



(12) 发明专利申请

(10) 申请公布号 CN 117081802 A

(43) 申请公布日 2023. 11. 17

(21) 申请号 202311030083.4

H04L 69/08 (2022.01)

(22) 申请日 2023.08.15

(71) 申请人 中移动信息技术有限公司

地址 102200 北京市昌平区未来科学城英才北三街16号院16号楼1006室

申请人 中国移动通信集团有限公司
北京大学

(72) 发明人 叶可可 关志 方有轩 赖思为
赵思远 郑旭晓 陈钟 王珂
孙磊

(74) 专利代理机构 深圳市世纪恒程知识产权代理事务所 44287

专利代理师 李静

(51) Int. Cl.

H04L 9/40 (2022.01)

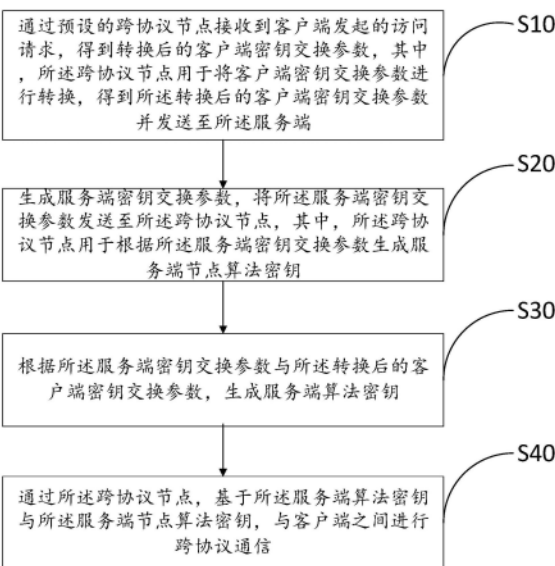
权利要求书3页 说明书16页 附图4页

(54) 发明名称

加密通信方法、装置、终端设备以及存储介质

(57) 摘要

本申请公开了加密通信方法、装置、终端设备以及存储介质,涉及通信技术领域,其方法包括:通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数;生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。本发明提高了不同密码协议间通信的自动化程度。



1. 一种加密通信方法,其特征在于,应用于服务端,所述加密通信方法包括:

通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

2. 根据权利要求1所述的加密通信方法,其特征在于,所述通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数和生成服务端密钥交换参数的步骤之前还包括:

生成服务端签名密钥和通信密钥;

将所述服务端签名密钥发送至所述客户端,与所述客户端进行密钥交换,生成密钥交换信息;

根据所述服务端签名密钥,对所述通信密钥进行重签名,生成服务端签署证书;

将所述密钥交换信息和所述服务端签署证书发送至预设的中间节点,其中,所述中间节点用于根据密钥交换信息对服务端签署证书进行重新签署得到中间节点签署后的服务端签署证书并发送至所述服务端;

将所述中间节点签署后的服务端签署证书发送至所述客户端,其中,所述客户端对所述中间节点签署后的服务端签署证书进行重新签署得到三方签署证书并发送至所述服务端;

根据所述三方签署证书,将所述中间节点部署为所述跨协议节点。

3. 根据权利要求1所述的加密通信方法,其特征在于,所述通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数的步骤包括:

当接收到客户端发起访问请求时,基于所述跨协议节点,获取转换后的客户端握手信息,其中,所述跨协议节点用于对所述客户端握手信息进行转换,得到所述转换后的客户端握手信息并发送至所述服务端;

生成服务端握手信息,将所述服务端握手信息发送至所述跨协议节点;其中,所述跨协议节点用于对所述服务端握手信息进行转换,得到所述转换后的服务端握手信息并发送至客户端;

基于所述跨协议节点,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于对所述客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至服务端;

根据所述转换后的客户端密钥交换参数,生成所述服务端密钥交换参数。

4. 根据权利要求1所述的加密通信方法,其特征在于,所述通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,客户端之间进行跨协议通信的步骤包括:

获取原始服务端通信信息；

根据所述服务端算法密钥,对所述原始服务端通信信息进行加密,得到加密后的服务端通信信息；

将所述加密后的服务端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端节点算法密钥,对所述加密后的服务端通信信息进行解密后加密得到节点加密后的服务端通信信息,将所述节点加密后的服务端通信信息发送至所述客户端。

5.根据权利要求4所述的加密通信方法,其特征在于,所述通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,客户端之间进行跨协议通信的步骤还包括:

当接收到节点加密后的客户端通信信息时,根据所述服务端算法密钥对所述节点加密后的客户端通信信息进行解密,得到原始客户端通信信息。

6.一种加密通信方法,其特征在于,应用于客户端,所述加密通信方法包括:

当发起访问请求时,生成客户端密钥交换参数并把所述客户端密钥交换参数发送至预设的跨协议节点;

基于所述跨协议节点,获得转换后的服务端密钥交换参数,其中,所述跨协议节点用于将服务端密钥交换参数进行转换,得到所述转换后的服务端密钥交换参数并发送至所述客户端,所述跨协议节点用于根据所述客户端密钥交换参数生成客户端节点算法密钥;

根据所述客户端密钥交换参数与所述转换后的服务端密钥交换参数,生成客户端算法密钥;

通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信。

7.根据权利要求6所述的加密通信方法,其特征在于,所述通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信的步骤包括:

获取原始客户端通信信息;

根据所述客户端算法密钥,对所述原始客户端通信信息进行加密,得到加密后的客户端通信信息;

将所述加密后的客户端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述客户端节点算法密钥,对所述加密后的客户端通信信息进行解密后加密得到节点加密后的客户端通信信息,将所述节点加密后的客户端通信信息发送至所述服务端。

8.根据权利要求7所述的加密通信方法,其特征在于,所述通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信的步骤还包括:

当接收到节点加密后的服务端通信信息时,根据所述客户端算法密钥对所述节点加密后的服务端通信信息进行解密,得到原始服务端通信信息。

9.一种加密通信装置,其特征在于,所述加密通信装置包括:

密钥参数生成模块,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

参数交换发模块,用于生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

算法密钥生成模块,用于根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

跨协议通信模块,用于通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

10.一种终端设备,其特征在于,所述终端设备包括存储器、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加密通信程序,所述加密通信程序被所述处理器执行时实现如权利要求1-5中任一项所述的加密通信方法的步骤。

11.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有加密通信程序,所述加密通信程序被处理器执行时实现如权利要求1-5中任一项所述的加密通信方法的步骤。

加密通信方法、装置、终端设备以及存储介质

技术领域

[0001] 本申请涉及通信技术领域,尤其涉及一种加密通信方法、装置、终端设备以及存储介质。

背景技术

[0002] 国密协议是国密应用中的关键技术之一,广泛用于Web、VPN、区块链等应用领域。国密的TLCP(Trusted Logical Connection Protocol,可信逻辑连接协议)虽然总体上和SSL(Secure Socket Layer,安全套接层)/TLS(Transport Layer Security,传输层安全性)国际协议标准类似,但是在采用的密码算法上和协议的一些细节上和国际标准有所不同。有的服务端只支持国密协议,有的客户端只支持国际协议,所以需要进行密码协议替换。

[0003] 目前,替换国际密码协议为国密协议的通用做法是,分析解读密码应用的源代码,找出其中所使用的密码协议算法,逐一将其替换为国密算法。例如,在源代码中发现使用了密码协议TLS,那么,需要将该算法修改替换为国密协议TLCP。

[0004] 然而,国际密码协议已经内置在很多密码应用系统中,比如浏览器、Web服务器、区块链节点、VPN软件等等,要替换这些通用软件中的国际密码协议需要阅读解析源码,而这些软件不一定是开源软件,而且对密码应用的国密替换需要对源码进行修改,找出修改位置并在源码上进行替换修改。因此,通用的替换密码协议方法的自动化程度比较低。

发明内容

[0005] 本申请的主要目的在于提供一种加密通信方法、装置、终端设备以及存储介质,旨在提高不同密码协议间通信的自动化程度。

[0006] 为实现上述目的,本申请提供一种加密通信方法,应用于服务端,所述加密通信方法包括:

[0007] 通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

[0008] 生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

[0009] 根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

[0010] 通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

[0011] 可选地,所述通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数和生成服务端密钥交换参数的步骤之前还包括:

[0012] 生成服务端签名密钥和通信密钥;

[0013] 将所述服务端签名密钥发送至所述客户端,与所述客户端进行密钥交换,生成密钥交换信息;

[0014] 根据所述服务端签名密钥,对所述通信密钥进行重签名,生成服务端签署证书;

[0015] 将所述密钥交换信息和所述服务端签署证书发送至预设的中间节点,其中,所述中间节点用于根据密钥交换信息对服务端签署证书进行重新签署得到中间节点签署后的服务端签署证书并发送至所述服务端;

[0016] 将所述中间节点签署后的服务端签署证书发送至所述客户端,其中,所述客户端对所述中间节点签署后的服务端签署证书进行重新签署得到三方签署证书并发送至所述服务端;

[0017] 根据所述三方签署证书,将所述中间节点部署为所述跨协议节点。

[0018] 可选地,所述通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数的步骤包括:

[0019] 当接收到客户端发起访问请求时,基于所述跨协议节点,获取转换后的客户端握手信息,其中,所述跨协议节点用于对所述客户端握手信息进行转换,得到所述转换后的客户端握手信息并发送至所述服务端;

[0020] 生成服务端握手信息,将所述服务端握手信息发送至所述跨协议节点;其中,所述跨协议节点用于对所述服务端握手信息进行转换,得到所述转换后的服务端握手信息并发送至客户端;

[0021] 基于所述跨协议节点,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于对所述客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至服务端;

[0022] 根据所述转换后的客户端密钥交换参数,生成所述服务端密钥交换参数。

[0023] 可选地,所述通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,客户端之间进行跨协议通信的步骤包括:

[0024] 获取原始服务端通信信息;

[0025] 根据所述服务端算法密钥,对所述原始服务端通信信息进行加密,得到加密后的服务端通信信息;

[0026] 将所述加密后的服务端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端节点算法密钥,对所述加密后的服务端通信信息进行解密后加密后得到节点加密后的服务端通信信息,将所述节点加密后的服务端通信信息发送至所述客户端。

[0027] 可选地,所述通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,客户端之间进行跨协议通信的步骤还包括:

[0028] 当接收到节点加密后的客户端通信信息时,根据所述服务端算法密钥对所述节点加密后的客户端通信信息进行解密,得到原始客户端通信信息。

[0029] 本申请还提供一种加密通信方法,应用于客户端,所述加密通信方法包括:

[0030] 当发起访问请求时,生成客户端密钥交换参数并把所述客户端密钥交换参数发送至预设的跨协议节点;

[0031] 基于所述跨协议节点,获得转换后的服务端密钥交换参数,其中,所述跨协议节点

用于将服务端密钥交换参数进行转换,得到所述转换后的服务端密钥交换参数并发送至所述客户端,所述跨协议节点用于根据所述客户端密钥交换参数生成客户端节点算法密钥;

[0032] 根据所述客户端密钥交换参数与所述转换后的服务端密钥交换参数,生成客户端算法密钥;

[0033] 通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信。

[0034] 可选地,所述通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信的步骤包括:

[0035] 获取原始客户端通信信息;

[0036] 根据所述客户端算法密钥,对所述原始客户端通信信息进行加密,得到加密后的客户端通信信息;

[0037] 将所述加密后的客户端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述客户端节点算法密钥,对所述加密后的客户端通信信息进行解密后加密得到节点加密后的客户端通信信息,将所述节点加密后的客户端通信信息发送至所述服务端。

[0038] 可选地,所述通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信的步骤还包括:

[0039] 当接收到节点加密后的服务端通信信息时,根据所述客户端算法密钥对所述节点加密后的服务端通信信息进行解密,得到原始服务端通信信息。

[0040] 本申请实施例还提出一种加密通信装置,所述加密通信装置包括:

[0041] 密钥参数生成模块,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

[0042] 参数交换发模块,用于生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

[0043] 算法密钥生成模块,用于根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

[0044] 跨协议通信模块,用于通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

[0045] 本申请实施例还提出一种终端设备,所述终端设备包括存储器、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加密通信程序,所述加密通信程序被所述处理器执行时实现如上所述的加密通信方法的步骤。

[0046] 本申请实施例还提出一种计算机可读存储介质,所述计算机可读存储介质上存储有加密通信程序,所述加密通信程序被处理器执行时实现如上所述的加密通信方法的步骤。

[0047] 本申请实施例提出的加密通信方法、装置、终端设备以及存储介质,通过通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所

述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,提高不同密码协议间通信的自动化程度。

附图说明

- [0048] 图1为本申请加密通信装置所属终端设备的功能模块示意图;
- [0049] 图2为本申请加密通信方法第一示例性实施例的流程示意图;
- [0050] 图3为本申请加密通信方法涉及的证书重签名流程示意图;
- [0051] 图4为本申请加密通信方法涉及的跨协议通信流程示意图1;
- [0052] 图5为本申请加密通信方法涉及的跨协议通信流程示意图2。
- [0053] 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。

具体实施方式

- [0054] 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。
 - [0055] 本申请实施例的主要解决方案是:通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,提高不同密码协议间通信的自动化程度。
 - [0056] 本申请实施例考虑到,目前替换国际密码协议为国密协议的通用做法是,分析解
- 读密码应用的源代码,找出其中所使用的密码协议算法,逐一将其替换为国密算法。例如,

在源代码中发现使用了密码协议TLS,那么,需要将该算法修改替换为国密协议TLCP。

[0057] 然而,国际密码协议已经内置在很多密码应用系统中,比如浏览器、Web服务器、区块链节点、VPN软件等等,要替换这些通用软件中的国际密码协议需要阅读解析源码,而这些软件不一定是开源软件,而且对密码应用的国密替换需要对源码进行修改,找出修改位置并在源码上进行替换修改。因此,通用的替换密码协议方法的自动化程度比较低。

[0058] 基于此,本申请实施例提出一种解决方案,当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议。

[0059] 具体地,参照图1,图1为本申请加密通信装置所属终端设备的功能模块示意图。该加密通信装置可以为独立于终端设备的、能够进行数据处理的装置,也可以通过硬件或软件的形式承载于终端设备上。

[0060] 在本实施例中,该加密通信装置所属终端设备至少包括输出模块110、处理器120、存储器130以及通信模块140。

[0061] 存储器130中存储有操作系统以及加密通信程序,当客户端向服务端发起访问请求时,基于预设的跨协议节点,建立所述客户端与所述服务端的握手连接,得到服务端密钥交换参数与客户端密钥交换参数;基于所述跨协议节点,根据所述服务端密钥交换参数与所述客户端密钥交换参数,建立所述客户端与所述服务端的密钥参数交换连接,生成服务端算法密钥、客户端算法密钥和节点算法密钥存储于该存储器130中;输出模块110可为显示屏、扬声器等。通信模块140可以包括WIFI模块、移动通信模块以及蓝牙模块等,通过通信模块140与外部设备或服务器进行通信。

[0062] 其中,存储器130中的加密通信程序被处理器执行时实现以下步骤:

[0063] 当接收到客户端发起的访问请求时,基于预设的跨协议节点,得到服务端密钥交换参数与客户端密钥交换参数;

[0064] 基于所述跨协议节点,根据所述服务端密钥交换参数与所述客户端密钥交换参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥;

[0065] 基于所述跨协议节点,通过所述服务端算法密钥、所述客户端算法密钥和所述节点算法密钥,在所述客户端与所述服务端之间进行跨协议通信。

[0066] 进一步地,存储器130中的加密通信程序被处理器执行时还实现以下步骤:

[0067] 通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

[0068] 生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

[0069] 根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端

算法密钥;

[0070] 通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

[0071] 进一步地,存储器130中的加密通信程序被处理器执行时还实现以下步骤:

[0072] 生成服务端签名密钥和通信密钥;

[0073] 将所述服务端签名密钥发送至所述客户端,与所述客户端进行密钥交换,生成密钥交换信息;

[0074] 根据所述服务端签名密钥,对所述通信密钥进行重签名,生成服务端签署证书;

[0075] 将所述密钥交换信息和所述服务端签署证书发送至预设的中间节点,其中,所述中间节点用于根据密钥交换信息对服务端签署证书进行重新签署得到中间节点签署后的服务端签署证书并发送至所述服务端;

[0076] 将所述中间节点签署后的服务端签署证书发送至所述客户端,其中,所述客户端对所述中间节点签署后的服务端签署证书进行重新签署得到三方签署证书并发送至所述服务端;

[0077] 根据所述三方签署证书,将所述中间节点部署为所述跨协议节点。

[0078] 进一步地,存储器130中的加密通信程序被处理器执行时还实现以下步骤:

[0079] 当接收到客户端发起访问请求时,基于所述跨协议节点,获取转换后的客户端握手信息,其中,所述跨协议节点用于对所述客户端握手信息进行转换,得到所述转换后的客户端握手信息并发送至所述服务端;

[0080] 生成服务端握手信息,将所述服务端握手信息发送至所述跨协议节点;其中,所述跨协议节点用于对所述服务端握手信息进行转换,得到所述转换后的服务端握手信息并发送至客户端;

[0081] 基于所述跨协议节点,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于对所述客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至服务端;

[0082] 根据所述转换后的客户端密钥交换参数,生成所述服务端密钥交换参数。

[0083] 进一步地,存储器130中的加密通信程序被处理器执行时还实现以下步骤:

[0084] 获取原始服务端通信信息;

[0085] 根据所述服务端算法密钥,对所述原始服务端通信信息进行加密,得到加密后的服务端通信信息;

[0086] 将所述加密后的服务端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端节点算法密钥,对所述加密后的服务端通信信息进行解密后加密后得到节点加密后的服务端通信信息,将所述节点加密后的服务端通信信息发送至所述客户端。

[0087] 进一步地,存储器130中的加密通信程序被处理器执行时还实现以下步骤:

[0088] 当接收到节点加密后的客户端通信信息时,根据所述服务端算法密钥对所述节点加密后的客户端通信信息进行解密,得到原始客户端通信信息。

[0089] 本实施例通过上述方案,通过当接收到客户端发起的访问请求时,基于预设的跨协议节点,得到服务端密钥交换参数与客户端密钥交换参数;基于所述跨协议节点,根据所

述服务端密钥交换参数与所述客户端密钥交换参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥;基于所述跨协议节点,通过所述服务端算法密钥、所述客户端算法密钥和所述节点算法密钥,在所述客户端与所述服务端之间进行跨协议通信。当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,提高不同密码协议间通信的自动化程度。

[0090] 基于上述终端设备架构但不限于上述架构,提出本申请方法实施例。

[0091] 参照图2,图2为本申请加密通信方法第一示例性实施例的流程示意图。

[0092] 本发明一实施例提供一种加密通信方法,该方法包括:

[0093] 步骤S10,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

[0094] 密码协议通常指密码设备之间、密码管理者之间、密码管理者与被管理者之间,以及密码系统与所服务的用户之间,为完成密钥传递、数据传输,或者状态信息、控制信息交换等与密码通信相关的活动,所约定的通信格式、步骤,以及规定的密码运算方法、所使用的密钥数据等。最常使用的密码协议是SSL/TLS。

[0095] 国密SSL协议(即国标GB/T标准的TLCP协议)是国密应用中的关键技术之一,广泛用于Web、VPN、区块链等应用领域。国密的TLCP协议虽然总体上和SSL/TLS国际协议标准类似,但是在采用的密码算法上和协议的一些细节上和国际标准有所不同。有的服务端只支持国密协议,有的客户端只支持国际协议,所以需要进行密码协议替换。

[0096] 目前,替换国际密码协议为国密协议的通用做法是,分析解读密码应用的源代码,找出其中所使用的密码协议算法,逐一将其替换为国密算法。例如,在源代码中发现使用了密码协议TLS,那么,需要将该算法修改替换为国密协议TLCP。

[0097] 然而,国际密码协议已经内置在很多密码应用系统中,比如浏览器、Web服务器、区块链节点、VPN软件等等,要替换这些通用软件中的国际密码协议需要阅读解析源码,而这些软件不一定是开源软件,而且对密码应用的国密替换需要对源码进行修改,找出修改位置并在源码上进行替换修改。因此,通用的替换密码协议方法的自动化程度比较低。

[0098] 因此,本实施例提出当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执

行,无需修改代码或密码协议,从而实现提高不同密码协议间通信的自动化程度。

[0099] 具体地,该跨协议节点会将国密协议以及字段自动转换为原国际密码协议软件可以识别的协议及字段,同理该跨协议节点会将国际协议以及字段自动转换为国密协议软件可以识别的协议及字段。

[0100] 进一步地,跨协议节点能够自动识别国际密码协议通信,并根据策略决定是否执行国密的转换工作。并且能够对信息中的执行标识符、对称密码、证书、签名值等字段的替换,实现跨协议通信交流。

[0101] 具体地,跨协议节点可以是代理服务器,也可以是网关服务器。通过跨协议节点作为客户端和服务端中间方的角色,转换对应密码协议的信息,实现客户端和服务端仅需发送自身密码协议对应的握手信息,即可建立握手连接,然后生成对应的服务端密钥交换参数与客户端密钥交换参数。

[0102] 步骤S20,生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

[0103] 步骤S30,根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

[0104] 为了加强后续的服务端与客户端的通信的安全性和便捷性,需要建立一套定制化的算法密钥用于后续通信。

[0105] 具体地,跨协议节点(网关)截取该服务端密钥交换参数,记录服务端密钥交换参数,使其符合国际协议标准,重新生成转换后的服务端密钥交换参数。

[0106] 客户端根据转换后的服务端密钥交换参数生成客户端算法密钥,即国际算法密钥,服务端根据转换后的客户端密钥交换参数生成服务端算法密钥,即国密算法密钥。网关分别生成与客户端和服务器的加密密钥,即国际算法加密密钥,与国密算法加密密钥。

[0107] 最后根据国际算法密钥、国密算法密钥、国际算法加密密钥,与国密算法加密密钥进行服务端和客户端的通信。

[0108] 根据转换后的服务端密钥交换参数和客户端密钥交换参数生成对应的算法密钥,即国际算法密钥和国密算法密钥。这种方式允许客户端和服务端在不同的密码协议之间进行通信,提高了跨协议通信的可行性,并且这意味着网关在加密通信过程中扮演了重要的角色,提供了独立的密钥生成机制。这样可以增强通信的安全性,使得客户端和服务端之间的加密密钥不会直接泄露或暴露给对方。

[0109] 可以理解地,基于跨协议节点,将服务端密钥交换参数与客户端密钥交换参数自动的转换为对方协议对应的转换后的服务端密钥交换参数和转换后的客户端密钥交换参数,服务端和客户端收到对方的转换后参数密钥后建立密钥参数交换连接,服务端和客户端交换密钥参数。并且生成用于后续通信的服务端算法密钥和客户端算法密钥,同时基于跨协议节点生成对应的节点算法密钥。

[0110] 步骤S40,通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

[0111] 具体地,在后续服务端与客户端通信时,通过三方的算法密钥对通信消息进行相应的处理,从而建立客户端和所述服务端的加密通信连接。

[0112] 步骤S41,获取原始服务端通信信息;

[0113] 步骤S42,根据所述服务端算法密钥,对所述原始服务端通信信息进行加密,得到加密后的服务端通信信息;

[0114] 步骤S43,将所述加密后的服务端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端节点算法密钥,对所述加密后的服务端通信信息进行解密后加密后得到节点加密后的服务端通信信息,将所述节点加密后的服务端通信信息发送至所述客户端。

[0115] 步骤S44,当接收到节点加密后的客户端通信信息时,根据所述服务端算法密钥对所述节点加密后的客户端通信信息进行解密,得到原始客户端通信信息。

[0116] 具体地,客户端可直接通过客户端算法密钥加密对应的原始客户端通信信息,得到加密后的客户端通信信息然后发送给跨协议节点;跨协议节点通过服务端节点算法密钥解密该加密后的客户端通信信息,得到节点中间信息;然后再通过服务端节点算法密钥加密节点中间信息得到节点加密后的客户端通信信息,发送给服务端;最后服务端通过服务端密钥解密相应的节点加密后的客户端通信信息,得到符合服务端的密码协议的原始客户端通信信息。

[0117] 具体地,服务端可直接通过服务端算法密钥加密对应的原始服务端通信信息,得到加密后的服务端通信信息然后发送给跨协议节点;跨协议节点通过服务端节点算法密钥解密该加密后的服务端通信信息,得到节点中间信息;然后再通过客户端节点算法密钥加密节点中间信息得到节点加密后的服务端通信信息,发送给客户端;最后客户端通过客户端密钥解密相应的节点加密后的服务端通信信息,得到符合客户端的密码协议的原始服务器通信信息。

[0118] 可以理解地,通过三方的算法密钥对通信消息进行相应的处理,从而建立客户端和所述服务端的有效的通信,本方案能够自动化实现密码协议替换,提高不同密码协议间通信的自动化程度。

[0119] 可以理解地,本实施例提出的加密通信方法相较于现有通用技术方案有两个技术优点,一是不用修改源码,提高工作效率。本提案通过部署在网络边界上的跨协议节点(网关设备或VPN)自动化的替换密码协议,故而提高了效率;二是更加安全可靠。本提案不会修改源码,故而不会对原始密码应用造成影响,不会引入新的安全问题,并且,网关设备对原证书进行重签名,且运行在可信执行环境中,能够提供可信的服务。

[0120] 本申请实施例提出的加密通信方法,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协

议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,提高不同密码协议间通信的自动化程度。

[0121] 基于第一实施例,提出本申请第二实施例,本申请第二实施例与第一实施例的区别在于:通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数和生成服务端密钥交换参数的步骤之前进行补充,其中该步骤可以包括:

[0122] 在本实施例中,步骤S10,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数和生成服务端密钥交换参数的步骤之前还包括:

[0123] 步骤S01,生成服务端签名密钥和通信密钥;

[0124] 步骤S02,将所述服务端签名密钥发送至所述客户端,与所述客户端进行密钥交换,生成密钥交换信息;

[0125] 步骤S03,根据所述服务端签名密钥,对所述通信密钥进行重签名,生成服务端签署证书;

[0126] 步骤S04,将所述密钥交换信息和所述服务端签署证书发送至预设的中间节点,其中,所述中间节点用于根据密钥交换信息对服务端签署证书进行重新签署得到中间节点签署后的服务端签署证书并发送至所述服务端;

[0127] 步骤S05,将所述中间节点签署后的服务端签署证书发送至所述客户端,其中,所述客户端对所述中间节点签署后的服务端签署证书进行重新签署得到三方签署证书并发送至所述服务端;

[0128] 步骤S06,根据所述三方签署证书,将所述中间节点部署为所述跨协议节点。

[0129] 为了实现自动化的替换密码协议,需要建立对应的跨协议节点,在服务端和客户端通信之前,可以通过交换签名密钥,重签名对应的证书,使得重签名的证书得到双方信任,从而根据重签名证书建立跨协议节点。

[0130] 具体地,此阶段是代理重签名生成可信证书的阶段,通过可信证书建立新的中间代理,即跨协议节点。

[0131] 更具体地,代理重签名是一个至少由三方组成的可信工作模型,服务端、客户端和中间节点(代理)。

[0132] 以下基于ElGamal(迪菲-赫尔曼,ElGamal加密算法是一个基于迪菲-赫尔曼密钥交换的非对称加密算法,它在1985年由塔希尔·盖莫尔提出)算法重签名的过程为例,具体加密算法过程是先声明有一个以大素数 q 为阶以 g 为生成元的群 G ,取随机数 $sk=a$ 为私钥,那么公钥即为 $pk=g^a$ 。取随机数 r ,那么加密数据为 $(pk^r, g^r \cdot m) = ((g^a)^r, g^r \cdot m)$,代理重签名密钥计算为 $rk_{A \rightarrow B} = sk_B / sk_A \bmod q = b/a \bmod q$,进行重签名的过程为 $((g^{ar})^{b/a}, m \cdot gr) = (gb^r, m \cdot g^r)$ 。

[0133] 进一步地,以一个支持国密TLCP协议的Web服务端,和一个仅支持SSL/TLS协议的浏览器的客户端为基础,部署跨协议节点为例。如图2所示,具体流程如下:

[0134] 首先,TLCP国密服务器的CA(Certificate Authority server,证书颁发机构)服务器生成服务端签名密钥 (g^a, a) ,SSL浏览器客户端的CA服务器生成客户端签名密钥 (g^b, b) ;

[0135] 然后, TLCP国密服务器生成通信密钥 m , 使用服务端签名密钥对通信密钥 m 进行重签名, CA服务器签署生成对应服务端签署证书 $((g^a)^r, g^r \cdot m)$, 其中, r 为随机因子。

[0136] 然后, TLCP国密服务器的CA服务器和SSL浏览器客户端的CA服务器使用DH协议交换密钥信息, 得到密钥交换信息 (a, b) 。

[0137] 然后, TLCP国密服务器根据密钥信息生成重签名密钥 b/a , 并秘密转交给中间节点(网关/代理)。

[0138] 中间节点(网关/代理)对服务端签署证书验证后, 使用重签名密钥 b/a 对服务端签署证书 $((g^a)^r, g^r \cdot m)$ 进行重签名, 得到节点服务端签署证书 $((g^{ar})^{b/a}, m \cdot g^r)$ 。

[0139] SSL浏览器客户端对节点服务端签署证书验证后, 对节点服务端签署证书重签名得到三方签署证书, 具体过程为 $((g^{ar})^{b/a}, m \cdot g^r) = (g^{br}, m \cdot g^r)$ 。

[0140] 根据三方签署证书, 把中间节点部署为双方可信的中间代理, 即跨协议节点, 从而实现后续的跨协议通信交流。

[0141] 可以理解地, 此阶段是重签名生成可信证书和部署跨协议节点的阶段。通过客户端和服务端双方的协议生成的签名密钥, 生成重签名生成可信证书即三方签署证书, 再根据该证书建立相应的跨协议节点, 使跨协议节点可以将国密协议以及字段自动转换为原国际密码协议软件可以识别的协议及字段, 同理该跨协议节点也可以将国际协议以及字段自动转换为国密协议软件可以识别的协议及字段。

[0142] 进一步地, 跨协议节点能够自动识别国际密码协议通信, 并根据策略决定是否执行国密的转换工作。并且能够对信息中的执行标识符、对称密码、证书、签名值等字段的替换, 实现跨协议通信交流。

[0143] 此外, 还需要通过对服务端签署证书和节点服务端签署证书检验进行验证, 可以确保所使用的证书是合法有效的。如果验证不通过, 即证书存在问题或未经授权, 就不会对该服务端签署证书进行重签名。这有助于减少潜在的安全风险和防止恶意的证书使用。

[0144] 此外, 可以防止篡改, 具体对服务端签署证书和节点服务端签署证书检验进行验证可以确保证书的完整性。如果证书在传输过程中被篡改或损坏, 验证将失败, 从而防止对篡改后的证书进行重签名, 保证了证书的可靠性。

[0145] 可以理解地, 对服务端签署证书和节点服务端签署证书检验, 有助于提高系统的安全性和可信度, 防止潜在的证书问题和安全威胁, 同时保护证书生态系统的完整性和可靠性。

[0146] 本申请实施例提出的加密通信方法, 通过生成服务端签名密钥和通信密钥; 将所述服务端签名密钥发送至所述客户端, 与所述客户端进行密钥交换, 生成密钥交换信息; 根据所述服务端签名密钥, 对所述通信密钥进行重签名, 生成服务端签署证书; 将所述密钥交换信息和所述服务端签署证书发送至预设的中间节点, 其中, 所述中间节点用于根据密钥交换信息对服务端签署证书进行重新签署得到中间节点签署后的服务端签署证书并发送至所述服务端; 将所述中间节点签署后的服务端签署证书发送至所述客户端, 其中, 所述客户端对所述中间节点签署后的服务端签署证书进行重新签署得到三方签署证书并发送至所述服务端; 根据所述三方签署证书, 将所述中间节点部署为所述跨协议节点, 根据三方签署证书, 把中间节点部署为双方可信的中间代理, 即跨协议节点, 使跨协议节点可以将国密协议以及字段自动转换为原国际密码协议软件可以识别的协议及字段, 同理该跨协议节点

也可以将国际协议以及字段自动转换为国密协议软件可以识别的协议及字段,从而实现后续的跨协议通信交流。

[0147] 基于第一实施例,提出本申请第三实施例,本申请第三实施例与第一实施例的区别在于:对步骤S10,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数和生成服务端密钥交换参数的步骤进行细化,其中细化的步骤可以包括:

[0148] 在本实施例中,步骤S10,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数的步骤包括:

[0149] 步骤S11,当接收到客户端发起访问请求时,基于所述跨协议节点,获取转换后的客户端握手信息,其中,所述跨协议节点用于对所述客户端握手信息进行转换,得到所述转换后的客户端握手信息并发送至所述服务端;

[0150] 步骤S12,生成服务端握手信息,将所述服务端握手信息发送至所述跨协议节点;其中,所述跨协议节点用于对所述服务端握手信息进行转换,得到所述转换后的服务端握手信息并发送至客户端;

[0151] 步骤S13,基于所述跨协议节点,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于对所述客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至服务端;

[0152] 步骤S14,根据所述转换后的客户端密钥交换参数,生成所述服务端密钥交换参数。

[0153] 具体地,以客户端为SSL浏览器客户端,服务端为TLCP国密服务器为例,说明握手过程。当SSL浏览器客户端发起对TLCP国密服务器的访问请求,获取客户端握手信息,如Client hello数据包。该数据包中包含典型的国际密码算法标识符和字段。

[0154] 跨协议节点(网关)收到该数据包,对所述客户端握手信息进行解析,截取并留存字段信息,跨协议节点(网关)修改该数据包中TLS VERSION、Client Random、Cipher Suites等字段,得到转换后客户端握手信息,可以理解地转换后客户端握手信息符合国密标准,重新打包数据包后发送给服务端。

[0155] 国密服务器收到来自跨协议节点(网关)的转换后客户端握手信息后,国密服务器向客户端回复服务端握手信息,包括ServerHello数据包,并附上国密双证书。

[0156] 跨协议节点(网关)截取该服务端握手信息,记录协议字段;并修改该服务端握手信息数据包中TLS VERSION、Client Random、Cipher Suites等字段,使其符合国际算法标准得到转换后的服务端握手信息,重新打包后发给客户端,并且附上自己的国际算法证书。

[0157] 客户端收到来自跨协议节点的转换后的服务端握手信息,验证转换后的服务端握手信息中的国际算法证书,有效则保存随机数。

[0158] 然后,客户端向国密服务器发送密钥交换所需要的客户端密钥交换参数。

[0159] 跨协议节点(网关)截取该客户端密钥交换参数,记录客户端密钥交换参数,使其符合国密协议,重新生成转换后的客户端密钥交换参数,打包后发送给国密服务端。

[0160] 国密服务端收到来自跨协议节点(网关)的转换后的客户端密钥交换参数,记录转换后的客户端密钥交换参数后,国密服务端向客户端发送服务端密钥交换参数并签名。

[0161] 可以理解地,基于跨协议节点自动化建立握手连接,并完成交换密钥参数,提高了

不同密码协议间通信的自动化程度。

[0162] 本申请实施例提出的加密通信方法,通过当接收到客户端发起访问请求时,基于所述跨协议节点,获取转换后的客户端握手信息,其中,所述跨协议节点用于对所述客户端握手信息进行转换,得到所述转换后的客户端握手信息并发送至所述服务端;生成服务端握手信息,将所述服务端握手信息发送至所述跨协议节点;其中,所述跨协议节点用于对所述服务端握手信息进行转换,得到所述转换后的服务端握手信息并发送至客户端;基于所述跨协议节点,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于对所述客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至服务端;根据所述转换后的客户端密钥交换参数,生成所述服务端密钥交换参数,基于跨协议节点自动化建立握手连接,并完成交换密钥参数,提高了不同密码协议间通信的自动化程度。

[0163] 本发明一实施例提供一种加密通信方法,该方法包括:

[0164] 步骤S50,当发起访问请求时,生成客户端密钥交换参数并把所述客户端密钥交换参数发送至预设的跨协议节点;

[0165] 本实施例提出当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,从而实现提高不同密码协议间通信的自动化程度。

[0166] 具体地,该跨协议节点会将国密协议以及字段自动转换为原国际密码协议软件可以识别的协议及字段,同理该跨协议节点会将国际协议以及字段自动转换为国密协议软件可以识别的协议及字段。

[0167] 进一步地,跨协议节点能够自动识别国际密码协议通信,并根据策略决定是否执行国密的转换工作。并且能够对信息中的执行标识符、对称密码、证书、签名值等字段的替换,实现跨协议通信交流。

[0168] 具体地,跨协议节点可以是代理服务器,也可以是网关服务器。通过跨协议节点作为客户端和服务端中间方的角色,转换对应密码协议的信息,实现客户端和服务端仅需发送自身密码协议对应的握手信息,即可建立握手连接,然后生成对应的服务端密钥交换参数与客户端密钥交换参数。

[0169] 步骤S60,基于所述跨协议节点,获得转换后的服务端密钥交换参数,其中,所述跨协议节点用于将服务端密钥交换参数进行转换,得到所述转换后的服务端密钥交换参数并发送至所述客户端,所述跨协议节点用于根据所述客户端密钥交换参数生成客户端节点算法密钥;

[0170] 步骤S70,根据所述客户端密钥交换参数与所述转换后的服务端密钥交换参数,生成客户端算法密钥;

[0171] 为了加强后续的服务端与客户端的通信的安全性和便捷性,需要建立一套定制化的算法密钥用于后续通信。

[0172] 具体地,跨协议节点(网关)截取该服务端密钥交换参数,记录服务端密钥交换参数,使其符合国际协议标准,重新生成转换后的服务端密钥交换参数。

[0173] 客户端根据转换后的服务端密钥交换参数生成客户端算法密钥,即国际算法密钥,服务端根据转换后的客户端密钥交换参数生成服务端算法密钥,即国密算法密钥。网关分别生成与客户端和服务器的加密密钥,即国际算法加密密钥,与国密算法加密密钥。

[0174] 最后根据国际算法密钥、国密算法密钥、国际算法加密密钥,与国密算法加密密钥进行服务端和客户端的通信。

[0175] 根据转换后的服务端密钥交换参数和客户端密钥交换参数生成对应的算法密钥,即国际算法密钥和国密算法密钥。这种方式允许客户端和服务端在不同的密码协议之间进行通信,提高了跨协议通信的可行性,并且这意味着网关在加密通信过程中扮演了重要的角色,提供了独立的密钥生成机制。这样可以增强通信的安全性,使得客户端和服务端之间的加密密钥不会直接泄露或暴露给对方。

[0176] 可以理解地,基于跨协议节点,将服务端密钥交换参数与客户端密钥交换参数自动的转换为对方协议对应的转换后的服务端密钥交换参数和转换后的客户端密钥交换参数,服务端和客户端收到对方的转换后参数密钥后建立密钥参数交换连接,服务端和客户端交换密钥参数。并且生成用于后续通信的服务端算法密钥和客户端算法密钥,同时基于跨协议节点生成对应的节点算法密钥。

[0177] 步骤S80,通过所述跨协议节点,基于所述客户端算法密钥与所述客户端节点算法密钥,与服务端之间进行跨协议通信。

[0178] 具体地,在后续服务端与客户端通信时,通过三方的算法密钥对通信消息进行相应的处理,从而建立客户端和所述服务端的加密通信连接。

[0179] 步骤S81,获取原始客户端通信信息;

[0180] 步骤S82,根据所述客户端算法密钥,对所述原始客户端通信信息进行加密,得到加密后的客户端通信信息;

[0181] 步骤S83,将所述加密后的客户端通信信息发送至所述跨协议节点,其中,所述跨协议节点用于根据所述客户端节点算法密钥,对所述加密后的客户端通信信息进行解密后加密得到节点加密后的客户端通信信息,将所述节点加密后的客户端通信信息发送至所述服务端;

[0182] 步骤S84当接收到节点加密后的服务端通信信息时,根据所述客户端算法密钥对所述节点加密后的服务端通信信息进行解密,得到原始服务端通信信息。

[0183] 具体地,客户端可直接通过客户端算法密钥加密对应的原始客户端通信信息,得到加密后的客户端通信信息然后发送给跨协议节点;跨协议节点通过服务端节点算法密钥解密该加密后的客户端通信信息,得到节点中间信息;然后再通过服务端节点算法密钥加密节点中间信息得到节点加密后的客户端通信信息,发送给服务端;最后服务端通过服务端密钥解密相应的节点加密后的客户端通信信息,得到符合服务端的密码协议的原始客户端通信信息。

[0184] 具体地,服务端可直接通过服务端算法密钥加密对应的原始服务端通信信息,得到加密后的服务端通信信息然后发送给跨协议节点;跨协议节点通过服务端节点算法密钥解密该加密后的服务端通信信息,得到节点中间信息;然后再通过客户端节点算法密钥加

密节点中间信息得到节点加密后的服务端通信信息,发送给客户端;最后客户端通过客户端密钥解密相应的节点加密后的服务端通信信息,得到符合客户端的密码协议的原始服务器通信信息。

[0185] 可以理解地,通过三方的算法密钥对通信消息进行相应的处理,从而建立客户端和所述服务端的有效的通信,本方案能够自动化实现密码协议替换,提高不同密码协议间通信的自动化程度。

[0186] 可以理解地,本实施例提出的加密通信方法相较于现有通用技术方案有两个技术优点,一是不用修改源码,提高工作效率。本提案通过部署在网络边界上的跨协议节点(网关设备或VPN)自动化的替换密码协议,故而提高了效率;二是更加安全可靠。本提案不会修改源码,故而不会对原始密码应用造成影响,不会引入新的安全问题,并且,网关设备对原证书进行重签名,且运行在可信执行环境中,能够提供可信的服务。

[0187] 其他内容可参照上述个各实施例,在此不再赘述。

[0188] 本实施例提出的方法,通过当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,提高不同密码协议间通信的自动化程度。

[0189] 图4为本申请加密通信方法涉及的跨协议通信流程示意图1;

[0190] 图5为本申请加密通信方法涉及的跨协议通信流程示意图2。

[0191] 此外,本申请实施例还提出一种加密通信装置,所述加密通信装置包括:

[0192] 密钥参数生成模块,通过预设的跨协议节点接收到客户端发起的访问请求,得到转换后的客户端密钥交换参数,其中,所述跨协议节点用于将客户端密钥交换参数进行转换,得到所述转换后的客户端密钥交换参数并发送至所述服务端;

[0193] 参数交换发模块,用于生成服务端密钥交换参数,将所述服务端密钥交换参数发送至所述跨协议节点,其中,所述跨协议节点用于根据所述服务端密钥交换参数生成服务端节点算法密钥;

[0194] 算法密钥生成模块,用于根据所述服务端密钥交换参数与所述转换后的客户端密钥交换参数,生成服务端算法密钥;

[0195] 跨协议通信模块,用于通过所述跨协议节点,基于所述服务端算法密钥与所述服务端节点算法密钥,与客户端之间进行跨协议通信。

[0196] 本实施例实现加密通信的原理及实施过程,请参照上述各实施例,在此不再赘述。

[0197] 此外,本申请实施例还提出一种终端设备,所述终端设备包括存储器、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加密通信程序,所述加密通信程序被所述处理器执行时实现如上所述的加密通信方法的步骤。

[0198] 由于本加密通信程序被处理器执行时,采用了前述所有实施例的全部技术方案,因此至少具有前述所有实施例的全部技术方案所带来的所有有益效果,在此不再一一赘

述。

[0199] 此外,本申请实施例还提出一种计算机可读存储介质,所述计算机可读存储介质上存储有加密通信程序,所述加密通信程序被处理器执行时实现如上所述的加密通信方法的步骤。

[0200] 由于本加密通信程序被处理器执行时,采用了前述所有实施例的全部技术方案,因此至少具有前述所有实施例的全部技术方案所带来的所有有益效果,在此不再一一赘述。

[0201] 相比现有技术,本申请实施例提出的加密通信方法、装置、终端设备以及存储介质,通过当客户端向服务端发起访问请求时,基于预设的跨协议节点,建立所述客户端与所述服务端的握手连接,得到服务端密钥交换参数与客户端密钥交换参数;基于所述跨协议节点,根据所述服务端密钥交换参数与所述客户端密钥交换参数,建立所述客户端与所述服务端的密钥参数交换连接,生成服务端算法密钥、客户端算法密钥和节点算法密钥;基于所述跨协议节点,通过所述服务端算法密钥、所述客户端算法密钥和所述节点算法密钥,建立所述客户端和所述服务端的加密通信连接。当仅支持国际密码协议的设备与国密协议的设备通信时(如客户端仅支持国际协议,服务端仅支持国密协议)通信时,设置一个跨协议节点,其中所有国际密码协议的消息在经过该跨协议节点时会进行自动的转换为国密协议对应的消息,同理所有国密协议的消息在经过跨协议节点时会进行自动的转换为国际协议对应的消息,当客户端向服务端发起访问请求时,先通过跨协议节点,建立服务端与客户端的握手连接,然后获取客户端和服务端的密钥,再根据两端的密钥参数,生成服务端算法密钥、客户端算法密钥和节点算法密钥等通信密钥,基于上述通信密钥进行加密通信,上述步骤均自动化执行,无需修改代码或密码协议,,提高不同密码协议间通信的自动化程度。

[0202] 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。

[0203] 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。

[0204] 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终端设备(可以是手机,计算机,服务器,被控终端,或者网络设备等)执行本申请每个实施例的方法。

[0205] 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。

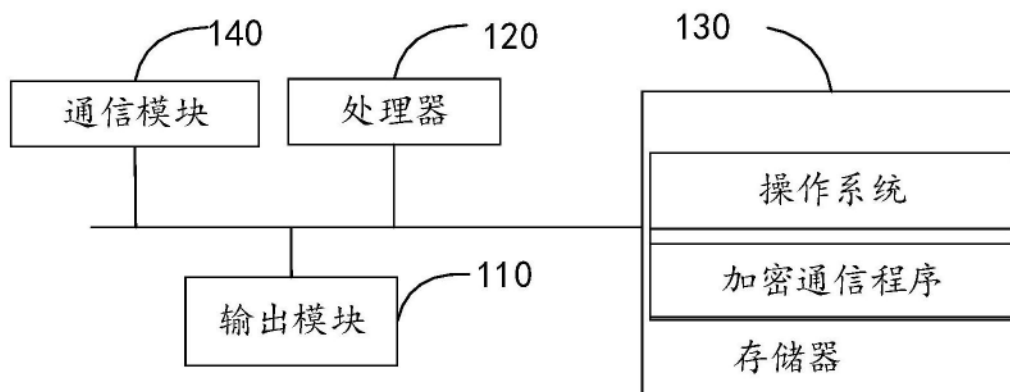


图1

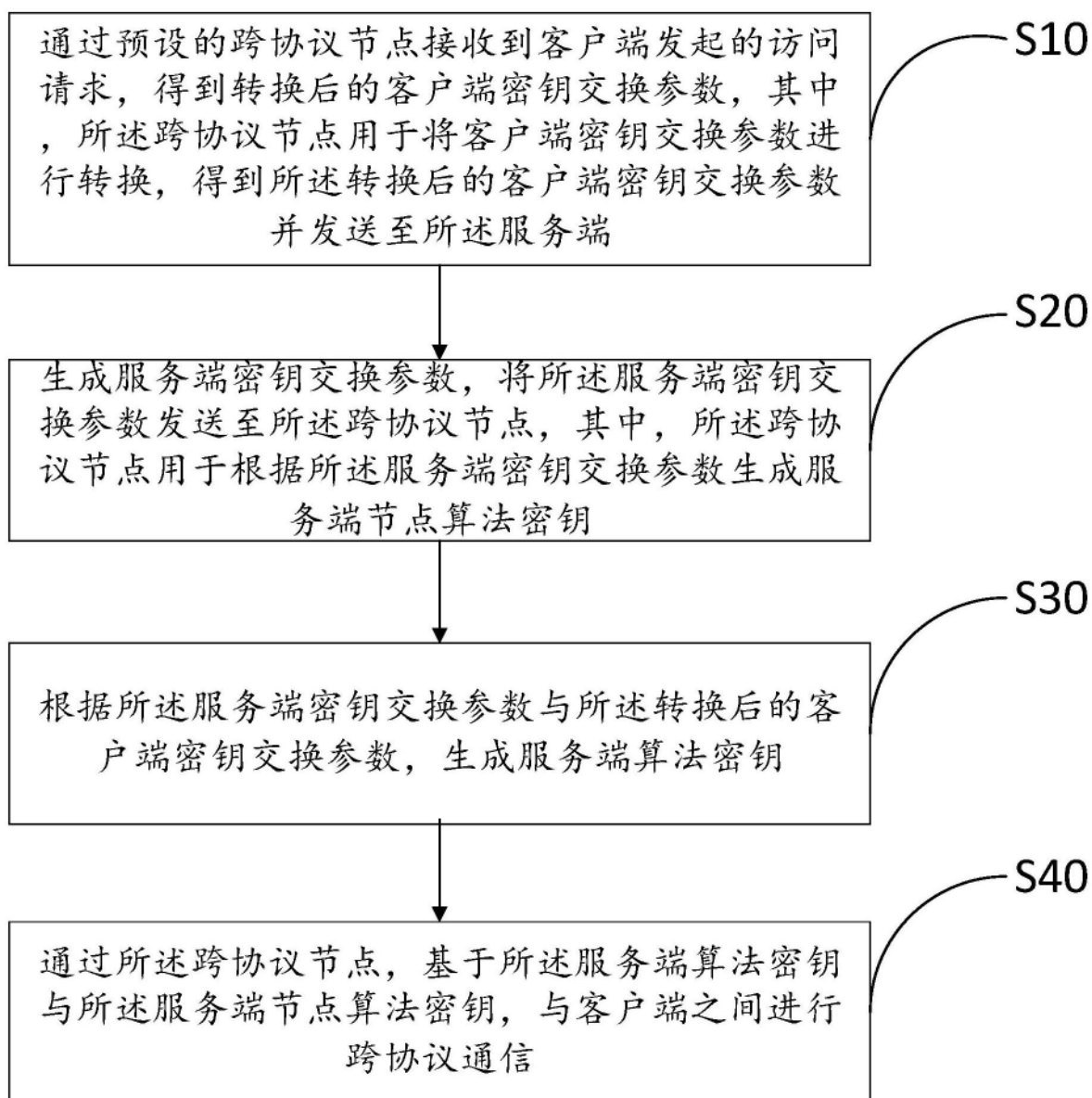


图2

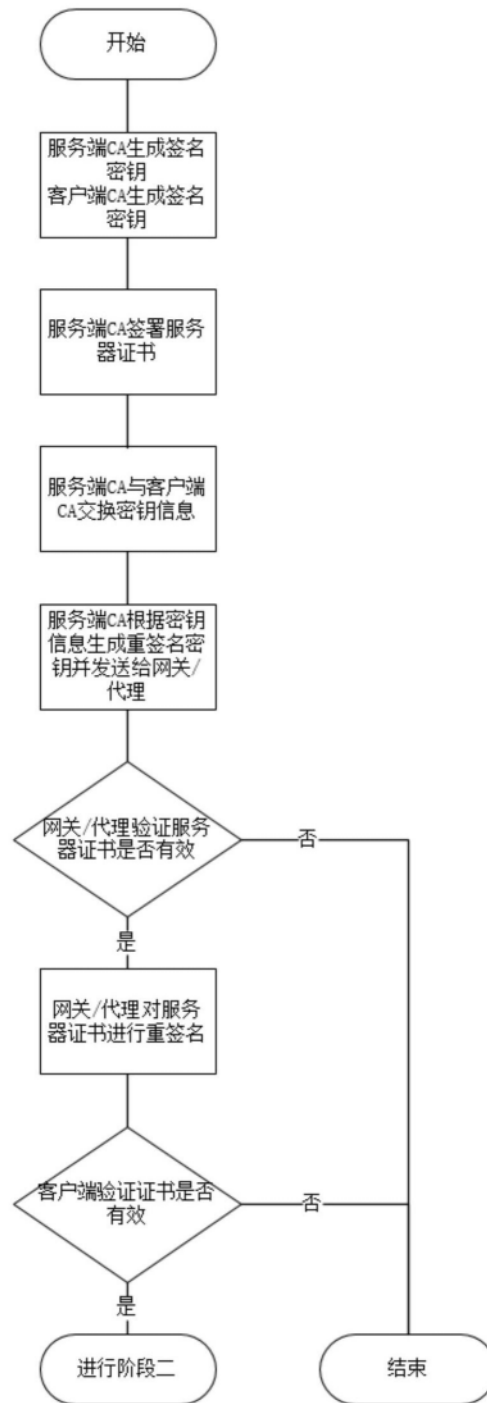


图3

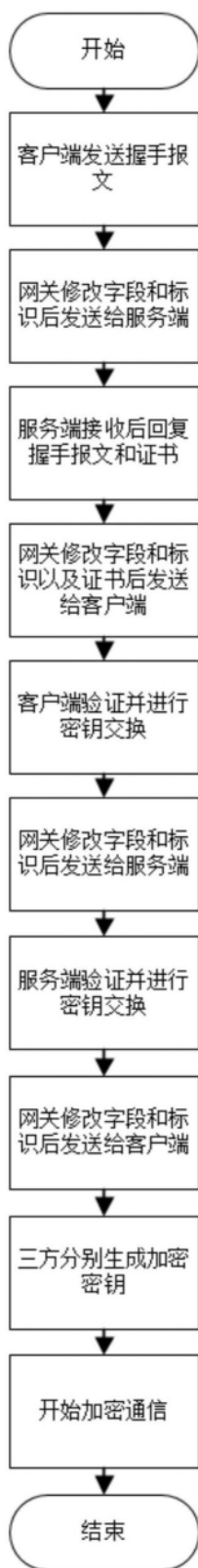


图4

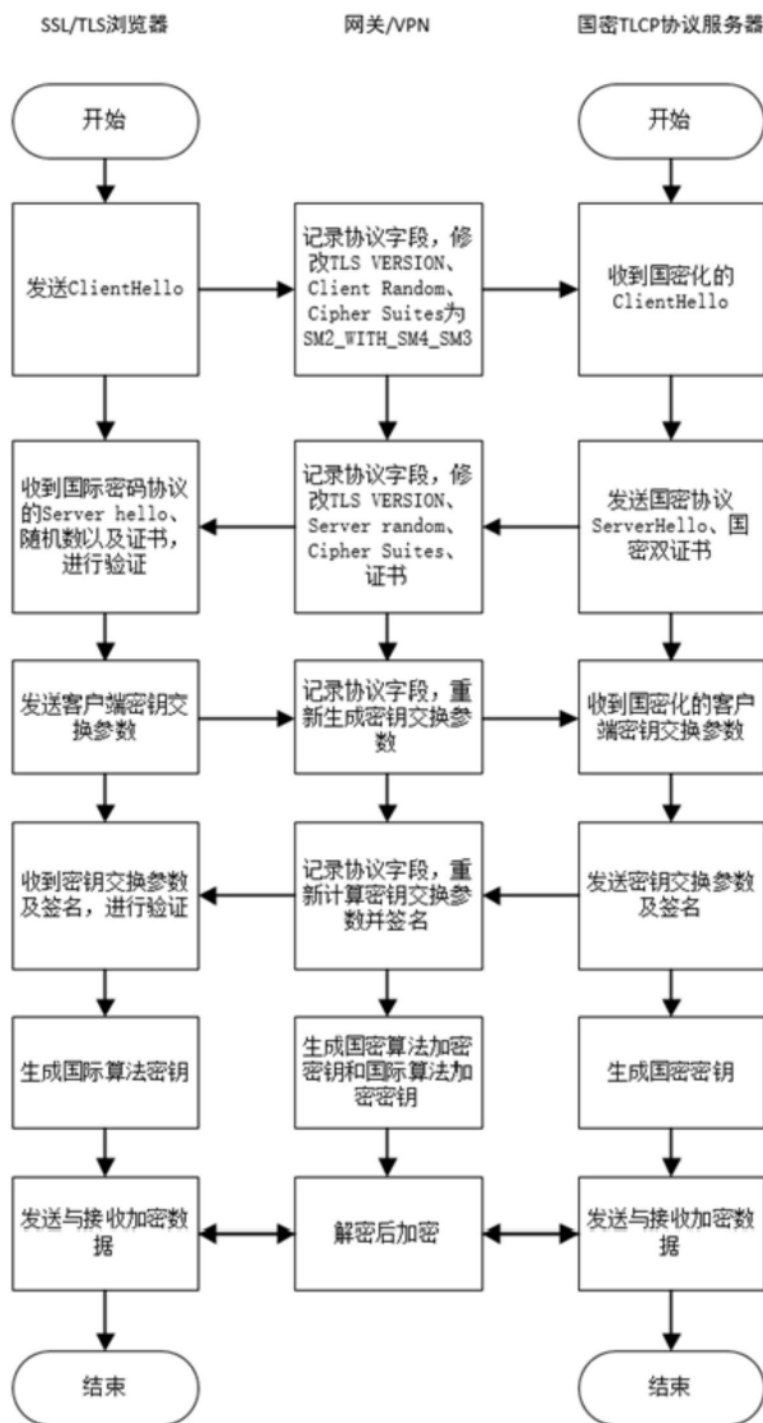


图5