

一种用于CDN节点间加密的方法、系统、装置、介质及设备

本申请要求在2017年2月8日提交中国专利局、申请号为201710069825.2、发明名称为“一种用于CDN节点间加密的方法及系统及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明实施例但不限于涉及通信领域，尤其涉及一种用于CDN节点间加密的方法、系统、装置、介质及设备。

背景技术

随着以安全为目标的HTTP通道（Hyper Text Transfer Protocol over Secure Socket Layer，HTTPS）在网络应用中的比例越来越大，迁移到HTTPS的网站数量也越来越多，对于在互联网中承担基础设施作用的内容分发网络（Content Delivery Network，简称CDN）来说，如何高效的提供全链路加密成为一个难题。CDN节点大多采用多级缓存的机制，有边缘节点，也有按照地理位置大区划分的二级节点。全链路的HTTPS是指客户端、边缘节点、二级节点、源站之间的所有环节均采用HTTPS通信。由于客户端到边缘节点以及二级节点到源站这两个环节均涉及到和第三方通信，导致优化手段有限，尤其在边缘节点和二级节点之间也需实施完整的HTTPS流程，这样对于两端参与运算的节点压力较大。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

为了解决上述技术问题，本发明实施例提供了一种用于CDN节点间加密的方法、系统、装置、介质及设备。

本发明实施例提供的用于CDN节点间加密的方法，包括：

密钥中心生成对称密钥集合和密钥索引，将所述对称密钥集合和所述密钥索引发送至各内容分发网络 CDN 节点；

CDN 节点从密钥中心接收所述对称密钥集合和所述密钥索引，根据所述密钥索引从所述对称密钥集合中确定密钥，在与其它 CDN 节点进行超文本传输协议 HTTP 数据传输时使用所述密钥进行加密和解密处理。

上述方法还具有以下特点：

所述密钥中心将所述对称密钥集合和所述密钥索引发送至各 CDN 节点包括：通过加密通道将所述对称密钥集合和所述密钥索引发送至各 CDN 节点。

上述方法还具有以下特点：

所述 CDN 节点在与其它 CDN 节点进行 HTTP 数据传输时使用所述密钥进行加密和解密处理包括：所述 CDN 节点为边缘节点时，使用所述密钥对 HTTP 请求进行加密，将加密后的 HTTP 请求向二级节点发送，在从二级节点接收到 HTTP 应答后，使用所述密钥对 HTTP 应答进行解密；和/或；所述 CDN 节点为二级节点时，在从边缘节点接收到 HTTP 请求后，使用所述密钥对 HTTP 请求进行解密，使用所述密钥对 HTTP 应答进行加密，将加密后的 HTTP 应答向边缘节点发送。

上述方法还具有以下特点：

所述密钥中心生成对称密钥集合和密钥索引，将所述对称密钥集合和所述密钥索引发送至各内容分发网络 CDN 节点包括：

所述密钥中心以第一时间间隔随机或根据预设算法生成密钥索引，向 CDN 节点发送所生成的密钥索引；所述密钥中心以第二时间间隔随机或根据预设算法生成对称密钥集合，向 CDN 节点发送所生成的对称密钥集合；所述第二时间间隔大于所述第一时间间隔；

或者，所述密钥中心以第一时间间隔随机或根据预设算法生成密钥索引，向 CDN 节点发送所生成的密钥索引；所述密钥中心以第二时间间隔随机或根据预设算法生成对称密钥集合以及随机或根据预设算法生成密钥索引，向 CDN 节点发送所生成的对称密钥集合和密钥索引；所述第二时间间隔大于所述第一时间间隔。

上述方法还具有以下特点：

所述密钥索引的范围为 $[x, y]$, x 和 y 均为整数, y 与 x 的差值加 1 为所述对称密钥集合中对称密钥的个数。

本发明实施例提供的用于 CDN 节点间加密的装置, 应用于密钥中心; 包括生成模块和发送模块;

所述生成模块, 用于生成对称密钥集合和密钥索引;

所述发送模块, 用于将所述生成模块生成的密钥集合发送至各 CDN 节点, 还用于将所述生成模块生成的密钥索引发送至各 CDN 节点。

上述装置方法还具有以下特点:

所述发送模块, 还用于通过加密通道将所述对称密钥集合和所述密钥索引发送至各 CDN 节点。

上述装置方法还具有以下特点:

所述生成模块, 还用于以第一时间间隔随机或根据预设算法生成密钥索引, 以第二时间间隔随机或根据预设算法生成对称密钥集合, 所述第二时间间隔大于所述第一时间间隔; 或者, 还用于以第一时间间隔随机或根据预设算法生成密钥索引, 以第二时间间隔随机或根据预设算法生成对称密钥集合以及随机或根据预设算法生成密钥索引, 所述第二时间间隔大于所述第一时间间隔。

本发明实施例提供的用于 CDN 节点间加密的装置, 应用于 CDN 节点; 包括接收模块和加密处理模块;

所述接收模块, 用于从密钥中心接收密钥集合, 还用于从密钥中心接收密钥索引;

所述加密处理模块, 用于根据所述密钥索引从所述对称密钥集合中确定密钥, 在与其它 CDN 节点进行 HTTP 数据传输时使用所述密钥进行加密和解密处理。

上述装置方法还具有以下特点:

所述加密处理模块, 还用于在所述 CDN 节点为边缘节点时, 使用所述密钥对 HTTP 请求进行加密, 将加密后的 HTTP 请求向二级节点发送, 在从二级节点接收到 HTTP 应答后, 使用所述密钥对 HTTP 应答进行解密; 还用于在所述 CDN 节点为二级节点时, 在从边缘节点接收到 HTTP 请求后, 使用所述密钥对 HTTP 请求进行解密, 使用所述密钥对 HTTP 应答进行加密, 将加密后的 HTTP 应答向

边缘节点发送。

本发明实施例还提供了计算机可读存储介质，所述存储介质上存储有计算机程序，所述程序被处理器执行时实现上述方法的步骤。

本发明实施例还提供了计算机设备，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计算机程序，所述处理器执行所述程序时实现上述方法的步骤。

本发明实施例跳过消耗最大的 HTTPS 握手过程，利用两端节点可控的特点，进行对称密钥的直接使用，实现轻量级的加密过程，达到同标准 HTTPS 一致的加密效果，降低了 CDN 边缘节点和二级节点之间的加密开销，减轻两端服务器的负载。本发明还采用随机生成并周期性动态更新对称密钥的机制，比传统的 HTTPS 使用证书中的公钥以及对应的私钥更加安全。

附图说明

此处所说明的附图用来提供对本发明实施例的进一步理解，构成本申请的一部分，本发明实施例的示意性实施例及其说明用于解释本发明实施例，并不构成对本发明实施例的不当限定。在附图中：

图 1 是实施例中用于 CDN 节点间加密的方法的流程图；

图 2 是实施例中应用于密钥中心的用于 CDN 节点间加密的装置的结构图；

图 3 是实施例中应用于 CDN 节点的用于 CDN 节点间加密的装置的结构图。

具体实施方式

现结合附图和具体实施方式对本发明实施例进一步说明。

图 1 是实施例中用于 CDN 节点间加密的方法的流程图；此方法包括：

步骤 101，密钥中心生成对称密钥集合和密钥索引，将此密钥集合和此密钥索引发送至各 CDN 节点；

步骤 102，CDN 节点从密钥中心接收对称密钥集合和密钥索引，根据此密钥索引从此对称密钥集合中确定密钥，在与其它 CDN 节点进行 HTTP 数据传输时使用此密钥进行加密和解密处理。

其中,

步骤 101 中对称密钥集合存储于密钥中心的内存中, 不存放于固定存储介质, 可提高密钥的安全性。

步骤 101 中, 密钥中心将密钥集合和密钥索引发送至各 CDN 节点包括: 通过加密通道将密钥集合和密钥索引发送至各 CDN 节点。

步骤 101 中, 密钥中心以第一时间间隔随机或根据预设算法生成密钥索引, 向 CDN 节点发送生成的密钥索引, 典型的发送方式为向各 CDN 节点同步发送; 密钥中心以第二时间间隔随机或根据预设算法生成对称密钥集合, 向 CDN 节点发送所生成的对称密钥集合, 典型的发送方式为向各 CDN 节点同步发送; 其中, 第二时间间隔大于第一时间间隔。或者, 密钥中心以第一时间间隔随机或根据预设算法生成密钥索引, 向 CDN 节点发送所生成的密钥索引; 密钥中心以第二时间间隔随机或根据预设算法生成对称密钥集合以及随机或根据预设算法生成密钥索引, 向 CDN 节点发送所生成的对称密钥集合和密钥索引; 第二时间间隔大于第一时间间隔。

本发明申请人考虑到边缘节点和二级节点之间这个环节中的通信双方均是 CDN 厂商可控的计算设施, 因此重点对此两种类型节点之间通信进行优化。步骤 102 中, CDN 节点在与其它 CDN 节点进行 HTTP 数据传输时使用此密钥进行加密和解密包括: CDN 节点为边缘节点时, 使用此密钥对 HTTP 请求进行加密, 将加密后的 HTTP 请求向二级节点发送, 在从二级节点接收到 HTTP 应答后, 使用此密钥对 HTTP 应答进行解密; 和/或; CDN 节点为二级节点时, 在从边缘节点接收到 HTTP 请求后, 使用此密钥对 HTTP 请求进行解密, 使用此密钥对 HTTP 应答进行加密, 将加密后的 HTTP 应答向边缘节点发送。

本方法中密钥索引的范围为 $[x, y]$, x 和 y 均为整数, y 与 x 的差值加 1 为对称密钥集合中对称密钥的个数。例如, 密钥索引的范围为 $[0, (n-1)]$, n 为对称密钥集合中对称密钥的个数; 再例如, 密钥索引的范围为 $[1, n]$, n 为对称密钥集合中对称密钥的个数。

本发明实施例中的用于 CDN 节点间加密的系统包括密钥中心和 CDN 节点。

密钥中心用于生成对称密钥集合和密钥索引, 将密钥集合和密钥索引发送至各 CDN 节点。

CDN 节点用于根据从密钥中心获取的索引从对称密钥集合中确定密钥, 在与

其它 CDN 节点进行 HTTP 数据传输时使用此密钥进行加密和解密处理。

图 2 是用于 CDN 节点间加密的装置的结构图，此装置应用于密钥中心，包括生成模块和发送模块。

生成模块用于生成对称密钥集合和密钥索引；

发送模块用于将生成模块生成的密钥集合发送至各 CDN 节点，还用于将生成模块生成的密钥索引发送至各 CDN 节点。

其中，

发送模块具体用于通过加密通道将密钥集合和密钥索引发送至各 CDN 节点。

生成模块还用于以第一时间间隔随机或根据预设算法生成密钥索引，以第二时间间隔随机或根据预设算法生成对称密钥集合，第二时间间隔大于第一时间间隔；或者，还用于以第一时间间隔随机或根据预设算法生成密钥索引，以第二时间间隔随机或根据预设算法生成对称密钥集合以及随机或根据预设算法生成密钥索引，第二时间间隔大于第一时间间隔。

图 3 是用于 CDN 节点间加密的装置的结构图，此装置应用于 CDN 节点，包括接收模块和加密处理模块。

接收模块用于从密钥中心接收密钥集合，还用于从密钥中心接收密钥索引。

加密处理模块用于根据密钥索引从对称密钥集合中确定密钥，在与其它 CDN 节点进行 HTTP 数据传输时使用此密钥进行加密和解密处理。

其中，加密处理模块还用于在 CDN 节点为边缘节点时，使用此密钥对 HTTP 请求进行加密，将加密后的 HTTP 请求向二级节点发送；在从二级节点接收到 HTTP 应答后，使用此密钥对 HTTP 应答进行解密；还用于在 CDN 节点为二级节点时，在从边缘节点接收到 HTTP 请求后，使用此密钥对 HTTP 请求进行解密，使用此密钥对 HTTP 应答进行加密，将加密后的 HTTP 应答向边缘节点发送。

本发明实施例还提供了计算机可读存储介质，存储介质上存储有计算机程序，程序被处理器执行时实现上述方法的步骤。

本发明实施例还提供了种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时实现上述方法的步骤。

具体实施例

步骤 1)， 密钥中心随机生成对称密钥集合 K，此对称密钥集合中包含若

千个对称密钥。

步骤 2)，对称密钥中心使用加密通道将对称密钥集合 K 同步发送到所有的边缘节点和二级节点上。

步骤 3)，对称密钥中心随机生成对称密钥索引 I ，索引范围 $[0, (n-1)]$ ， n 为密钥集合 K 中对称密钥的数量。

步骤 4)，对称密钥中心使用加密通道将对称密钥索引 I 同步发送到所有的边缘节点和二级节点上。

步骤 5)，边缘节点向二级节点发送 HTTP 请求时，使用 $K[I]$ 作为密钥，对 HTTP 请求进行加密。

步骤 6)，二级节点收到加密的 HTTP 请求时，同样使用 $K[I]$ 作为密钥对数据进行解密，得到 HTTP 请求原文。

步骤 7)，二级节点向边缘节点发送 HTTP 应答时，使用 $K[I]$ 作为密钥对 HTTP 应答进行加密。

步骤 8)，边缘节点收到加密的 HTTP 应答时，同样使用 $K[I]$ 作为密钥对数据进行解密，得到 HTTP 应答原文。

步骤 9)，对称密钥中心每隔时间间隔 $T1$ ，重新执行步骤 3) 和 4)，生成新的密钥索引 I 并同步发送给所有的边缘节点和二级节点。

步骤 10)，对称密钥中心每隔时间间隔 $T2$ ($T2 > T1$)，重新执行步骤 1)、2)，生成新的密钥集合 K 并同步发送给所有的边缘节点和二级节点。或者，对称密钥中心每隔时间间隔 $T2$ ($T2 > T1$)，重新执行步骤 1)、2)、3)、4)，生成新的密钥集合 K 和新的密钥索引 I 并同步发送给所有的边缘节点和二级节点。

本发明实施例跳过消耗最大的 HTTPS 握手过程，利用两端节点可控的特点，进行对称密钥的直接使用，实现轻量级的加密过程，达到同标准 HTTPS 一致的加密效果，降低了 CDN 边缘节点和二级节点之间的加密开销，减轻两端服务器的负载。本发明实施例还采用随机生成并周期性动态更新对称密钥的机制，比传统的 HTTPS 使用证书中的公钥以及对应的私钥更加安全。

本领域的普通技术人员应当理解，可以对本发明实施例的技术方案进行修改或者等同替换，而不脱离本发明实施例技术方案的精神和范围，均应涵盖在权利要求范围当中。

本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器，如数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质（或非暂时性介质）和通信介质（或暂时性介质）。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息（诸如计算机可读指令、数据结构、程序模块或其他数据）的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘（DVD）或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

工业实用性

在本发明实施例中跳过消耗最大的 HTTPS 握手过程，利用两端节点可控的特点，进行对称密钥的直接使用，实现轻量级的加密过程，达到同标准 HTTPS 一致的加密效果，降低了 CDN 边缘节点和二级节点之间的加密开销，减轻两端服务器的负载。