(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111447276 A
(43)申请公布日 2020.07.24

(21)申请号 202010227436.X

(22)申请日 2020.03.27

(71)申请人 东南大学
地址 210096 江苏省南京市玄武区四牌楼2号

(72)发明人 蒋睿 郭学心 蒋立霄

(74)专利代理机构 南京众联专利代理有限公司 32206
代理人 蒋昱

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

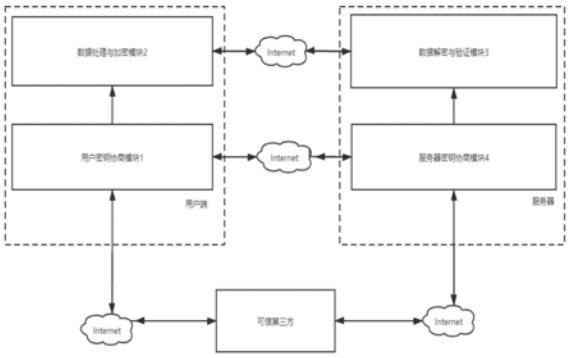
权利要求书3页 说明书11页 附图6页

(54)发明名称

一种具有密钥协商功能的加密续传方法

(57)摘要

本发明公开了一种具有密钥协商功能的加密续传方法，包括用户密钥协商模块、数据处理与加密模块、数据解密与验证模块和服务器密钥协商模块。用户密钥协商模块通过与服务器密钥协商模块进行协议交互，产生会话密钥；数据处理与加密模块实现数据的分组与分组后数据的加密；数据解密与验证模块实现数据的解密、数据的整合、以及数据的完整性验证。本发明可为不同大小的数据，通过不安全的Internet网络，提供一种安全、可续传的通信方法。



CN 111447276 A

1.一种具有密钥协商功能的加密续传方法,所述具有密钥协商功能的加密续传方法配套系统包括用户密钥协商模块(1)、数据处理与加密模块(2)、数据解密与验证模块(3)和服务器密钥协商模块(4);其特征在于,具体步骤如下;

首先用户密钥协商模块(1)负责生成挑战信息,并与服务器密钥协商模块(4)进行协议交互,通过自行设计的会话交互协议,产生一组会话密钥,用于加密分组后的通信数据;服务器密钥协商模块(4)生成应答消息,完成与用户密钥协商模块(1)的协议交互,并最终产生一组会话密钥,用于密文的解密;

然后数据处理与加密模块(2)负责对即将传输的数据基于遗传算法进行分组标记,并对标记后的分组数据进行加密与完整性保护;最后数据解密与验证模块(3)对接收到的所有密文进行解密,并对每组解密明文进行完整性验证;

最后将所有解密明文进行组合,再一次进行完整性验证。

2.根据权利要求1所述的一种具有密钥协商功能的加密续传方法,其特征在于:所述的用户密钥协商模块(1)包括协商挑战生成模块(1-1)和用户组密钥计算模块(1-2);负责在认证基础上,发起协商挑战与接收应答,产生一组会话密钥,并且在密钥协商过程中抵抗中间人攻击;

所述的协商挑战生成模块(1-1)首先保存当前通信实体向可信第三方申请的公钥证书$Cert_A$和私钥SK_A,同时生成私有随机数N_{ID_A},并且定义一个大素数p及其本原根a,公开p和a,然后随机选择一个私有的随机数X_A(X_A<p),计算当前实体参数$Y_A = a^{X_A} \bmod p$,生成包含当前实体参数Y_A的签名$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$,并采用服务器的公钥进行加密得到$C_A = E_{PK_B}(Sig(Y_A \| N_{ID_A}))$,最后将协商参数$Y_A$、$C_A$和公钥证书$Cert_A$作为密钥协商参数,发送到服务器密钥协商模块(4)中的服务器组密钥计算模块(4-2);

所述的用户组密钥计算模块(1-2)接收来自协商应答生成模块(4-1)发送的密钥协商参数,包括密文$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A}))$、参数$Y_B$、公钥证书$Cert_B$以及由协商挑战生成模块(1-1)产生的$Y_A$;使用私钥$SK_A$对$C_B$进行解密得到$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$,再采用公钥证书$Cert_B$中的公钥$PK_B$,通过签名验证恢复算法恢复出$Y_B \| N_{ID_B} \| N_{ID_A} = V_{PK_B}(Sig_B)$,将恢复出的$Y_B$、$N_{ID_A}$与接收到的$Y_B$、$N_{ID_A}$进行比对,若一致,则系统正常;否则,中止当前会话;从而验证数据来源的可靠性,接着计算得到会话密钥$K_{AB} = (Y_B)^{X_A} \bmod p$,并将会话密钥$K_{AB}$传输至数据处理与加密模块(2),同时计算$K_{AB}$的Hash值$H(K_{AB})$,结合$N_{ID_B}$使用服务器方公钥$PK_B$进行加密计算,得到$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$,将该密文发送至服务器密钥协商模块(4)。

3.根据权利要求1所述的一种具有密钥协商功能的加密续传方法,其特征在于:所述的数据处理与加密模块(2)包括基于遗传算法的续传数据预处理模块(2-1)和数据加密模块(2-2);负责对发送数据基于遗传算法进行分组分块,封装编号,采用改进的SM4算法进行加密与完整性保护,最后将加密后的分组数据发送至数据解密与验证模块(3),由于采用遗传算法及改进的SM4算法,提高了系统的处理能力与安全性;

所述的基于遗传算法的续传数据预处理模块(2-1)基于socket接口，通过TCP/IP传输协议，接收用户需要传输的明文数据M，基于遗传算法对该数据进行分类分组得到$M_1||\cdots||M_X=M$和组数num，对分组后的明文M_X进行编码，生成相应的数据标签L_x，L_1即为00000001，对应分组明文M_1，将带有数据标签的分组明文数据$M_X||L_x$，以服务请求方式传输至数据加密模块(2-2)；

所述的数据加密模块(2-2)，接收基于遗传算法的续传数据预处理模块(2-1)的服务请求数据，对每一组数据M_X进行Hash运算得到$H_X=Hash(M_X)$，对M_X、H_X、L_X使用改进后的SM4算法，采用由用户密钥协商模块(1)协商的会话密钥K_{AB}，进行加密得到密文$E_{K_{AB}}(M_X||L_X||H_X)$，最后将消息$E_{K_{AB}}(M_X||L_X||H_X)||L_X||num$，按照$L_X$标签顺序发送至数据解密与验证模块(3)，若收到数据解密与验证模块(3)返回数据标签信息L_X，则从当前数据标签L_X处发送，待最后一组数据密文发出后，计算$H(M)=H(M_1||\cdots||M_X)$，并使用会话密钥K_{AB}加密得到$E_{K_{AB}}(H(M))$，发送至数据解密与验证模块(3)，若连续两次收到由数据解密与验证模块(3)返回的超时信息111111000，则重新发送$E_{K_{AB}}(H(M))$至数据解密与验证模块(3)。

4.根据权利要求1所述的一种具有密钥协商功能的加密续传方法，其特征在于：所述的数据解密与验证模块(3)包括数据解密模块(3-1)以及数据完整性验证与聚合模块(3-2)；所述数据解密与验证模块(3)通过设计改进的SM4加解密算法，设计改进的完整性验证模块算法，实现多分组密文的解密与完整性验证，其中通过为每个分组的密文进行分别验证，保证个体和集体的一致性；通过分组个体和整体的分别验证，使得整体数据不会存在安全风险，保证数据的安全性；

所述的数据解密模块(3-1)接收来自数据加密模块(2-2)发送的$E_{K_{AB}}(M_X||L_X||H_X)||L_X||num$密文消息以及$E_{K_{AB}}(H(M))$，获得来自服务器密钥协商模块(4)协商成功的会话密钥K_{AB}，若未收到$E_{K_{AB}}(H(M))$则说明数据未传输完整，向数据处理与加密模块(2)返回当前传输的数据标签信息L_X，比对L_X与num，若相同，则表示接收到最后一组标签数据，若不同，则表示接收到的非最后一组数据，继续传输下一组数据；之后若在规定时间内未收到$E_{K_{AB}}(H(M))$，连续两次向数据处理与加密模块(2)返回超时代码111111000，若所有信息正常接收，数据解密模块(3-1)对收到的消息进行解密$D_{K_{AB}}(E_{K_{AB}}(M_X||L_X||H_X))$，得到$M_X$、$L_X$、$H_X$；

所述的数据完整性验证与聚合模块(3-2)通过设计改进的完整性验证模块算法，分别针对个体完整性与集体完整性进行分类验证，该模块按照发送信息所对应的标签L_X对每一分组数据进行完整性验证，用数据解密模块(3-1)解密所得的L_X与消息中的L_X进行比对，判别是否满足组别相同，若相同则表示系统正常，若不同则中止会话；用明文M_X的Hash值与解密信息中H_X进行比对，若相同表示系统正常，否则中止会话；根据遗传算法的分组特性与标签信息L_X对解密所得的明文进行聚合$M=M_1||\cdots||M_X$，最后对聚合后的明文M进行Hash运算得到H(M)，与$D_{K_{AB}}(E_{K_{AB}}(H(M)))$进行比对，若两者相同，则系统正常完成传输，否则，系统解密所得明文不符合完整性要求，中止当前会话。

5.根据权利要求1所述的一种具有密钥协商功能的加密续传方法，其特征在于：所述的

服务器密钥协商模块(4)包括协商应答生成模块(4-1)和服务器组密钥计算模块(4-2)，负责在每次完成认证基础上，接收用户密钥协商模块(1)发起的挑战，并作出应答，然后协商生成一组会话密钥，并且在密钥协商过程中抵抗中间人攻击；

所述的协商应答生成模块(4-1)首先保存当前实体向可信第三方申请的公钥证书$Cert_B$和私钥SK_B，同时生成私有随机数N_{ID_B}，并接收协商挑战生成模块(1-1)所公开的大素数p及其本原根a，然后随机选择一个私有的随机数X_B(X_B＜P)，计算当前实体参数$Y_B = a^{X_B} \bmod p$，生成包含当前实体参数Y_B的签名$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$，再使用用户公钥$PK_A$进行加密得到$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A}))$，并将协商参数$Y_B$、密文$C_B$和公钥证书$Cert_B$作为密钥协商参数，发送到用户组密钥计算模块(1-2)；

所述的服务器组密钥计算模块(4-2)接收来自协商挑战生成模块(1-1)所发送的密钥协商参数Y_A，密文C_A和公钥证书$Cert_A$，同时获得协商应答生成模块(4-1)传输的密钥协商参数Y_B，应用服务器私钥SK_B对密文$C_A = E_{PK_B}(Sig_{SK_A}(Y_A \| N_{ID_A}))$进行解密，得到$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$，再使用公钥证书$Cert_A$中的公钥$PK_A$，通过签名验证恢复算法恢复出$Y_A \| N_{ID_A} = V_{PK_A}(Sig_A)$，将恢复出的$Y_A$与接收到的$Y_A$进行比对，若一致，则系统正常，计算得到会话密钥$K_{AB} = (Y_A)^{X_B} \bmod p$；否则，中止当前会话；接收协商挑战生成模块(1-1)发送的$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$，通过解密计算$D_{SK_B}(E_{PK_B}(N_{ID_B} \| H(K_{AB})))$，将结果与$N_{ID_B} \| H(K_{AB})$比对，若一致，则系统正常；否则，中止当前会话；最后将所生成的会话密钥K_{AB}传输给数据解密与验证模块(3)。

一种具有密钥协商功能的加密续传方法

技术领域

[0001] 本发明涉及计算机网络通信领域以及信息安全领域,特别涉及一种具有密钥协商功能的加密续传方法。

背景技术

[0002] 目前,移动定位系统中所使用的文件上传技术与大多数文件上传技术一样,有一个共同的缺点,即遭遇网络故障,数据需要重新传输,且传输过程中会存在无法保证机密性和完整性的问题,导致系统缺乏安全性和有效性。本发明专利所研究的文件传输技术面向开放的互联网,存在各种各样的攻击行为,时刻威胁着网络上所传输数据的安全性与效率。近年来,数据劫持问题引起的安全问题频发,如AcFun受到黑客信息劫持攻击,数千万条用户信息被泄露,瑞士电信80万条数据被盗,医疗软件公司MedEvolve因服务器漏洞被劫持信息高达20 万条等。为了实现网络中的数据安全,传输的文件或数据应当只有符合规定的用户才可以获取,因此,认证技术,加密算法被应用在数据传输技术中,仅有符合条件的用户才能够接收数据,并正确解密密文从而确保传输数据的安全。同时,在当今的网络环境中,高效一直是共同追求的一个目标,断点续传技术能够保证数据在网络传输中的高效。因此,本发明针对传输数据在开放的Internet网络中机密性与完整性无法保护,以及数据文件传输低效的问题,开发一种具有密钥协商功能的加密续传方法,应用于不同大小的文件数据传输系统,保证文件传输系统的高效与安全。

[0003] 专利申请一种数据断点续传技术方法(201610536678)提供了一种基于链表结构的数据断点续传技术方法,解决了传统数据传输系统在网络故障情况下效率低下问题,实现了数据的断点续传,该发明可用于对数据传输可靠性要求极高但网络环境又存在不确定性的环境,如无线网路,该数据位于网络协议层的应用层。但是,该发明存在以下缺陷,第一,传输数据无法保证完整性;第二,传输过程以明文形式传输,无法保证数据的机密性;第三,传输过程对通信双方身份无法进行认证。

[0004] 专利申请一种文件下载断点续传的方法及系统(201610697034.X),采用控制控制文件下载地址预设生命周期的技术,实现了数据的断点续传。所述文件下载断点续传的方法包括:步骤1、创建存储有文件的第一下载地址的下载地址列表;所述第一下载地址的有效的时间点为第一生命周期;步骤2、间隔预设时长,获取文件的第二下载地址,判断第二下载地址的第二生命周期是否等于第一生命周期,若否,则进入步骤3;步骤3、将第二下载地址与第一下载地址相关联;步骤4、下载客户端通过第一下载地址下载所述文件时,由第一下载地址链接到第二下载地址进行文件下载。用户在文件下载过程中突然掉电或中断后,继续使用旧地址下载,代理模块将旧地址链接至新地址,从而实现从下载服务器上继续下载带有生命周期的文件。该发明存在以下缺陷,第一,传输完成后对传输数据的完整性无法进行验证;第二,通信双方身份无法确认;第三,传输过程采用明文传输,无法保证传输数据的机密性。

[0005] 专利申请一种基于动态窗口的连续传输方法(201611006503.5),针对小规模可见

光通信网络流量饱和的情况，提出一种基于动态窗口的连续传输(DCW-ST)方法。该发明基于对网络吞吐量的分析，得到使网络吞吐量最大化动态竞争窗口，然后基于对周期时延的分析，提出了兼顾吞吐量和时延的动态竞争窗口调节方法；进一步地，根据网络节点数目的情况，提出连续传输方案，以降低节点接入时延，从而达到网络吞吐量与时延的平衡。但是该发明存在以下缺陷，第一，在传输数据前无法对数据交互双方进行身份认证；第二，传输过程全部以明文传输，安全性低；第三，遇到断网等突发情况需要重新传输，系统灵活性差。

[0006] 专利申请一种文件断点续传方法(201810094808.9)，该发明方法基于客户端获取断点信息，并基于断点信息执行文件流续传，客户端发起文件上传请求及文件检查请求；服务端确定并保存文件断点位置；客户端获取文件断点信息；服务端响应续传文件流请求；客户端接收文件上传结果标识。该发明的文件断点续传方法能够节省文件的上传时间和网络资源，并且能够保证文件续传的准确及稳定性。但是该发明存在以下缺陷，第一，在传输数据前无法对通信双方进行身份确认，接收数据无法确认完整性；第二，传输过程中以明文形式传输，安全性低。

[0007] 专利申请一种支持断点续传的数据抽取方法及系统(201811076270.5)，基于开源ETL工具-NIFI进行二次开发，原生处理器支持配置数据源信息，配置物理表信息，配置增量抽取字段，并将截止当前时间该字段的数据最大值保存到处理器状态中。提供设置每次抽取最大记录数、每次调度分页抽取记录数、开始时间、间隔时间，并记录整个流程抽取总共抽取记录数、上次执行抽取记录数、调度次数，当前调度抽取完成记录数、已完成分页数、总分页数等信息，以供实现断点续传功能。该发明的数据抽取方法可避免服务器负载过大，确保服务器的稳定性，不会重复抽取已完成的数据，提高了数据抽取的效率。但是该发明存在安全缺陷，即抽取系统以明文传输，存在数据泄密的安全问题。

[0008] 专利申请一种下载断点续传的方法及装置(201811539333.6)，用以解决现有技术当下载中断时，需重新下载整个录像文件，导致浪费时间和流量的问题。该方法包括：接收到录像系统发送的与第一下载录像请求相匹配的多个监控录像；当所述监控录像中止发送所述第一目标监控录像时，将接收到的多个所述第一目标监控录像与多个第一监控录像文件相匹配，将未匹配成功的多个所述第一监控录像文件确认为第二监控录像文件；通过服务端向所述录像系统发送第二下载录像请求，所述下载录像请求内携带有第二目标监控录像的开始时刻和结束时刻。该发明存在以下缺陷，第一，下载录像过程无法对下载中心进行认证，出现多个源头无法进行确认；第二，传输过程录像文件未经加密处理，造成安全性低，传输完成无法保证录像的完整性。

[0009] 专利申请一种跨网络的断点续传方法和系统(201811583080.2)，通过文件分片与异步上传技术控制并发数量，实现了断点续传。前端对待上传文件进行加密，获得文件唯一标识发送给后端；后端根据文件唯一标识查询数据库，若文件上传过，则直接返回文件信息给前端；前端根据自定义配置开始对待上传文件进行分片，获得分片文件；前端将分片文件上传给后端，并展示上传进度，若分片上传失败，则重新上传失败的分片；后端接收前端上传的分片文件，进行唯一标识验证，若验证失败，则返回上传文件失败信息给前端，若验证成功，则验证分片是否全部上传完毕，当全部分片上传完成后，按照分片排序组合文件，将完整文件保存在文件服务器，并返回完整文件信息给前端，并把完整文件信息保存在数据库。其可以节约时间、流量，节省存储空间。该发明存在以下缺陷，第一，无法对跨网络的传

输双方进行身份认证;第二,传输过程采用明文传输,无法保证数据的机密性。

[0010] 专利申请一种断点续传文件传输的方法(201811636717.X),包括如下步骤:1)当通道中断时,发送端将通道中断期需要发送的文件进行缓存,形成续传文件;2)当通道恢复时,发送端以帧为单位向接收端发送续传文件,接收端收到每一帧续传文件都进行校验,并给发送端反馈校验信息,正确,则继续发送,错误,则重新发送上一帧;不存在续存文件时,发送端向接收端发送测试信息,收到则反馈;当发送端或接收端在设定时间内未收到对方的信息时,则重启通道;3)当整个续传文件传输完毕,发送端发送文件传输结束标志,接收端对整个续传文件长度进行校验,正确,发送正确确认信息;错误,则发送错误确认信息,重新启动整个流程。通过本发明使续传文件可以通过防火墙及安全隔离网闸。该发明存在以下缺陷,第一,传输数据以明文形式传输,无法保证传输的部分完整性;第二,无法对建立的通道进行身份识别,造成通信的双方无法认证身份。

[0011] 专利申请一种断点续传的无人车航线数据传输系统及其方法(201910147368.3),通过实时采样,校验,连续上传等技术克服现有数据传输系统存在的数据不连续与信息不同步问题。包括服务器和车载终端,车载终端接收服务器发送的航线数据,同时在车辆行驶时采集路况信息和车况信息并上传给服务器,服务器和车辆终端轮流作为发送端和接收端收发数据,发送端包括数据分块模块、数据发送模块和信号检测模块,接收端包括数据接收模块和数据校验模块。本发明可有效确保车辆在行驶过程中航线数据传输的连续性和实时性,减少数据传输时间,提高传输效率。但是目前该专利存在以下缺陷,第一,无法对数据的完整性进行验证;第二,传输过程采用明文传输,无法保证航线数据的安全性。

[0012] 专利申请集群式基于云平台的大数据断点续传的标书上传系统(201910485216.4),该系统包括客户端、服务端和云平台。服务端分别于客户端和云平台通信连接。在标书上传的过程中,客户端响选中标书文件,向服务端发送上传请求,服务端识别出编号信息,查找是否存在对应的上传记录。当存在时,从数据库中调取应标书信息,并向客户端发送续传请求;当不存在时,服务端发送上传命令,接收到标书信息后临时存储。当服务端接收完成标书信息后,将标书信息上传至云平台并删除临时存储的标书信息,采用上传信息验证的方式,通过终端交互设计,在上传中断时能够实现断点续传,提高标书上传的效率。但是,目前该系统存在以下缺陷,第一,上传的标书无法保证完整性;第二,采用明文传输,无法保证标书数据的机密性;第三,无法确认接收方身份。

[0013] 期刊论文基于Linux的文件加密传输技术(《计算机测量与控制》2015.12期),通过使用RSA加密算法与Linux系统线程池技术,实现了Linux系统客户端与服务端文件加密传输技术;通过在Linux上配置安装Openssl库来实现非对称RSA加密过程,并且利用线程池技术处理一个服务器与多个客户端的文件传输过程;最终实现了嵌入式ARM客户端与Linux服务器端的网络连接功能,并完成了基于TCP/IP协议上的文件加密以及传输过程;结论表明使用SSL协议设计的加密系统能够完成加密和传输过程,充分保障资料的私密性,并且能够方便的移植到安全级别需求高的嵌入式系统。该论文存在以下缺陷,第一,对于传输文件无法进行完整性验证;第二,传输中断,需要重新传输,无法实现断点续传;第三,公钥加密繁琐复杂,无法实现一次一密机制。

[0014] 期刊论文基于HTML5大文件断点续传的实现方案(《计算机与现代化》2016.3期),在 Web应用中,文件上传是一个常用的功能,而目前的文件上传方式在处理大文件上传方

面不尽人意，常常因为文件过大或者网络中断导致上传失败，不得不重新上传。通过使用一系列对文件操作的API，如File List、Blob、File、FileReader等接口技术，使得Web端能够使用Java Script对本地文件进行分片操作进而实现文件断点续传功能。该文在此基础上解决了服务器端文件合并过程中用户等待超时问题以及如何保证合并文件正确性的问题。该论文存在以下缺陷，第一，大文件在传输后，无法对其部分文件以及整体文件完整性进行验证；第二，对于传输文件的双方无法进行身份认证；第三，传输文件形式以明文传输，无法保证文件的机密性。

[0015] 期刊论文一种基于SIP和MSRP协议实现文件断点续传的方法(《无线电工程》2018.5期)，在文件传输过程中发生中断后，下次为了减少重复传输断点前的文件内容，提高传输效率，提升用户体验，需要文件传输服务具备断点续传功能。通过对会话初始协议(SIP)和消息会话中继协议(MSRP)进行了研究，提出一种基于SIP和MSRP协议实现断点续传的文件传输流程，并分别从协议字段扩展、信令流程和断点续传3个方面进行了详细阐述；对文件传输软件架构进行了设计。在统一通信系统中应用表明，该方法达到了无缝断点续传的效果。该论文存在以下缺陷，第一，传输文件虽然支持断点续传，但是对于文件的部分完整性和整体完整性无法保证；第二，文件传输以明文传输，无法保证传输数据的机密性。

[0016] 期刊论文动态对称密钥加密算法下终端升级文件安全传输(《信息技术》2019.12期)，为了提高终端升级文件的安全传输能力，需要进行文件加密设计，提出基于动态对称密钥设计的终端升级文件加密安全传输方法。采用无代理密钥发布协议进行终端升级文件的访问控制，构建终端升级文件的动态对称密钥；结合双线性映射方法进行终端升级文件安全加密过程中的密钥构造和算术编码设计；根据明文攻击的强度对终端升级文件进行置乱度重排，采用随机线性编码方法完成终端升级文件的动态对称密钥加密，实现文件的安全传输。该论文存在以下缺陷，第一，该系统无法保证传输文件的完整性；第二，传输中出现中断情况，需要重新传输，无法实现断点续传。

发明内容

[0017] 针对以上文件传输机密性差、无法进行部分以及整体的完整性验证、无法实现中断传输的数据续传、加密过程无法实现一次一密、系统兼容性差技术问题，本发明提供一种具有密钥协商功能的加密续传方法，本发明基于断点续传技术和密钥协商技术，提供了一种安全的、可完成一次一密的加密断点续传方法，该方法可针对不同的文件传输系统，对不同大小的文件在传输时进行细分，保证传输过程中不会发生网络拥塞，实现在传输过程中网络中断的情况下，下次传输可以从中断位置继续传输，同时在传输过程中对文件进行加密与完整性保护，预留了传输窗口大小可设置，以应对网络情况的好坏，扩展性强；另外，通过数据加密、签名技术以及完整性保护技术确保数据的安全，采用断点续传技术保证高效率。为达此目的：

[0018] 本发明提供一种具有密钥协商功能的加密续传方法，所述具有密钥协商功能的加密续传方法配套系统包括用户密钥协商模块、数据处理与加密模块、数据解密与验证模块和服务器密钥协商模块，具体步骤如下；

[0019] 首先用户密钥协商模块负责生成挑战信息，并与服务器密钥协商模块进行协议交互，通过自行设计的会话交互协议，产生一组会话密钥，用于加密分组后的通信数据；服务

器密钥协商模块生成应答消息，完成与用户密钥协商模块的协议交互，并最终产生一组会话密钥，用于密文的解密；

[0020] 然后数据处理与加密模块负责对即将传输的数据基于遗传算法进行分组标记，并对标记后的分组数据进行加密与完整性保护；最后数据解密与验证模块对接收到的所有密文进行解密，并对每组解密明文进行完整性验证；

[0021] 最后将所有解密明文进行组合，再一次进行完整性验证。

[0022] 作为本发明进一步改进，所述的用户密钥协商模块包括协商挑战生成模块和用户组密钥计算模块；负责在认证基础上，发起协商挑战与接收应答，产生一组会话密钥，并且在密钥协商过程中抵抗中间人攻击；

[0023] 所述的协商挑战生成模块首先保存当前通信实体向可信第三方申请的公钥证书$Cert_A$和 私钥SK_A，同时生成私有随机数N_{ID_A}，并且定义一个大素数p及其本原根a，公开p和a，然 后随机选择一个私有的随机数X_A(X_A＜p)，计算当前实体参数$Y_A = a^{X_A} \bmod p$，生成包含当 前实体参数Y_A的签名$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$，并采用服务器的公钥进行加密得到$C_A = E_{PK_B}(Sig(Y_A \| N_{ID_A}))$，最后将协商参数$Y_A$、$C_A$和公钥证书$Cert_A$作为密钥协商参数，发送到服务器密钥协商模块中的服务器组密钥计算模块；

[0024] 所述的用户组密钥计算模块接收来自协商应答生成模块发送的密钥协商参数，包括密文$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A}))$、参数$Y_B$、公钥证书$Cert_B$以及由协商挑战生成模块产生的 Y_A；使用私钥SK_A对C_B进行解密得到$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$，再采用公钥证书$Cert_B$中的公钥$PK_B$，通过签名验证恢复算法恢复出$Y_B \| N_{ID_B} \| N_{ID_A} = V_{PK_B}(Sig_B)$，将恢复出的$Y_B$、$N_{ID_A}$与接收到的$Y_B$、$N_{ID_A}$进行比对，若一致，则系统正常；否则，中止当前会话；从而验证数据来源的可靠性，接着计算得到会话密钥$K_{AB} = (Y_B)^{X_A} \bmod p$，并将会话密钥$K_{AB}$传输至数据处理与加密模块，同时计算$K_{AB}$的Hash值H($K_{AB}$)，结合$N_{ID_B}$使用服务器方公钥$PK_B$进行加密计算，得到$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$，将该密文发送至服务器密钥协商模块。

[0025] 作为本发明进一步改进，所述的数据处理与加密模块包括基于遗传算法的续传数据预处理模块和数据加密模块；负责对发送数据基于遗传算法进行分组分块，封装编号，采用改进的SM4算法进行加密与完整性保护，最后将加密后的分组数据发送至数据解密与验证模块，由于采用遗传算法及改进的SM4算法，提高了系统的处理能力与安全性；

[0026] 所述的基于遗传算法的续传数据预处理模块基于socket接口，通过TCP/IP传输协议，接收用户需要传输的明文数据M，基于遗传算法对该数据进行分类分组得到$M_1||\cdots||M_X$＝M和组数num，对分组后的明文M_X进行编码，生成相应的数据标签L_x，L_1即为00000001，对应分组明文M_1，将带有数据标签的分组明文数据$M_X||L_x$，以服务请求方式传输至数据加密模块；

[0027] 所述的数据加密模块，接收基于遗传算法的续传数据预处理模块的服务请求数据，对每一组数据M_X进行Hash运算得到H_X＝Hash(M_X)，对M_X、H_X、L_X使用改进后的SM4算法，采用由用户密钥协商模块协商的会话密钥K_{AB}，进行加密得到密文$E_{K_{AB}}(M_X \| L_X \| H_X)$，最后将消

息$E_{K_{AB}}(M_X\|L_X\|H_X)\|L_X\|num$，按照$L_X$标签顺序发送至数据解密与验证模块，若收到数据解密与验证模块返回数据标签信息L_X，则从当前数据标签L_X处发送，待最后一组数据密文发出后，计算H(M)＝H(M_1||…||M_X)，并使用会话密钥K_{AB}加密得到$E_{K_{AB}}(H(M))$，发送至数据解密与验证模块，若连续两次收到由数据解密与验证模块返回的超时信息111111000，则重新发送$E_{K_{AB}}(H(M))$至数据解密与验证模块。

[0028] 作为本发明进一步改进，所述的数据解密与验证模块包括数据解密模块以及数据完整性验证与聚合模块；所述数据解密与验证模块通过设计改进的SM4加解密算法，设计改进的完整性验证模块算法，实现多分组密文的解密与完整性验证，其中通过为每个分组的密文进行分别验证，保证个体和集体的一致性；通过分组个体和整体的分别验证，使得整体数据不会存在安全风险，保证数据的安全性；

[0029] 所述的数据解密模块接收来自数据加密模块发送的$E_{K_{AB}}(M_X\|L_X\|H_X)\|L_X\|num$密文消息以及$E_{K_{AB}}(H(M))$，获得来自服务器密钥协商模块协商成功的会话密钥$K_{AB}$，若未收到$E_{K_{AB}}(H(M))$则说明数据未传输完整，向数据处理与加密模块返回当前传输的数据标签信息 L_X，比对L_X与num，若相同，则表示接收到最后一组标签数据，若不同，则表示接收到的非最后一组数据，继续传输下一组数据；之后若在规定时间内未收到$E_{K_{AB}}(H(M))$，连续两次向数据处理与加密模块返回超时代码111111000，若所有信息正常接收，数据解密模块对收到的消息进行解密$D_{K_{AB}}(E_{K_{AB}}(M_X\|L_X\|H_X))$，得到$M_X$、$L_X$、$H_X$；

[0030] 所述的数据完整性验证与聚合模块通过设计改进的完整性验证模块算法，分别针对个体完整性与集体完整性进行分类验证，该模块按照发送信息所对应的标签L_X对每一分组数据进行完整性验证，用数据解密模块解密所得的L_X与消息中的L_X进行比对，判别是否满足组别相同，若相同则表示系统正常，若不同则中止会话；用明文M_X的Hash值与解密信息中H_X进行比对，若相同表示系统正常，否则中止会话；根据遗传算法的分组特性与标签信息L_X对解密所得的明文进行聚合M＝M_1||…||M_X，最后对聚合后的明文M进行Hash运算得到H(M)，与$D_{K_{AB}}(E_{K_{AB}}(H(M)))$进行比对，若两者相同，则系统正常完成传输，否则，系统解密所得明文不符合完整性要求，中止当前会话。

[0031] 作为本发明进一步改进，所述的服务器密钥协商模块包括协商应答生成模块和服务器组密钥计算模块，负责在每次完成认证基础上，接收用户密钥协商模块发起的挑战，并作出应答，然后协商生成一组会话密钥，并且在密钥协商过程中抵抗中间人攻击；

[0032] 所述的协商应答生成模块首先保存当前实体向可信第三方申请的公钥证书$Cert_B$和私钥SK_B，同时生成私有随机数N_{ID_B}，并接收协商挑战生成模块所公开的大素数p及其本原根a，然后随机选择一个私有的随机数X_B(X_B＜P)，计算当前实体参数$Y_B=a^{X_B}\bmod p$，生成包含 当前实体参数Y_B的签名$Sig_B=Sig_{SK_B}(Y_B\|N_{ID_B}\|N_{ID_A})$，再使用用户公钥$PK_A$进行加密得到 $C_B=E_{PK_A}(Sig_{SK_B}(Y_B\|N_{ID_B}\|N_{ID_A}))$，并将协商参数$Y_B$、密文$C_B$和公钥证书$Cert_B$作为密钥协商 参数，发送到用户组密钥计算模块；

[0033] 所述的服务器组密钥计算模块接收来自协商挑战生成模块所发送的密钥协商参数Y_A,密文C_A和公钥证书$Cert_A$,同时获得协商应答生成模块传输的密钥协商参数Y_B,应用服务器私钥SK_B对密文$C_A = E_{PK_B}(Sig_{SK_A}(Y_A \| N_{ID_A}))$进行解密,得到$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$,再使用公钥证书$Cert_A$中的公钥$PK_A$,通过签名验证恢复算法恢复出$Y_A \| N_{ID_A} = V_{PK_A}(Sig_A)$,将恢复出的 Y_A与接收到的Y_A进行比对,若一致,则系统正常,计算得到会话密钥$K_{AB} = (Y_A)^{X_B} \bmod p$;否则,中止当前会话;接收协商挑战生成模块发送的$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$,通过解密计算$D_{SK_B}(E_{PK_B}(N_{ID_B} \| H(K_{AB})))$,将结果与$N_{ID_B} \| H(K_{AB})$比对,若一致,则系统正常;否则,中止当前会话;最后将所生成的会话密钥K_{AB}传输给数据解密与验证模块。

[0034] 有益效果:

[0035] 与现有技术相比,本发明基于断点续传技术,加密技术,以及密钥协商,提供了一种具有密钥协商功能的加密续传方法,可针对不同规模的文件或数据传输系统,对所传输的数据和文件进行基于遗传算法的分类分组,保证系统在数据传输时可以实现安全高效的传输,遭遇网络故障时可以从传输故障之前的断点继续传输,实现了安全与效率的一个平衡。在系统预留了针对不同大小文件传输系统的空间,以应系统大小的变动,安全扩展性强。对SM4算法进行改进,以更好的针对文件类数据加密;加密续传方法的使用不受任何系统限制;用户与服务器交互时采用数据加密、认证等技术,确保数据的安全。本发明系统完整、整体安全性能好,高效,具有良好的扩展性和稳定性。

附图说明

[0036] 图1是本发明的整体框图;

[0037] 图2是本发明的整体原理结构图;

[0038] 图3是本发明的服务响应流程图;

[0039] 图4是本发明的用户密钥协商模块结构图;

[0040] 图5是本发明的数据处理与加密模块结构图;

[0041] 图6是本发明的数据解密与验证模块结构图;

[0042] 图7是本发明的服务器密钥协商模块结构图;

[0043] 图8是本发明的密钥协商原理图;

[0044] 附图标记;

[0045] 1、用户密钥协商模块;1-1、协商挑战生成模块;1-2、用户组密钥计算模块;2、数据处理与加密模块;2-1、续传数据预处理模块;2-2、数据加密模块;3、数据解密与验证模块;3-1、数据解密模块;3-2、数据完整性验证与聚合模块;4、服务器密钥协商模块;4-1、协商应答生成模块;4-2、服务器组密钥计算模块。

具体实施方式

[0046] 下面结合附图与具体实施方式对本发明作进一步详细描述:

[0047] 本发明基于断点续传技术与加密认证等技术进行改进设计,提供了一种安全的、高效的、可扩展的加密续传方法,该方法可针对不同大小的文件传输系统,需要传输的文件

进行分类分组，保证在实现可断点续传的同时满足安全与高效的平衡，实现在文件传输的高效与安全并存的特点；通过密钥协商、数据加密、认证技术确保数据的安全，改进断点续传技术切合加密技术保证系统的高效。

[0048] 如图1所示为本发明的整体框图，本发明所提出的一种具有密钥协商功能的加密续传方法包括：用户密钥协商模块1，数据处理与加密模块2，数据解密与验证模块3，服务器密钥协商模块4。本发明适用于任何能通过3G/4G/WiFi接入互联网的文件传输系统。用户密钥协商模块1与数据处理与加密模块2，数据解密与验证模块3与服务器密钥协商模块4，均通过 socket接口完成数据交互。

[0049] 如图2所示为本发明的整体原理结构图，本发明主要包括四大部分：用户密钥协商模块 1，数据处理与加密模块2，数据解密与验证模块3，服务器密钥协商模块4。所述的用户密钥协商模块1包括协商挑战生成模块1-1，用户组密钥计算模块1-2。所述的数据处理与加密模块2包括基于遗传算法的续传数据预处理模块2-1，数据加密模块2-2。所述的数据解密与验证模块3包括数据解密模块3-1，数据完整性验证与聚合模块3-2。所述的服务器密钥协商模块4包括协商应答生成模块4-1，服务器组密钥计算模块4-2。

[0050] 本发明的服务请求流程如图3所示：

[0051] 第一步，用户发起文件上传或下载请求，用户密钥协商模块1拿到公钥证书后，协商挑战生成模块1-1发送协商挑战信息；同时接收协商应答生成模块4-1发送的协商应答信息，然后由用户组密钥计算模块1-2对信息进行整合并计算出当前的组密钥信息发送至出数据处理与加密模块2，服务器组密钥计算模块4-2整合挑战信息计算出组密钥信息发送至数据解密与验证模块3。

[0052] 第二步，数据处理与加密；基于遗传算法的续传数据预处理模块2-1首先判断是否有该文件的处理记录，如果没有则对当前需要传输的数据进行分类分组，并赋予标签，通过设计改进SM4加密算法结合组密钥对分组后的每一组数据进行加密与完整性保护，传输分组后的密文数据至数据解密与验证模块3；如果有该文件的处理记录，则根据标签信息继续之前未完成的传输任务，将未传输完的数据继续发送至数据解密与验证模块3。

[0053] 第三步，数据解密与验证；首先数据解密模块3-1对接收到的密文数据进行解密，恢复至加密前的状态，然后，数据完整性验证与聚合模块3-2根据标签信息判断是否已经传输完数据，若数据已经传输完全，对恢复后的数据进行部分完整性验证与整体完整性验证，并按照标签信息对恢复的明文数据进行整合；若数据传输未完成，则只针对接收到的密文数据进行解密并完成该部分的完整性验证，数据不做整合，直至接收到最后一组密文数据；

[0054] 第四步，信息反馈；数据完整性验证与聚合模块4-2，对所有收到的数据进行整合，并验证数据的完整性信息，最后去除标签等信息，将数据信息反馈给用户，完成数据传输。

[0055] 用户密钥协商模块1如图4所示，所述的用户密钥协商模块1包括协商挑战生成模块1-1、用户组密钥计算模块1-2；负责在认证基础上，发起协商挑战与接收应答，产生一组会话密钥，并且在密钥协商过程中抵抗中间人攻击；所述的协商挑战生成模块1-1首先保存当前通信实体向可信第三方申请的公钥证书$Cert_A$和私钥SK_A，同时生成私有随机数N_{ID_A}，并且定义一个大素数p及其本原根a，公开p和a，然后随机选择一个私有的随机数X_A(X_A＜p)，计算当前实体参数$Y_A = a^{X_A} \bmod p$，生成包含当前实体参数Y_A的签名$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$，

并采用服务器的公钥进行加密得到$C_A = E_{PK_B}(Sig(Y_A \| N_{ID_A}))$，最后将协商参数$Y_A$、$C_A$和公钥证书 $Cert_A$作为密钥协商参数，发送到服务器密钥协商模块4中的服务器组密钥计算模块4-2；所述的用户组密钥计算模块1-2接收来自协商应答生成模块4-1发送的密钥协商参数，包括密文$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A}))$、参数$Y_B$、公钥证书$Cert_B$以及由协商挑战生成模块1-1产生的$Y_A$；使用私钥$SK_A$对$C_B$进行解密得到$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$，再采用公钥证书 $Cert_B$中的公钥PK_B，通过签名验证恢复算法恢复出$Y_B \| N_{ID_B} \| N_{ID_A} = V_{PK_B}(Sig_B)$，将恢复出的 Y_B、N_{ID_A}与接收到的Y_B、N_{ID_A}进行比对，若一致，则系统正常；否则，中止当前会话；从而验证数据来源的可靠性，接着计算得到会话密钥$K_{AB} = (Y_B)^{X_A} \bmod p$，并将会话密钥$K_{AB}$传输至数据处理与加密模块2，同时计算$K_{AB}$的Hash值$H(K_{AB})$，结合$N_{ID_B}$使用服务器方公钥$PK_B$进行加密计算，得到$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$，将该密文发送至服务器密钥协商模块4。

[0056] 数据处理与加密模块2如图5所示，所述的数据处理与加密模块2包括基于遗传算法的续传数据预处理模块2-1、数据加密模块2-2；负责对发送数据基于遗传算法进行分组分块，封装编号，采用改进的SM4算法进行加密与完整性保护，最后将加密后的分组数据发送至数据解密与验证模块3，由于采用遗传算法及改进的SM4算法，提高了系统的处理能力与安全性；所述的基于遗传算法的续传数据预处理模块2-1基于socket接口，通过TCP/IP传输协议，接收用户需要传输的明文数据M，基于遗传算法对该数据进行分类分组得到$M_1||\cdots||M_X=M$和组数num，对分组后的明文M_X进行编码，生成相应的数据标签L_x（L_1即为00000001，对应分组明文M_1），将带有数据标签的分组明文数据$M_X||L_x$，以服务请求方式传输至数据加密模块2-2；所述的数据加密模块2-2，接收基于遗传算法的续传数据预处理模块2-1的服务请求数据，对每一组数据M_X进行Hash运算得到$H_X=Hash(M_X)$，对M_X、H_X、L_X使用改进后的SM4算法，采用由用户密钥协商模块1协商的会话密钥K_{AB}，进行加密得到密文$E_{K_{AB}}(M_X||L_X||H_X)$，最后将消息$E_{K_{AB}}(M_X||L_X||H_X)||L_X \| num$，按照$L_X$标签顺序发送至数据解密与验证模块3，若收到数据解密与验证模块3返回数据标签信息L_X，则从当前数据标签L_X处发送，待最后一组数据密文发出后，计算$H(M)=H(M_1||\cdots||M_X)$，并使用会话密钥K_{AB}加密得到$E_{K_{AB}}(H(M))$，发送至数据解密与验证模块，若连续两次收到由数据解密与验证模块返回的超时信息 111111000，则重新发送$E_{K_{AB}}(H(M))$至数据解密与验证模块。

[0057] 数据解密与验证模块3如图6所示，所述的数据解密与验证模块3包括数据解密模块3-1 以及数据完整性验证与聚合模块3-2；所述数据解密与验证模块3通过设计改进的SM4加解密算法，设计改进的完整性验证模块算法，实现多分组密文的解密与完整性验证，其中通过为每个分组的密文进行分别验证，保证个体和集体的一致性；通过分组个体和整体的分别验证，使得整体数据不会存在安全风险，保证数据的安全性；所述的数据解密模块3-1接收来自数据加密模块2-2发送的$E_{K_{AB}}(M_X||L_X||H_X)||L_X \| num$密文消息以及$E_{K_{AB}}(H(M))$，获得来自服务器密钥协商模块4协商成功的会话密钥$K_{AB}$，若未收到$E_{K_{AB}}(H(M))$则说明数据未传输完整，向数据处理与加密模块2返回当前传输的数据标签信

息L_X,比对L_X与num,若相同,则表示接收到最后一组标签数据,若不同,则表示接收到的非最后一组数据,继续传输下一组数据;之后若在规定时间内未收到$E_{K_{AB}}(H(M))$,连续两次向数据处理与加密模块2返回超时代码111111000,若所有信息正常接收,数据解密模块3-1对收到的消息进行解密$D_{K_{AB}}(E_{K_{AB}}(M_X\|L_X\|H_X))$,得到$M_X$、$L_X$、$H_X$;所述的数据完整性验证与聚合模块3-2通过设计改进的完整性验证模块算法,分别针对个体完整性与集体完整性进行分类验证,该模块按照发送信息所对应的标签L_X对每一分组数据进行完整性验证,用数据解密模块3-1解密所得的L_X与消息中的L_X进行比对,判别是否满足组别相同,若相同则表示系统正常,若不同则中止会话;用明文M_X的Hash值与解密信息中H_X进行比对,若相同表示系统正常,否则中止会话;根据遗传算法的分组特性与标签信息L_X对解密所得的明文进行聚合,最后对聚合后的明文M 进行Hash运算得到H(M),与$D_{K_{AB}}(E_{K_{AB}}(H(M)))$进行比对,若两者相同,则系统正常完成传输,否则,系统解密所得明文不符合完整性要求,中止当前会话。

[0058] 服务器密钥协商模块4如图7所示,所述的服务器密钥协商模块4包括协商应答生成模 块4-1和服务器组密钥计算模块4-2,负责在每次完成认证基础上,接收用户密钥协商模块1 发起的挑战,并作出应答,然后协商生成一组会话密钥,并且在密钥协商过程中抵抗中间人 攻击;所述的协商应答生成模块4-1首先保存当前实体向可信第三方申请的公钥证书$Cert_B$和 私钥SK_B,同时生成私有随机数N_{ID_B},并接收协商挑战生成模块1-1所公开的大素数p及其 本原根a,然后随机选择一个私有的随机数X_B(X_B<P),计算当前实体参数$Y_B=a^{X_B}\bmod p$,生成包含当前实体参数Y_B的签名$Sig_B=Sig_{SK_B}(Y_B\|N_{ID_B}\|N_{ID_A})$,再使用用户公钥$PK_A$进行加 密得到$C_B=E_{PK_A}(Sig_{SK_B}(Y_B\|N_{ID_B}\|N_{ID_A}))$,并将协商参数$Y_B$、密文$C_B$和公钥证书$Cert_B$作为密 钥协商参数,发送到用户组密钥计算模块1-2;所述的服务器组密钥计算模块4-2接收来自协 商挑战生成模块1-1所发送的密钥协商参数Y_A,密文C_A和公钥证书$Cert_A$,同时获得协商应 答生成模块4-1传输的密钥协商参数Y_B,应用服务器私钥SK_B对密文$C_A=E_{PK_B}(Sig_{SK_A}(Y_A\|N_{ID_A}))$进行解密,得到$Sig_A=Sig_{SK_A}(Y_A\|N_{ID_A})$,再使用公钥证书$Cert_A$中 的公钥$PK_A$,通过签名验证恢复算法恢复出$Y_A\|N_{ID_A}=V_{PK_A}(Sig_A)$,将恢复出的$Y_A$与接收到的 Y_A进行比对,若一致,则系统正常,计算得到会话密钥$K_{AB}=(Y_A)^{X_B}\bmod p$;否则,中止当前 会话;接收协商挑战生成模块1-1发送的$E_{PK_B}(N_{ID_B}\|H(K_{AB}))$,通过解密计算$D_{SK_B}(E_{PK_B}(N_{ID_B}\|H(K_{AB})))$,将结果与$N_{ID_B}\|H(K_{AB})$比对,若一致,则系统正常;否则,中止当前会话;最后将所生成的会话密钥K_{AB}传输给数据解密与验证模块3。

[0059] 系统的密钥协商原理如图8所示:

[0060] 第一步,实体A获取一个大素数p以及p的本原根a,将p和a公开,然后随机选择一个私有的随机数X_A(X_A<p),通过这三个初始化参数、私钥SK_A和公钥证书$Cert_A$计算$Y_A=a^{X_A}\bmod p$,通过参数Y_A、私钥SK_A和公钥证书$Cert_A$,计算当前实体参数Y_A和身份随机数N_{ID_A}(由服务器认证模块提供)签名$Sig_A=Sig_{SK_A}(Y_A\|N_{ID_A})$,使用服务器公钥$PK_B$进行加密得到密文$C_A=E_{PK_B}(Sig_{SK_A}(Y_A\|N_{ID_A}))$,并将密文$C_A$和公钥证书$Cert_A$以及协商参数$Y_A$送给实体

B；

[0061] 第二步，实体B获取公开的大素数p以及p的本原根a，并接收A发送的密文C_A和公钥证书$Cert_A$以及协商参数Y_A，使用服务器私钥SK_B解密得到$Sig_A = Sig_{SK_A}(Y_A \| N_{ID_A})$，再通过签名恢复算法$Y_A \| N_{ID_A} = V_{PK_A}(Sig_A)$得到$Y_A$和$N_{ID_A}$，然后随机选择一个私有的随机数 X_B(X_B＜p)，通过这三个初始化参数p，a，X_B(X_B＜p)计算$Y_B = a^{X_B} \bmod p$，并通过参数Y_B、身份随机数N_{ID_B}(由用户认证模块提供)、私钥SK_B和公钥证书$Cert_B$计算当前实体参数Y_B的 签名$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$，使用用户端的公钥对签名进行加密得到$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A}))$，并将密文$C_B$和公钥证书$Cert_B$以及协商参数$Y_B$发送给实体 A；

[0062] 第三步，实体A接收实体B发送的协商参数即密文C_B和公钥证书$Cert_B$以及Y_B，使用用户端私钥SK_A对C_B进行解密得到$Sig_B = Sig_{SK_B}(Y_B \| N_{ID_B} \| N_{ID_A})$，再使用公钥证书$Cert_B$中的公钥$PK_B$，通过签名验证恢复算法计算$Y_B \| N_{ID_B} \| N_{ID_A} = V_{PK_B}(Sig_B)$，比对协商参数中的$Y_B$、$N_{ID_A}$是否和签名验证恢复的结果一致，若一致，则系统正常；否则，中止当前会话；从而验证数据来源的可靠性，再计算$K_{AB} = (Y_B)^{X_A} \bmod p$得到会话密钥，最后实体A发送$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$至实体B；

[0063] 第四步，实体B计算$K_{AB} = (Y_A)^{X_B} \bmod p$得到会话密钥，接收实体A发送的验证消息即$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$，使用私钥$SK_B$进行计算验证$D_{SK_B}(E_{PK_B}(N_{ID_B} \| H(K_{AB})))$，若结果和服务器身份认证模块接收的$N_{ID_B}$相同，系统正常；否则，中止当前会话；从而验证数据来源的可靠性。

[0064] 以上所述，仅是本发明的较佳实施例而已，并非是对本发明作任何其他形式的限制，而依据本发明的技术实质所作的任何修改或等同变化，仍属于本发明所要求保护的范围。

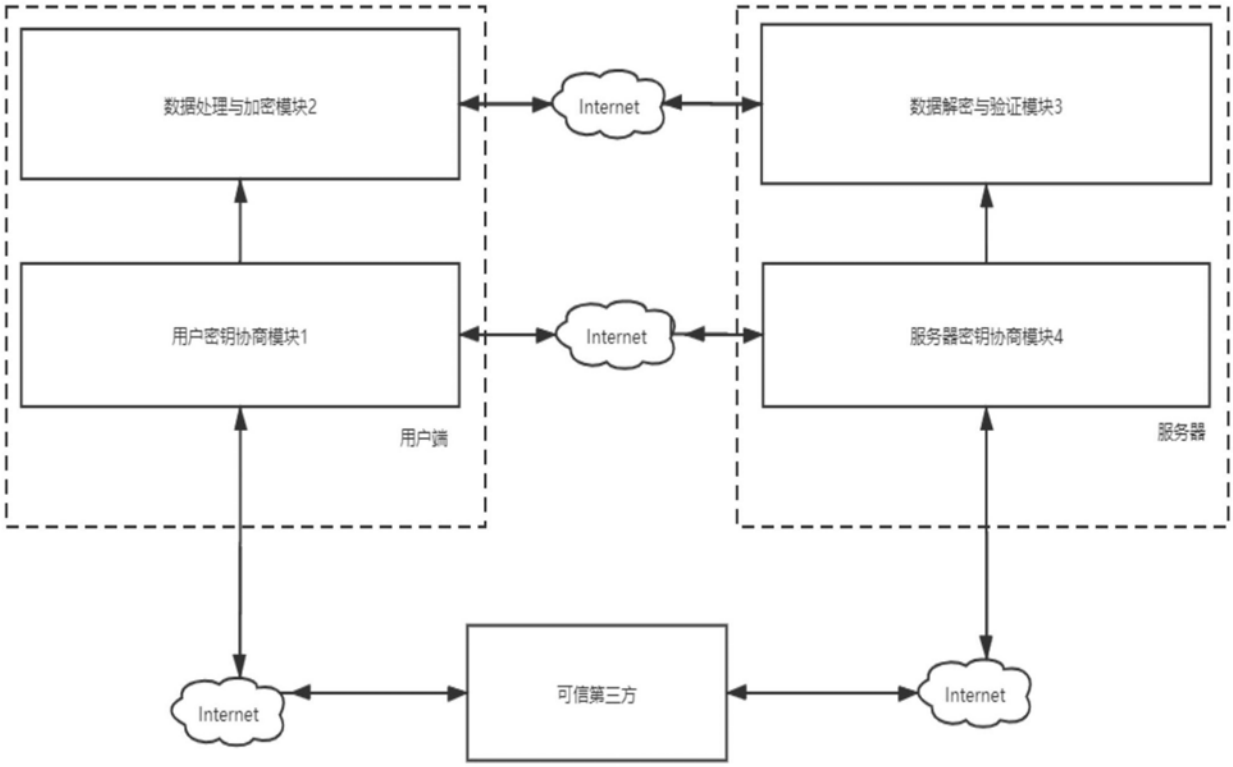

数据处理与加密模块2
Internet
数据解密与验证模块3
用户密钥协商模块1
Internet
服务器密钥协商模块4
用户端
服务器
Internet
可信第三方
Internet

图1

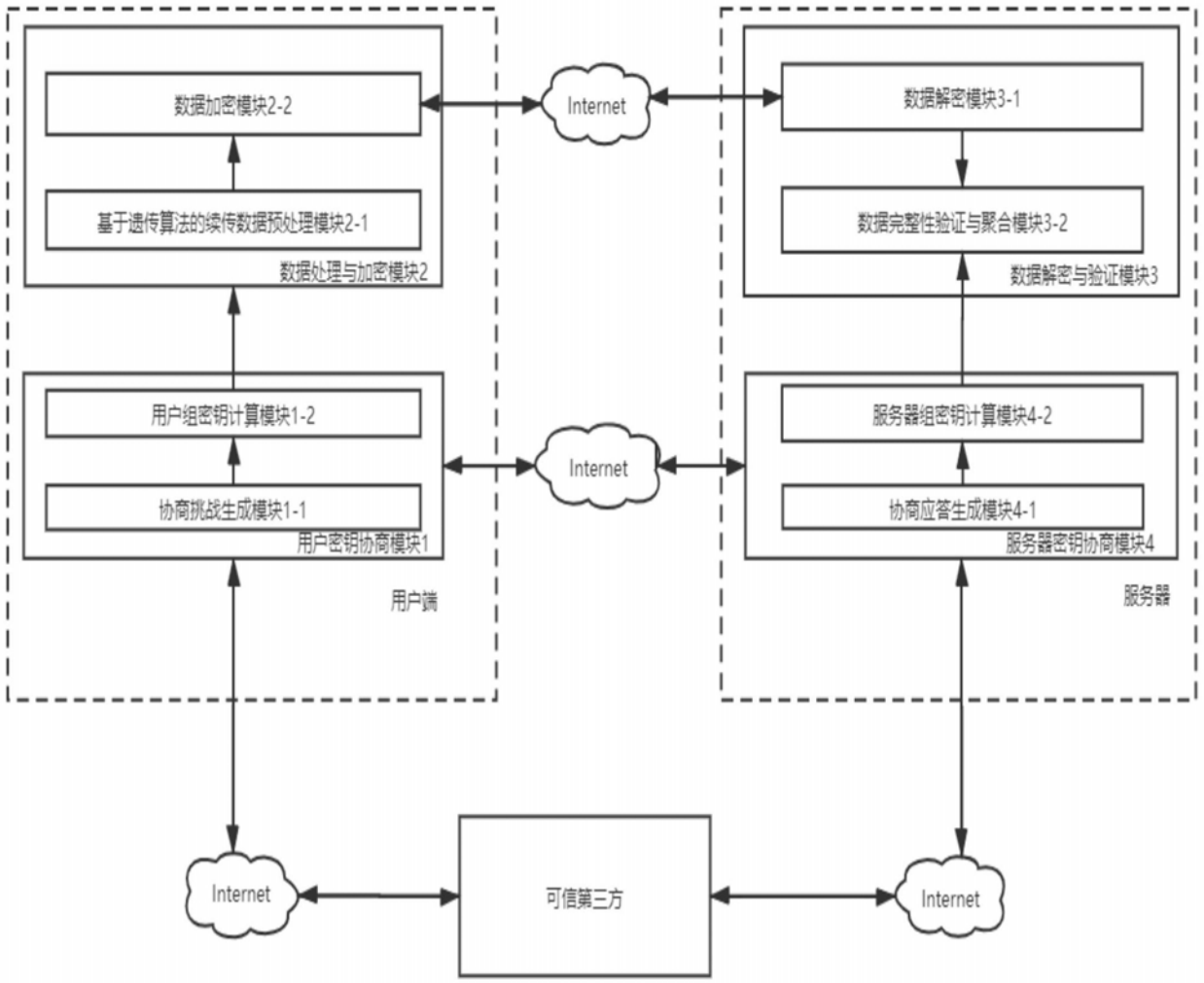

数据加密模块2-2
基于遗传算法的续传数据预处理模块2-1
数据处理与加密模块2
用户组密钥计算模块1-2
协商挑战生成模块1-1
用户密钥协商模块1
用户端
Internet
数据解密模块3-1
数据完整性验证与聚合模块3-2
数据解密与验证模块3
服务器组密钥计算模块4-2
协商应答生成模块4-1
服务器密钥协商模块4
服务器
Internet
Internet
可信第三方
Internet

图2

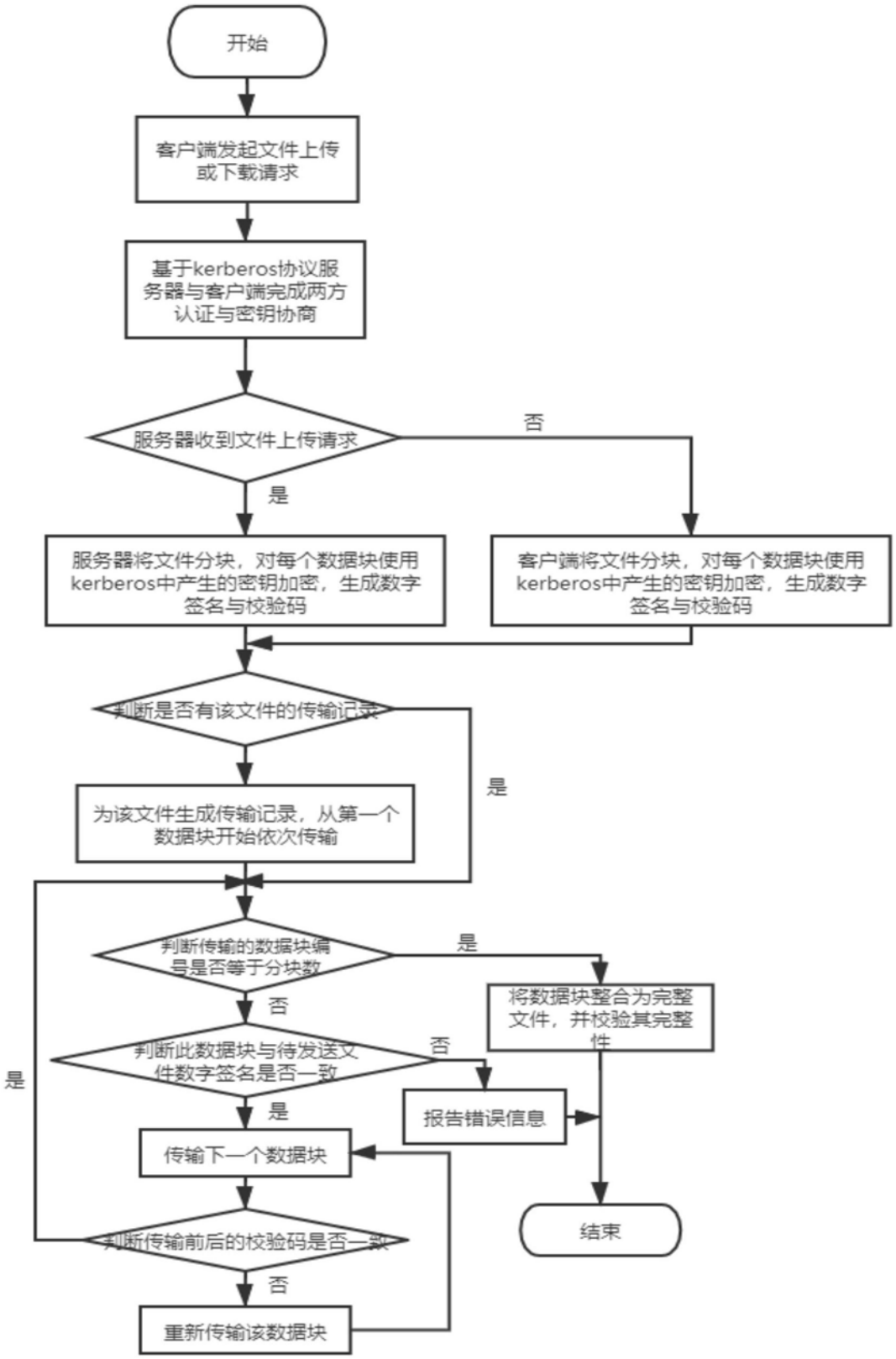

开始
客户端发起文件上传或下载请求
基于kerberos协议服务器与客户端完成两方认证与密钥协商
服务器收到文件上传请求
否
是
服务器将文件分块，对每个数据块使用kerberos中产生的密钥加密，生成数字签名与校验码
客户端将文件分块，对每个数据块使用kerberos中产生的密钥加密，生成数字签名与校验码
判断是否有该文件的传输记录
是
为该文件生成传输记录，从第一个数据块开始依次传输
判断传输的数据块编号是否等于分块数
是
将数据块整合为完整文件，并校验其完整性
否
判断此数据块与待发送文件数字签名是否一致
否
是
报告错误信息
传输下一个数据块
结束
判断传输前后的校验码是否一致
是
否
重新传输该数据块

图3

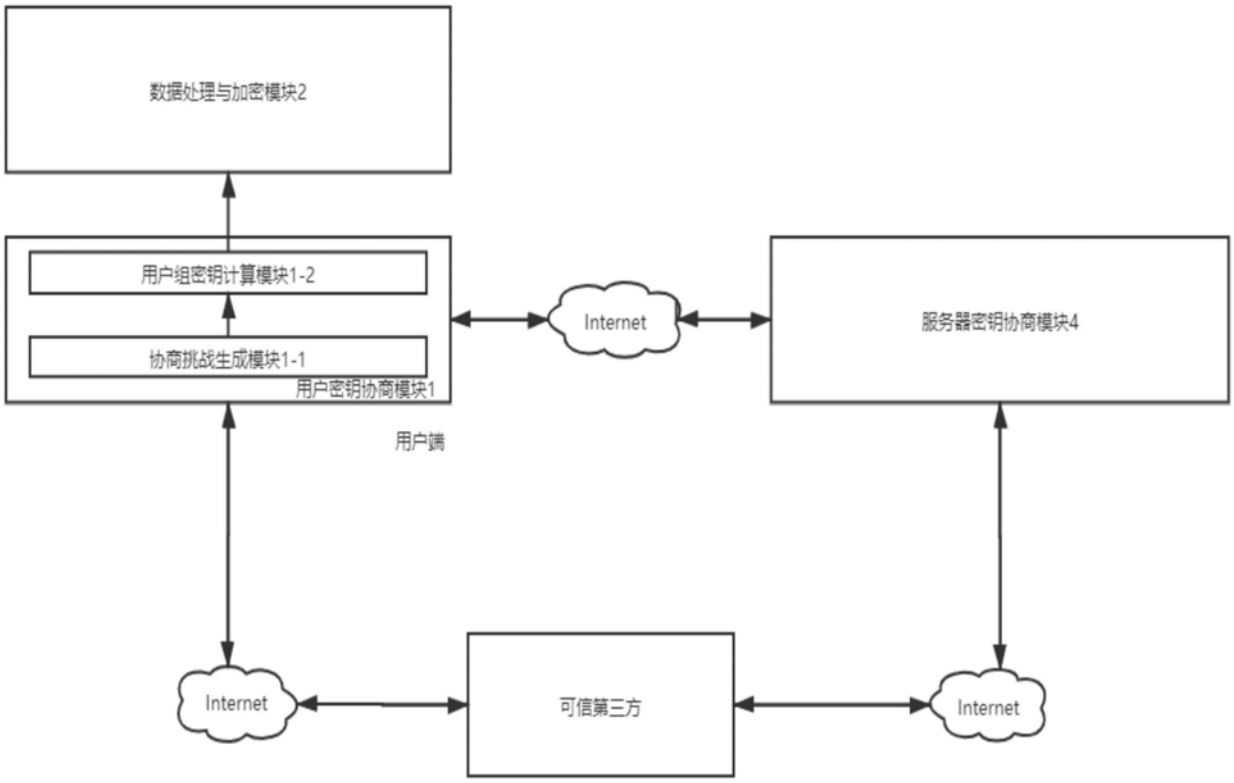

数据处理与加密模块2
用户组密钥计算模块1-2
协商挑战生成模块1-1
用户密钥协商模块1
用户端
Internet
服务器密钥协商模块4
Internet
可信第三方
Internet

图4

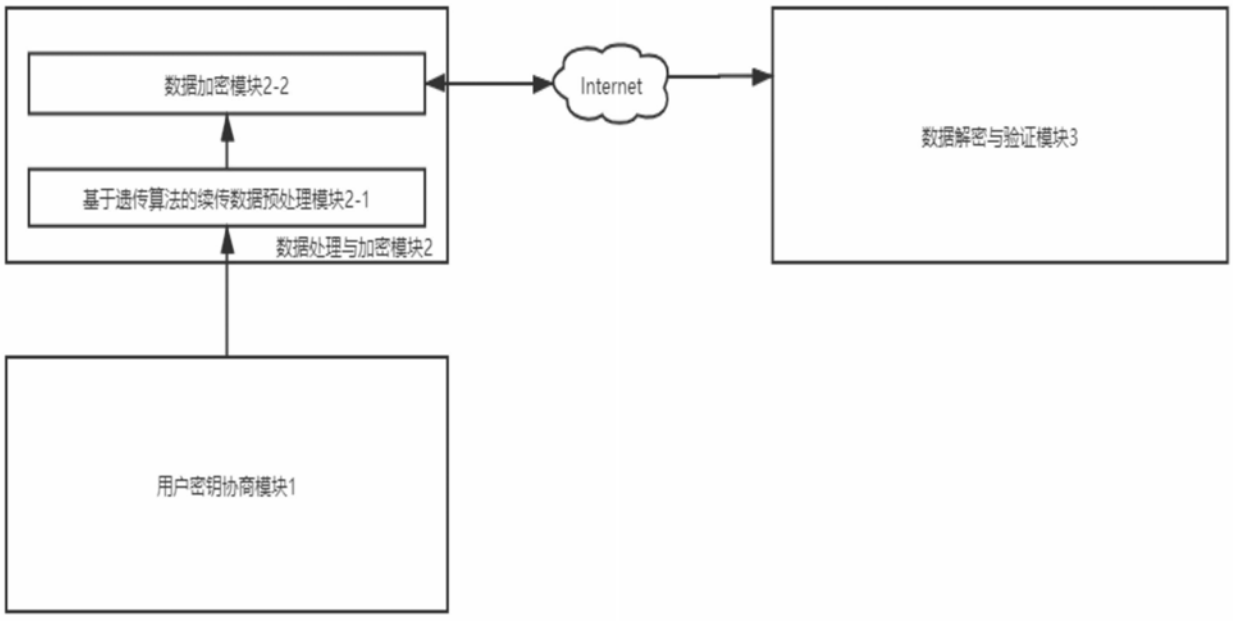

数据加密模块2-2
基于遗传算法的续传数据预处理模块2-1
数据处理与加密模块2
用户密钥协商模块1
Internet
数据解密与验证模块3

图5

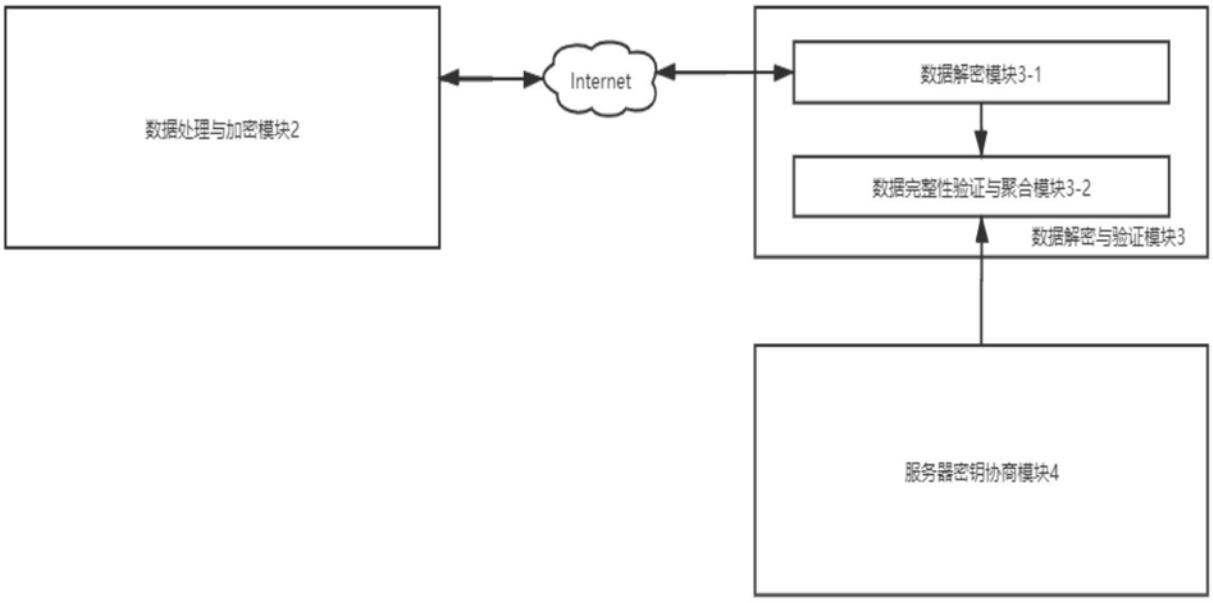

数据处理与加密模块2
Internet
数据解密模块3-1
数据完整性验证与聚合模块3-2
数据解密与验证模块3
服务器密钥协商模块4

图6

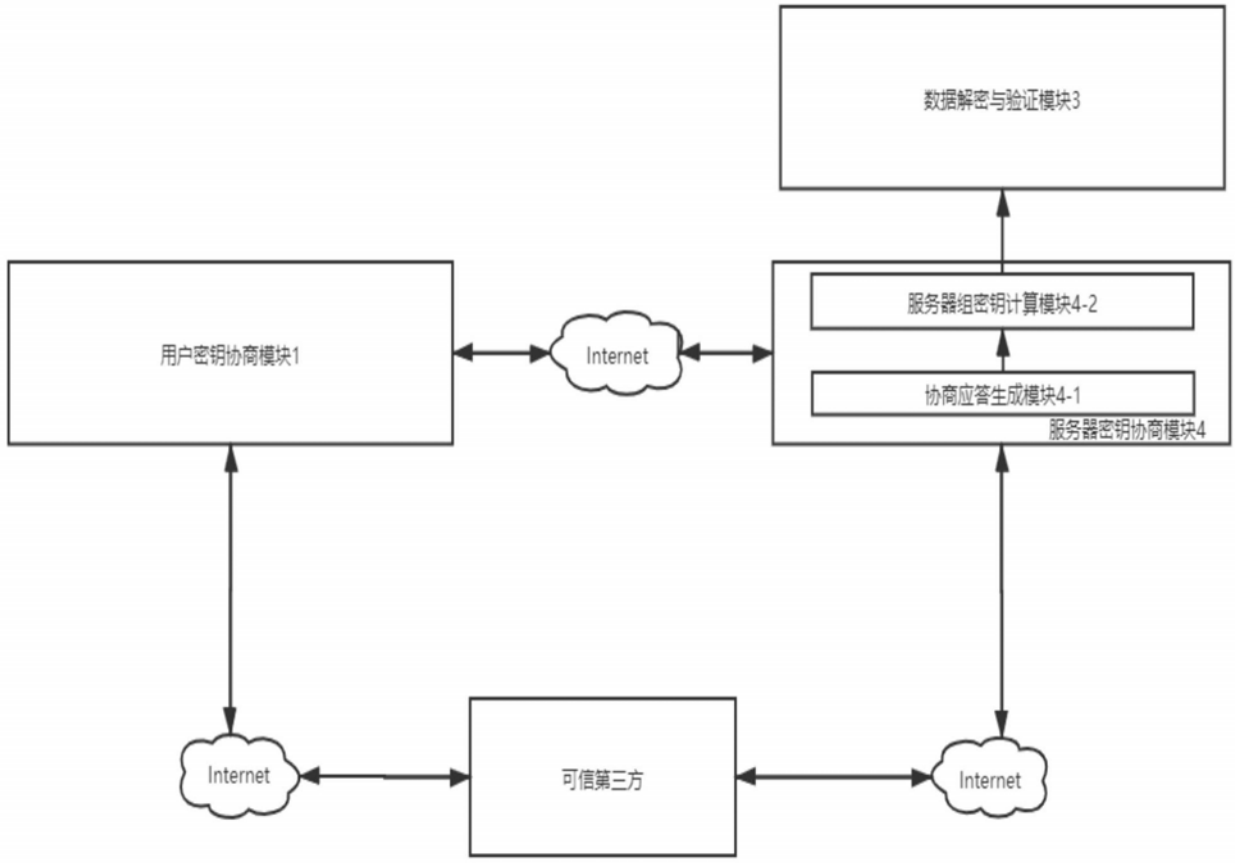

数据解密与验证模块3
用户密钥协商模块1
Internet
服务器组密钥计算模块4-2
协商应答生成模块4-1
服务器密钥协商模块4
Internet
可信第三方
Internet

图7

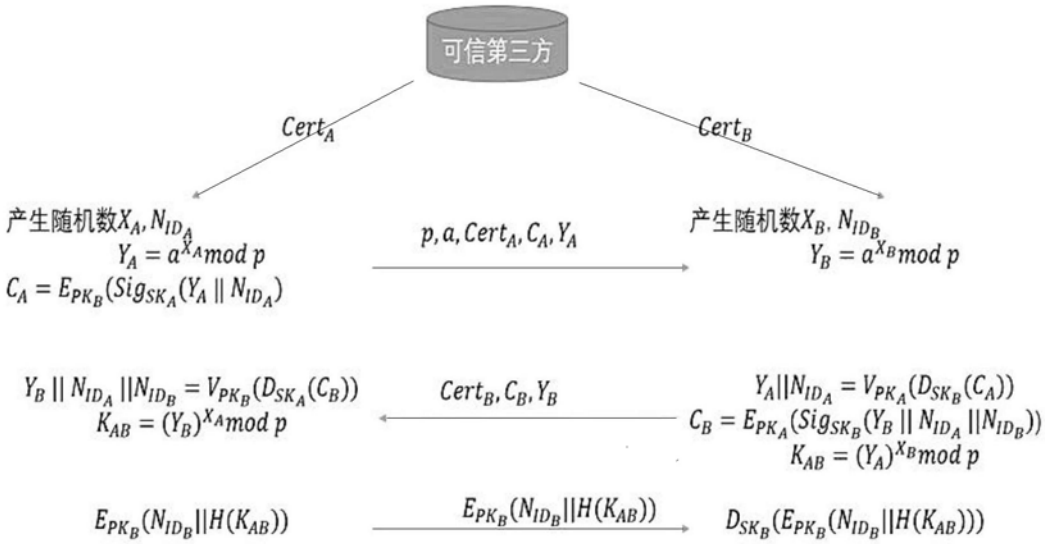

可信第三方
$Cert_A$
$Cert_B$
产生随机数X_A, N_{ID_A}
$Y_A = a^{X_A} mod\ p$
$C_A = E_{PK_B}(Sig_{SK_A}(Y_A \| N_{ID_A}))$
$p, a, Cert_A, C_A, Y_A$
产生随机数X_B, N_{ID_B}
$Y_B = a^{X_B} mod\ p$
$Y_B \| N_{ID_A} \| N_{ID_B} = V_{PK_B}(D_{SK_A}(C_B))$
$K_{AB} = (Y_B)^{X_A} mod\ p$
$Cert_B, C_B, Y_B$
$Y_A \| N_{ID_A} = V_{PK_A}(D_{SK_B}(C_A))$
$C_B = E_{PK_A}(Sig_{SK_B}(Y_B \| N_{ID_A} \| N_{ID_B}))$
$K_{AB} = (Y_A)^{X_B} mod\ p$
$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$
$E_{PK_B}(N_{ID_B} \| H(K_{AB}))$
$D_{SK_B}(E_{PK_B}(N_{ID_B} \| H(K_{AB})))$

图8