(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116743372 A
(43)申请公布日 2023.09.12

(21)申请号 202310897927.9

(22)申请日 2023.07.20

(71)申请人 上海循态量子科技有限公司
地址 200241 上海市闵行区东川路555号丙楼1139室

(72)发明人 周颖明 黄镇涛 方昊

(74)专利代理机构 上海段和段律师事务所 31334
专利代理师 李佳俊

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 69/04(2022.01)

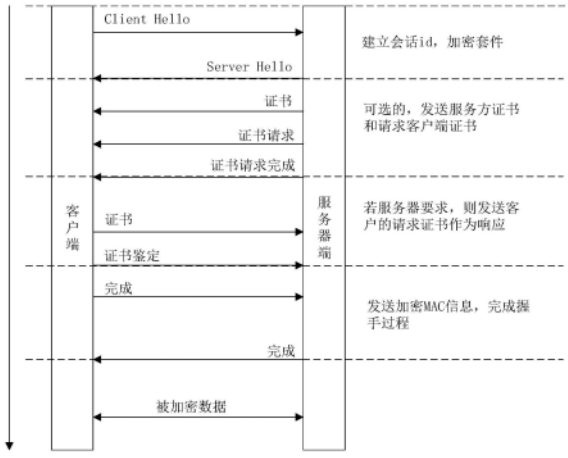
权利要求书3页 说明书7页 附图2页

(54)发明名称

基于SSL协议的量子安全协议实现方法及系统

(57)摘要

本发明提供了一种基于SSL协议的量子安全协议实现方法及系统,涉及量子保密通信技术领域,包括:步骤A:通过握手协议将客户端和服务器之间建立连接,由客户端对服务器进行鉴别,随后服务器对客户端进行鉴别,完成握手协议;步骤B:通过记录层协议将查询请求或者数据中心回传的明文数据切分为数据段,并对数据段进行压缩,对压缩后的数据段进行加密,并添加记录信息,客户端接收到加密信息后,进行解密。本发明能够实现量子密钥分发技术与网络安全协议的融合,防止业务数据泄密和检验数据防篡改,强化了信息传输的安全性。



CN 116743372 A

1.一种基于SSL协议的量子安全协议实现方法,其特征在于,包括:

步骤A:通过握手协议将客户端和服务器之间建立连接,由客户端对服务器进行鉴别,随后服务器对客户端进行鉴别,完成握手协议;

步骤B:通过记录层协议将查询请求或者数据中心回传的明文数据切分为数据段,并对数据段进行压缩,对压缩后的数据段进行加密,并添加记录信息,客户端接收到加密信息后,进行解密;

其中,握手协议和记录层协议相互依赖,在建立SSL连接时,握手协议首先进行,通过身份验证、算法协商在内的相关步骤来确保通信双方的安全性;握手协议的成功完成会导致生成量子密钥帧头和其他安全参数,这些参数将用于记录层协议的数据加密和完整性保护,一旦握手成功,记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

2.根据权利要求1所述的基于SSL协议的量子安全协议实现方法,其特征在于,所述步骤A包括:

步骤A1:包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分;由客户端先发起,告知服务器可支持的加密算法组合、加密套件列表以及会话ID,服务器从客户端传来的加密套件列表中选择加密算法和压缩算法,并连同会话ID一起回传;

步骤A2:服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文;

步骤A3:如果服务器要求客户端证书,则执行此阶段,客户端首先验证服务器是否提供合法证书,若满足条件,则向服务器发送客户端证书报文、证书鉴定报文;

步骤A4:完成握手协议,客户端发送完成信息,使用量子密钥计算明文数据的MAC值,并用协商好的加密算法对MAC值和Finished字符段进行加密,传输给服务器,服务器解密完成识别出Finished字符段后计算MAC值,若MAC值相同,则返回完成信息,若不同则立即终止会话。

3.根据权利要求2所述的基于SSL协议的量子安全协议实现方法,其特征在于,MAC算法为:根据明文数据和量子密钥计算出MAC值,然后将计算出的MAC值和明文数据再用量子密钥对称加密,得到最终密文。

4.根据权利要求2所述的基于SSL协议的量子安全协议实现方法,其特征在于,所述步骤B包括:

步骤B1:将明文数据切分为数据段;

步骤B2:通过步骤A中选择的压缩算法对数据段进行压缩,压缩后的数据段称为压缩单元,若没有选择压缩算法,默认不进行压缩;

步骤B3:利用握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC值,然后使用量子密钥对压缩单元和MAC值进行加密,加密后的压缩单元和MAC值称为加密单元;

步骤B4:在加密单元添加记录信息,所述记录信息包括高层协议信息、协议版本、压缩长度信息;

步骤B5:传输数据到客户端,客户端接收到加密信息后,进行解密。

5.根据权利要求4所述的基于SSL协议的量子安全协议实现方法，其特征在于，切分的数据块长度为16K字节。

6.根据权利要求4所述的基于SSL协议的量子安全协议实现方法，其特征在于，压缩后的压缩单元长度不超过1024字节。

7.一种基于SSL协议的量子安全协议实现系统，其特征在于，包括：

模块A：通过握手协议将客户端和服务器之间建立连接，由客户端对服务器进行鉴别，随后服务器对客户端进行鉴别，完成握手协议；

模块B：通过记录层协议将查询请求或者数据中心回传的明文数据切分为数据段，并对数据段进行压缩，对压缩后的数据段进行加密，并添加记录信息，客户端接收到加密信息后，进行解密；

其中，握手协议和记录层协议相互依赖，在建立SSL连接时，握手协议首先进行，通过身份验证、算法协商在内的相关步骤来确保通信双方的安全性；握手协议的成功完成会导致生成量子密钥帧头和其他安全参数，这些参数将用于记录层协议的数据加密和完整性保护，一旦握手成功，记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

8.根据权利要求7所述的基于SSL协议的量子安全协议实现系统，其特征在于，所述模块A包括：

模块A1：包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分；由客户端先发起，告知服务器可支持的加密算法组合、加密套件列表以及会话ID，服务器从客户端传来的加密套件列表中选择加密算法和压缩算法，并连同会话ID一起回传；

模块A2：服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文；

模块A3：如果服务器要求客户端证书，则执行此阶段，客户端首先验证服务器是否提供合法证书，若满足条件，则向服务器发送客户端证书报文、证书鉴定报文；

模块A4：完成握手协议，客户端发送完成信息，使用量子密钥计算明文数据的MAC值，并用协商好的加密算法对MAC值和Finished字符段进行加密，传输给服务器，服务器解密完成识别出Finished字符段后计算MAC值，若MAC值相同，则返回完成信息，若不同则立即终止会话；

MAC算法为：根据明文数据和量子密钥计算出MAC值，然后将计算出的MAC值和明文数据再用量子密钥对称加密，得到最终密文；

所述模块B包括：

模块B1：将明文数据切分为数据段，切分的数据块长度为16K字节；

模块B2：通过模块A中选择的压缩算法对数据段进行压缩，压缩后的数据段称为压缩单元，若没有选择压缩算法，默认不进行压缩；压缩后的压缩单元长度不超过1024字节；

模块B3：利用握手协议协商的量子密钥帧头信息提取相应的量子密钥，并计算量子密钥和压缩单元的MAC值，然后使用量子密钥对压缩单元和MAC值进行加密，加密后的压缩单元和MAC值称为加密单元；

模块B4：在加密单元添加记录信息，所述记录信息包括高层协议信息、协议版本、压缩

长度信息；

模块B5：传输数据到客户端，客户端接收到加密信息后，进行解密。

9.一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的基于SSL协议的量子安全协议实现方法的步骤。

10.一种电子设备，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，其特征在于，所述计算机程序被处理器执行时实现权利要求1至6中任一项所述的基于SSL协议的量子安全协议实现方法的步骤。

基于SSL协议的量子安全协议实现方法及系统

技术领域

[0001] 本发明涉及量子保密通信技术领域,具体地,涉及一种基于SSL协议的量子安全协议实现方法及系统。

背景技术

[0002] 进入二十一世纪之后,量子计算机快速发展,将对现有的主流公钥体系产生巨大的威胁,主流的公钥算法,如基于大数分解的RSA算法将被量子计算机轻易破解,而目前的浏览器安全协议SSL中使用非对称加密的方式进行加密,浏览器的加密方式已经越来越难以满足安全性的需求。

[0003] 量子保密通信被认为是能够确保信息安全的重要手段之一,而量子密钥分发(QKD)是量子保密通信中最快走向工程实用化的技术,是量子通信中的重要方向。QKD基于量子物理学的基本特性而不是计算的复杂性,可以在空间分离的用户之间通过量子信道以绝对安全的方式共享密钥QKD技术并不直接传送信息,而是进行密钥的分配,在密钥协商之后通信双方可以得到相同的量子密钥,然后用量子密钥对明文进行加密后,将密文通过经典信道传输。

发明内容

[0004] 针对现有技术中的缺陷,本发明提供一种基于SSL协议的量子安全协议实现方法及系统。

[0005] 根据本发明提供的一种基于SSL协议的量子安全协议实现方法及系统,所述方案如下:

[0006] 第一方面,提供了一种基于SSL协议的量子安全协议实现方法,所述方法包括:

[0007] 步骤A:通过握手协议将客户端和服务器之间建立连接,由客户端对服务器进行鉴别,随后服务器对客户端进行鉴别,完成握手协议;

[0008] 步骤B:通过记录层协议将查询请求或者数据中心回传的明文数据切分为数据段,并对数据段进行压缩,对压缩后的数据段进行加密,并添加记录信息,客户端接收到加密信息后,进行解密;

[0009] 其中,握手协议和记录层协议相互依赖,在建立SSL连接时,握手协议首先进行,通过身份验证、算法协商在内的相关步骤来确保通信双方的安全性;握手协议的成功完成会导致生成量子密钥帧头和其他安全参数,这些参数将用于记录层协议的数据加密和完整性保护,一旦握手成功,记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

[0010] 优选地,所述步骤A包括:

[0011] 步骤A1:包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分;由客户端先发起,告知服务器可支持的加密算法组合、加密套件列表以及会话ID,服务器从客户端传来的加密套件列表中选择加密算法和压缩算法,并连同会话ID一起

回传；

[0012] 步骤A2:服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文；

[0013] 步骤A3:如果服务器要求客户端证书,则执行此阶段,客户端首先验证服务器是否提供合法证书,若满足条件,则向服务器发送客户端证书报文、证书鉴定报文；

[0014] 步骤A4:完成握手协议,客户端发送完成信息,使用量子密钥计算明文数据的MAC值,并用协商好的加密算法对MAC值和Finished字符段进行加密,传输给服务器,服务器解密完成识别出Finished字符段后计算MAC值,若MAC值相同,则返回完成信息,若不同则立即终止会话。

[0015] 优选地,MAC算法为:根据明文数据和量子密钥计算出MAC值,然后将计算出的MAC值和明文数据再用量子密钥对称加密,得到最终密文。

[0016] 优选地,所述步骤B包括：

[0017] 步骤B1:将明文数据切分为数据段；

[0018] 步骤B2:通过步骤A中选择的压缩算法对数据段进行压缩,压缩后的数据段称为压缩单元,若没有选择压缩算法,默认不进行压缩；

[0019] 步骤B3:利用握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC值,然后使用量子密钥对压缩单元和MAC值进行加密,加密后的压缩单元和MAC值称为加密单元；

[0020] 步骤B4:在加密单元添加记录信息,所述记录信息包括高层协议信息、协议版本、压缩长度信息；

[0021] 步骤B5:传输数据到客户端,客户端接收到加密信息后,进行解密。

[0022] 优选地,切分的数据块长度为16K字节。

[0023] 优选地,压缩后的压缩单元长度不超过1024字节。

[0024] 第二方面,提供了一种基于SSL协议的量子安全协议实现系统,所述系统包括：

[0025] 模块A:通过握手协议将客户端和服务器之间建立连接,由客户端对服务器进行鉴别,随后服务器对客户端进行鉴别,完成握手协议；

[0026] 模块B:通过记录层协议将查询请求或者数据中心回传的明文数据切分为数据段,并对数据段进行压缩,对压缩后的数据段进行加密,并添加记录信息,客户端接收到加密信息后,进行解密；

[0027] 其中,握手协议和记录层协议相互依赖,在建立SSL连接时,握手协议首先进行,通过身份验证、算法协商在内的相关步骤来确保通信双方的安全性;握手协议的成功完成会导致生成量子密钥帧头和其他安全参数,这些参数将用于记录层协议的数据加密和完整性保护,一旦握手成功,记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

[0028] 优选地,所述模块A包括：

[0029] 模块A1:包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分;由客户端先发起,告知服务器可支持的加密算法组合、加密套件列表以及会话ID,服务器从客户端传来的加密套件列表中选择加密算法和压缩算法,并连同会话ID一起回传；

[0030] 模块A2:服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文;

[0031] 模块A3:如果服务器要求客户端证书,则执行此阶段,客户端首先验证服务器是否提供合法证书,若满足条件,则向服务器发送客户端证书报文、证书鉴定报文;

[0032] 模块A4:完成握手协议,客户端发送完成信息,使用量子密钥计算明文数据的MAC值,并用协商好的加密算法对MAC值和Finished字符段进行加密,传输给服务器,服务器解密完成识别出Finished字符段后计算MAC值,若MAC值相同,则返回完成信息,若不同则立即终止会话;

[0033] MAC算法为:根据明文数据和量子密钥计算出MAC值,然后将计算出的MAC值和明文数据再用量子密钥对称加密,得到最终密文;

[0034] 所述模块B包括:

[0035] 模块B1:将明文数据切分为数据段,切分的数据块长度为16K字节;

[0036] 模块B2:通过模块A中选择的压缩算法对数据段进行压缩,压缩后的数据段称为压缩单元,若没有选择压缩算法,默认不进行压缩;压缩后的压缩单元长度不超过1024字节;

[0037] 模块B3:利用握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC值,然后使用量子密钥对压缩单元和MAC值进行加密,加密后的压缩单元和MAC值称为加密单元;

[0038] 模块B4:在加密单元添加记录信息,所述记录信息包括高层协议信息、协议版本、压缩长度信息;

[0039] 模块B5:传输数据到客户端,客户端接收到加密信息后,进行解密。

[0040] 第三方面,提供了一种存储有计算机程序的计算机可读存储介质,所述计算机程序被处理器执行时实现所述基于SSL协议的量子安全协议实现方法中的步骤。

[0041] 第四方面,提供了一种电子设备,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,所述计算机程序被处理器执行时实现所述基于SSL协议的量子安全协议实现方法中的步骤。

[0042] 与现有技术相比,本发明具有如下的有益效果:

[0043] 1、本发明能够实现量子密钥分发技术与网络安全协议的融合,防止业务数据泄密和检验数据防篡改,强化了信息传输的安全性;

[0044] 2、本发明所述的量子安全协议可以与传统的对称加密算法兼容,无需对现有系统进行过多改动;

[0045] 3、本发明所述的基于SSL协议的量子安全协议使用量子密钥分发的密钥代替非对称加密算法,可以抵御量子计算机的攻击,具有无条件的安全性。

[0046] 本发明的其他有益效果,将在具体实施方式中通过具体技术特征和技术方案的介绍来阐述,本领域技术人员通过这些技术特征和技术方案的介绍,应能理解所述技术特征和技术方案带来的有益技术效果。

附图说明

[0047] 通过阅读参照以下附图对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

[0048] 图1为基于SSL协议的量子安全协议的握手协议；

[0049] 图2为基于SSL协议的量子安全协议的记录层协议。

具体实施方式

[0050] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明，但不以任何形式限制本发明。应当指出的是，对本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0051] 本发明实施例提供了一种基于SSL协议的量子安全协议实现方法，参照图1所示，该方法具体包括：

[0052] 步骤A：通过握手协议将客户端和服务器之间建立连接，由客户端对服务器进行鉴别，随后服务器对客户端进行鉴别，完成握手协议；

[0053] 步骤B：通过记录层协议将明文数据切分为数据段并进行压缩，对压缩后的数据段进行加密，并添加记录信息，客户端接收到加密信息后，进行解密。

[0054] 其中，握手协议和记录层协议是相互依赖的，在建立SSL连接时，握手协议首先进行，通过身份验证、算法协商等步骤来确保通信双方的安全性。握手协议的成功完成会导致生成量子密钥帧头和其他安全参数，这些参数将用于记录层协议的数据加密和完整性保护。一旦握手成功，记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

[0055] 具体地，步骤A包括：

[0056] 步骤A1：包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分；由客户端先发起，告知服务器可支持的加密算法组合、压缩算法组合(也即加密套件列表)以及会话ID，服务器从客户端传来的加密套件列表中选择加密算法和压缩算法，并连同会话ID一起回传；

[0057] 步骤A2：服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文；

[0058] 步骤A3：如果服务器要求客户端证书，则执行此阶段，客户端首先验证服务器是否提供合法证书，若满足条件，则向服务器发送客户端证书报文、证书鉴定报文；

[0059] 步骤A4：完成握手协议，客户端发送完成信息，使用量子密钥计算明文数据(包括使用的加密算法、压缩算法以及量子密钥帧头信息)的MAC值，并用协商好的加密算法对MAC值和Finished字符段进行加密，传输给服务器，服务器解密完成识别出Finished字符段后计算MAC值，若MAC值相同，则返回完成信息，若不同则立即终止会话。

[0060] 其中，MAC算法为：根据明文数据和量子密钥计算出MAC值，然后将计算出的MAC值和明文数据再用量子密钥对称加密，得到最终密文。

[0061] 步骤B包括：

[0062] 步骤B1：将明文数据切分为数据段，切分的数据块长度为16K字节，这里的明文数据可以是查询请求或者数据中心回传的明文信息。

[0063] 步骤B2：通过步骤A中选择的压缩算法对数据段进行压缩，压缩后的数据段称为压缩单元，若没有选择压缩算法，默认不进行压缩；压缩后的压缩单元长度不超过1024字节。

[0064] 步骤B3:利用握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC值,然后使用量子密钥对压缩单元和MAC值进行加密,加密后的压缩单元和MAC值称为加密单元。

[0065] 步骤B4:在加密单元添加记录信息,记录信息包括高层协议信息、协议版本、压缩长度信息,封装为TCP数据包;

[0066] 步骤B5:传输数据到客户端,客户端接收到加密信息后,进行解密。

[0067] 本发明还提供一种基于SSL协议的量子安全协议实现系统,所述基于SSL协议的量子安全协议实现系统可以通过执行所述基于SSL协议的量子安全协议实现方法的流程步骤予以实现,即本领域技术人员可以将所述基于SSL协议的量子安全协议实现方法理解为所述基于SSL协议的量子安全协议实现系统的优选实施方式。该系统具体包括:

[0068] 模块A:通过握手协议将客户端和服务器之间建立连接,由客户端对服务器进行鉴别,随后服务器对客户端进行鉴别,完成握手协议;

[0069] 模块B:通过记录层协议将明文数据切分为数据段并进行压缩,对压缩后的数据段进行加密,并添加记录信息,客户端接收到加密信息后,进行解密。

[0070] 其中,握手协议和记录层协议是相互依赖的,在建立SSL连接时,握手协议首先进行,通过身份验证、算法协商等步骤来确保通信双方的安全性。握手协议的成功完成会导致生成量子密钥帧头和其他安全参数,这些参数将用于记录层协议的数据加密和完整性保护。一旦握手成功,记录层协议将使用握手阶段协商的量子密钥和算法来加密和保护上层应用数据的传输。

[0071] 具体地,模块A包括:

[0072] 模块A1:包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分;由客户端先发起,告知服务器可支持的加密算法组合、压缩算法组合(也即加密套件列表)以及会话ID,服务器从客户端传来的加密套件列表中选择加密算法和压缩算法,并连同会话ID一起回传;

[0073] 模块A2:服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文;

[0074] 模块A3:如果服务器要求客户端证书,则执行此阶段,客户端首先验证服务器是否提供合法证书,若满足条件,则向服务器发送客户端证书报文、证书鉴定报文;

[0075] 模块A4:完成握手协议,客户端发送完成信息,使用量子密钥计算,包括使用的加密算法、压缩算法以及量子密钥帧头信息的MAC值,并用协商好的加密算法对MAC值和Finished字符段进行加密,传输给服务器,服务器解密完成识别出Finished字符段后计算MAC值,若MAC值相同,则返回完成信息,若不同则立即终止会话。

[0076] 其中,MAC算法为:根据明文数据和量子密钥计算出MAC值,然后将计算出的MAC值和明文数据再用量子密钥对称加密,得到最终密文。

[0077] 模块B包括:

[0078] 模块B1:将明文数据切分为数据段,切分的数据块长度为16K字节,这里的明文数据可以是查询请求或者数据中心回传的明文信息。

[0079] 模块B2:通过模块A中选择的压缩算法对数据段进行压缩,压缩后的数据段称为压缩单元,若没有选择压缩算法,默认不进行压缩;压缩后的压缩单元长度不超过1024字节。

[0080] 模块B3:利用握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC值,然后使用量子密钥对压缩单元和MAC值进行加密,加密后的压缩单元和MAC值称为加密单元。

[0081] 模块B4:在加密单元添加记录信息,记录信息包括高层协议信息、协议版本、压缩长度信息,封装为TCP数据包;

[0082] 模块B5:传输数据到客户端,客户端接收到加密信息后,进行解密。

[0083] 接下来,对本发明进行更为具体的说明。

[0084] 本发明提供的一种基于SSL协议的量子安全协议实现方法,该方法包括握手协议与记录层协议,具体如下:

[0085] 握手协议:客户端和服务器之间建立连接,然后客户端对服务器进行鉴别,随后服务器对客户端进行鉴别、最后完成握手协议。

[0086] 参照图1所示,握手协议步骤包括:

[0087] 步骤A1:包括客户端向服务器发送Client Hello报文和服务器回传Server Hello报文两部分,由客户端先发起,告知服务器可支持的加密算法组合、压缩算法组合(也即加密套件列表)以及会话ID,服务器从客户端传来的加密套件列表中选择加密算法和压缩算法,并连同会话ID一起回传。

[0088] 步骤A2:服务器向客户端发送证书报文、客户端证书请求报文、以及证书请求完成报文。

[0089] 步骤A3:如果服务器要求客户端证书,则执行此阶段,客户端首先验证服务器是否提供合法证书,若满足条件,则向服务器发送客户端证书报文、证书鉴定报文。

[0090] 步骤A4:最后一个阶段完成握手协议,客户端发送完成信息,使用量子密钥计算,包括使用的加密算法、压缩算法以及量子密钥帧头信息的MAC值,并用协商好的加密算法对MAC值和数据信息进行加密,传输给服务器,服务器解密完成后计算MAC值,若MAC值相同,则返回完成信息,若不同则立即终止会话。

[0091] MAC算法为MtE(MAC-then-Encrypt):首先根据明文和量子密钥计算出MAC值,然后将计算出的MAC值和明文再用量子密钥对称加密,得到最终密文。

[0092] 参照图2所示,记录层协议将用户层数据切分为数据段,然后使用握手协议中定义的压缩算法进行压缩,计算所需使用的量子密钥和压缩单元的MAC(消息验证码)并对整个单元进行加密,最后在加密单元添加记录信息,传输数据到客户端,客户端接收到加密信息后,进行解密。

[0093] 记录层协议包括:应用层数据、记录协议单元、压缩单元、加密单元以及TCP数据包;

[0094] 其中,应用层数据指来自应用程序的原始信息,是在协议中需要进行加密、传输和保护的实际数据,也即明文数据。

[0095] 记录协议单元是协议中的基本数据单位,由类型(Type)、版本(Version)、长度(Length)、内容(Content)组成,发送方将应用层数据封装成记录协议单元,并使用握手协议中协商的加密算法对数据进行加密。接收方在接收到记录协议单元后,根据记录的类型和加密算法进行解密和处理,以获取原始的应用层数据。

[0096] 压缩单元是指在记录层协议中对应用层数据进行压缩后的数据单元。在记录层

中,可以使用握手协议中协商的压缩算法对应用层数据进行压缩,以减少传输的数据量。

[0097] 加密单元是指对压缩单元和MAC值进行加密后的数据单元。在记录层中,使用握手协议中协商的加密算法对压缩单元和MAC值进行加密,以确保数据在传输过程中的机密性和安全性。

[0098] TCP数据包是是承载着记录层数据的基本传输单位,包括加密单元、高层协议信息、协议版本、压缩长度信息,负责在网络中将记录层数据从一个端点传输到另一个端点。

[0099] 具体实现流程如下:

[0100] 步骤B1:将明文数据切分为记录协议单元,切分的单元长度为16K字节,这里的明文数据可以是查询请求或者数据中心回传的明文信息。16K是经典SSL协议中的默认设置,可根据具体的实现和配置进行调整。

[0101] 步骤B2:数据段被握手协议中定义的压缩算法进行压缩,若没有选择压缩算法,默认不进行压缩。为平衡数据传输效率与安全性,并减小潜在的安全漏洞,压缩后的压缩单元长度不超过1024字节。

[0102] 步骤B3:利用权利握手协议协商的量子密钥帧头信息提取相应的量子密钥,并计算量子密钥和压缩单元的MAC(消息验证码)值,利用量子密钥加密MAC值和压缩单元形成加密单元,此处MAC是消息和密钥的函数MAC=C(K,M),M为输入信息,K为共享的密钥,C为MAC函数,在握手过程中决定。

[0103] 步骤B4:在加密单元添加记录信息,包括高层协议信息、协议版本、压缩长度信息,封装为TCP数据包。

[0104] 步骤B5:传输TCP数据包到客户端,客户端接收到TCP数据包后,进行解密。解密过程为加密过程的逆过程。

[0105] 本发明实施例提供了一种基于SSL协议的量子安全协议实现方法及系统,实现量子密钥分发技术与网络安全协议的融合,防止业务数据泄密和检验数据防篡改,强化了信息传输的安全性。

[0106] 本领域技术人员知道,除了以纯计算机可读程序代码方式实现本发明提供的系统及其各个装置、模块、单元以外,完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系统及其各个装置、模块、单元以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同功能。所以,本发明提供的系统及其各项装置、模块、单元可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置、模块、单元也可以视为硬件部件内的结构;也可以将用于实现各种功能的装置、模块、单元视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0107] 以上对本发明的具体实施例进行了描述。需要理解的是,本发明并不局限于上述特定实施方式,本领域技术人员可以在权利要求的范围内做出各种变化或修改,这并不影响本发明的实质内容。在不冲突的情况下,本申请的实施例和实施例中的特征可以任意相互组合。

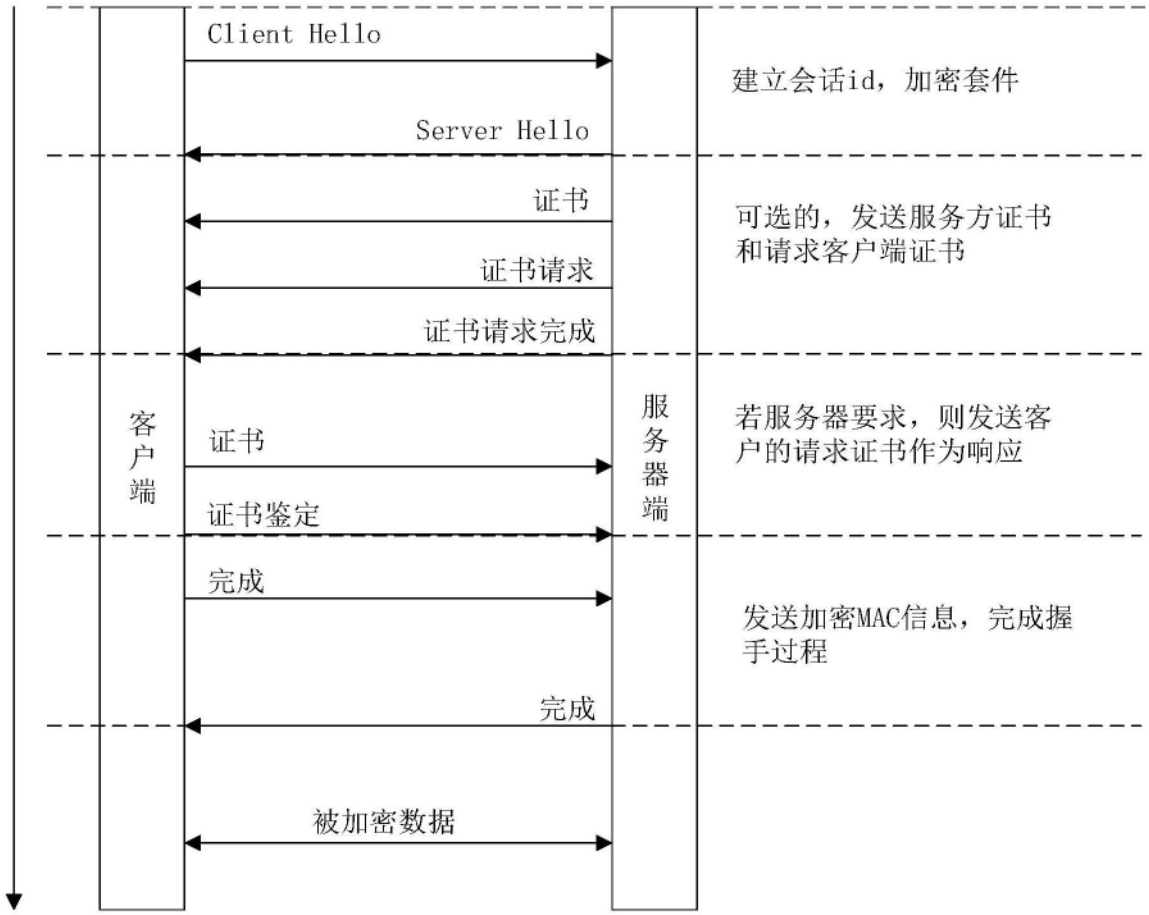

Client Hello
建立会话id，加密套件
Server Hello
证书
可选的，发送服务方证书
和请求客户端证书
证书请求
证书请求完成
客户端
服务器端
证书
若服务器要求，则发送客
户的请求证书作为响应
证书鉴定
完成
发送加密MAC信息，完成握
手过程
完成
被加密数据

图1

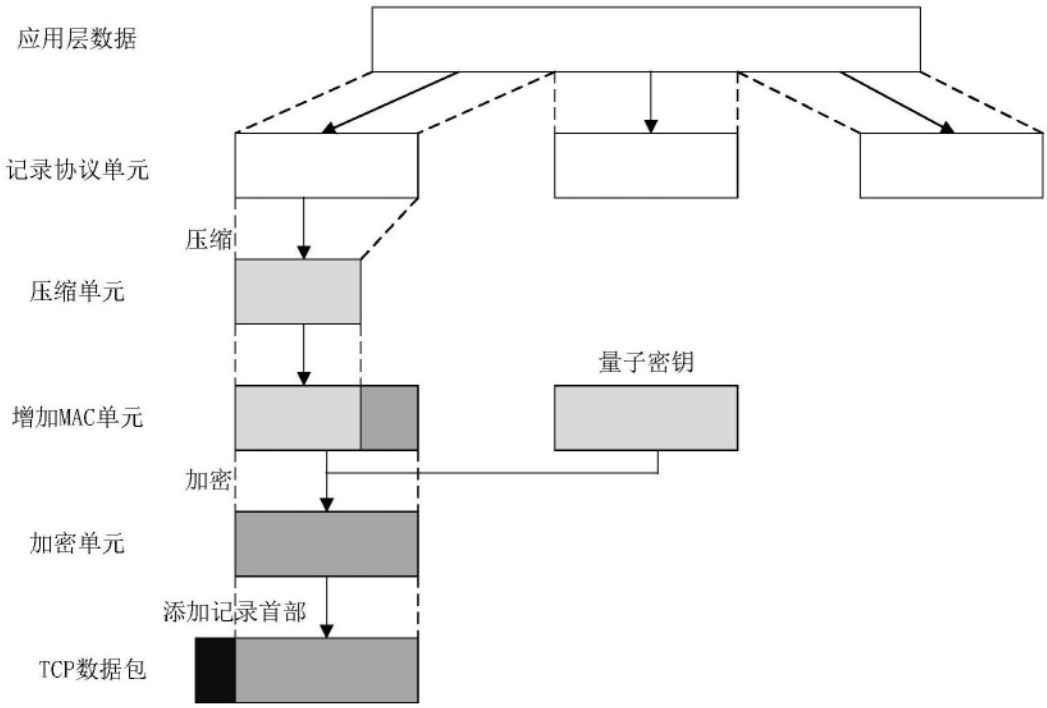


图2