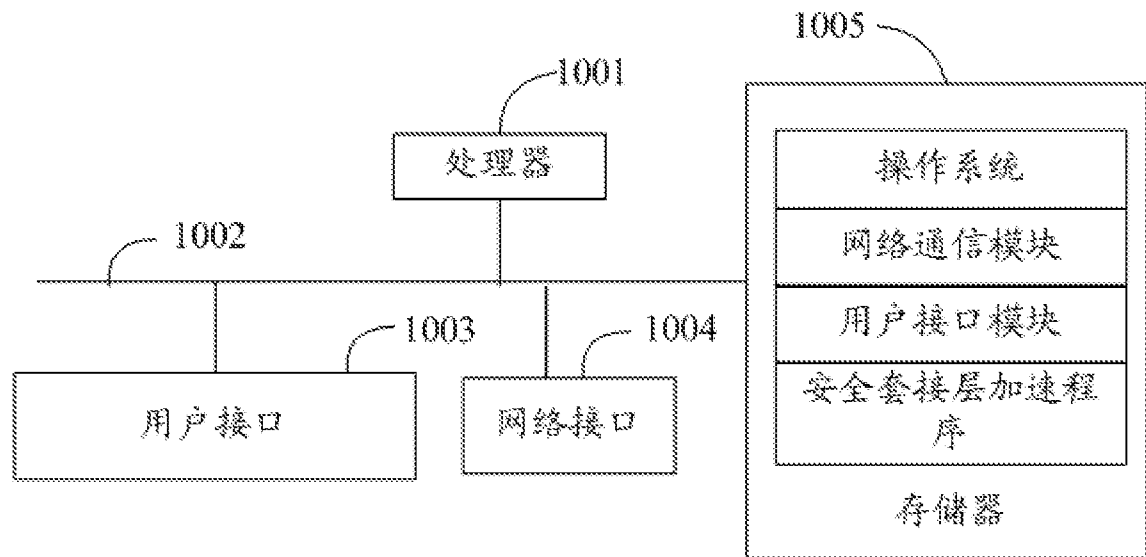


图 1

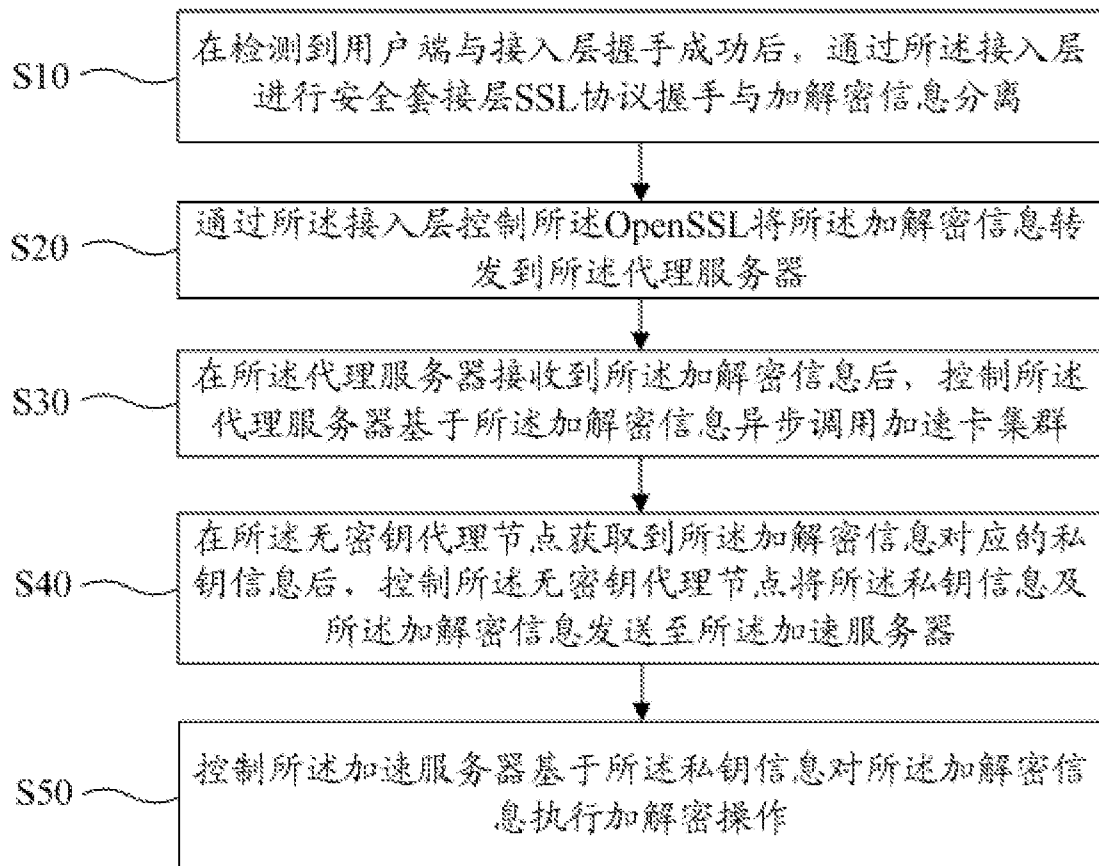


图 2

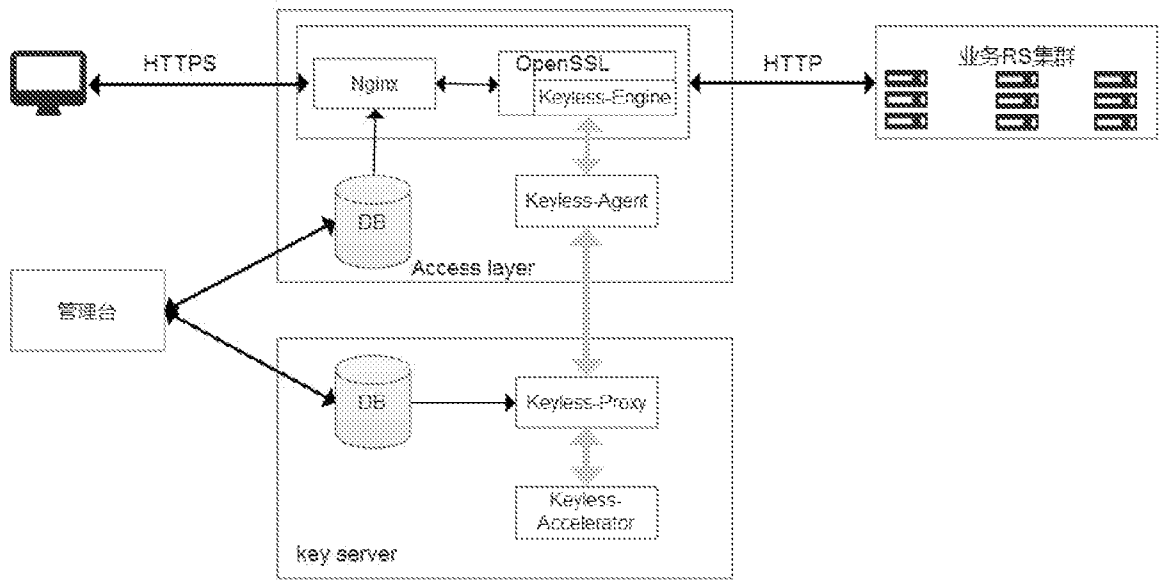


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/078395

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i; G06F 8/65(2018.01)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; 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)

CNPAT, EPODOC, WPI, CNKI, GOOGLE: 安全套接层, 加速, 速度, 握手, 分离, 分开, 分解, 加密, 解密, 异步, 调用, 加速卡, 代理, 服务器, SSL, secure socket layer, accelerat+, speed, handshake, separat+, crypto+, encrypt+, decrypt+, async+, proxy, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110071933 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 30 July 2019 (2019-07-30) claims 1-15	1-20
A	CN 109428876 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 05 March 2019 (2019-03-05) description, paragraphs [0036]-[0083]	1-20
A	CN 106027646 A (DU, Zaidong) 12 October 2016 (2016-10-12) entire document	1-20
A	US 2007074282 A1 (BLACK, Jeffrey T. et al.) 29 March 2007 (2007-03-29) entire document	1-20
A	HU, Xiaokang et al. "QTLS: High-Performance TLS Asynchronous Offload Framework with Intel® QuickAssist Technology," PPoPP'19, https://doi.org/10.1145/3293883.3295705 , 20 February 2019 (2019-02-20), entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 May 2020

Date of mailing of the international search report

29 May 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/078395

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	李爱玲 (LI, Ailing). "基于SSL加速的电子商务安全机制 (Safe Mechanism of Electronic Commerce Based on SSL Acceleration)" 安阳大学学报 (<i>Journal of Anyang Institute of Technology</i>), No. 3, 30 September 2003 (2003-09-30), entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/078395

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110071933	A	30 July 2019	None	
CN	109428876	A	05 March 2019	None	
CN	106027646	A	12 October 2016	None	
US	2007074282	A1	29 March 2007	None	

国际检索报告

国际申请号

PCT/CN2020/078395

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i; G06F 8/65(2018.01)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; 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))

CNPAT, EP0DOC, WPI, CNKI, G00GLE: 安全套接层, 加速, 速度, 握手, 分离, 分开, 分解, 加密, 解密, 异步, 调用, 加速卡, 代理, 服务器, SSL, secure socket layer, accelerat+, speed, handshake, separat+, crypto+, encr-ypt+, decrypt+, async+, proxy, server

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 110071933 A (深圳前海微众银行股份有限公司) 2019年 7月 30日 (2019 - 07 - 30) 权利要求1-15	1-20
A	CN 109428876 A (腾讯科技深圳有限公司) 2019年 3月 5日 (2019 - 03 - 05) 说明书第[0036]-[0083]段	1-20
A	CN 106027646 A (杜在东) 2016年 10月 12日 (2016 - 10 - 12) 全文	1-20
A	US 2007074282 A1 (BLACK, Jeffrey T. 等) 2007年 3月 29日 (2007 - 03 - 29) 全文	1-20
A	HU, Xiaokang等, . "QTLS: High-Performance TLS Asynchronous Offload Framework with Intel® QuickAssist Technology, " PPOPP' 19, https://doi.org/10.1145/3293883.3295705 , , 2019年 2月 20日 (2019 - 02 - 20), 全文	1-20
A	李爱玲, . "基于SSL加速的电子商务安全机制, " 安阳大学学报, , 第3期, 2003年 9月 30日 (2003 - 09 - 30), 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2020年 5月 18日

国际检索报告邮寄日期

2020年 5月 29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

受权官员

刘姗

电话号码 86-10-53961626

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/078395

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	110071933	A	2019年 7月 30日	无	
CN	109428876	A	2019年 3月 5日	无	
CN	106027646	A	2016年 10月 12日	无	
US	2007074282	A1	2007年 3月 29日	无	