(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103986716 B
(45)授权公告日 2017.02.01

(21)申请号 201410215917.3

(22)申请日 2014.05.21

(65)同一申请的已公布的文献号
申请公布号 CN 103986716 A

(43)申请公布日 2014.08.13

(73)专利权人 深圳大学
地址 518060 广东省深圳市南山区南海大道3688号

(72)发明人 段孝茹 陈剑勇 林秋镇 喻建平

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文

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

(56)对比文件
CN 103763356 A,2014.04.30,
CN 102833253 A,2012.12.19,
US 2008034057 A1,2008.02.07,
乔艳飞.SSL安全分析以及中间人攻击和防范研究.《中国优秀硕士学位论文全文数据库信息科技辑(月刊)》.2013,I139-125页.

审查员 李腾

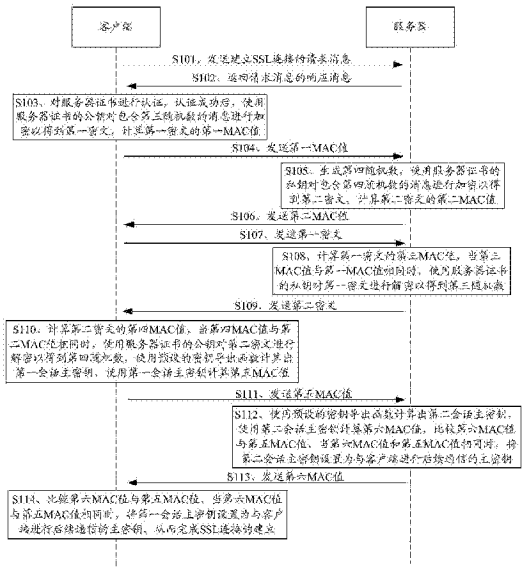
权利要求书3页 说明书9页 附图3页

(54)发明名称

SSL连接的建立方法以及基于SSL连接的通信方法及装置

(57)摘要

本发明适用通信安全领域，提供了SSL连接的建立方法以及基于SSL连接的通信方法及装置，在客户端和服务器之间建立SSL连接的过程中引入联锁机制，客户端和服务器首先分别收到密文数据对应的MAC值，再收到密文数据，之后分别计算收到加密后消息密文数据的MAC值，通过对比判断是否有中间人攻击，从而保证了后续生成的会话主密钥的安全性，有效地避免了中间人攻击。




CN 103986716 B

1.一种SSL连接的通信方法，其特征在于，所述方法包括下述步骤：

客户端向服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数；

所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数；

所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值，将所述第一MAC值发送给所述服务器；

所述服务器接收到所述第一MAC值后，生成第四随机数，使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文，计算所述第二密文的MAC值，将该MAC值记为第二MAC值，将所述第二MAC值发送给所述客户端；

所述客户端接收到所述第二MAC值后，将所述第一密文发送给所述服务器；

所述服务器接收到所述第一密文后，计算所述第一密文的MAC值，记为第三MAC值，当所述第三MAC值与所述第一MAC值相同时，使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数，将所述第二密文发送给所述客户端；

所述客户端接收到所述第二密文后，计算所述第二密文的MAC值，记为第四MAC值，当所述第四MAC值与所述第二MAC值相同时，使用所述服务器证书的公钥对所述第二密文进行解密以得到所述第四随机数，根据所述第一随机数、第二随机数以及第三随机数，使用预设的密钥导出函数计算出一会话主密钥，记为第一会话主密钥，使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第五MAC值，将所述第五MAC值发送给所述服务器；

所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第六MAC值发送给所述客户端，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥；

所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立；

所述客户端使用所述第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值，将所述第七MAC值发送给服务器；

所述服务器接收到所述客户端的第七MAC值后，使用所述第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值，将所述第八MAC值发送给客户端；

所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器；

所述服务器接收到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据，并将所述第四密文发送给所述客户端；

所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八

MAC值相同时，对所述第四密文进行解密以得到所述服务器数据，从而完成一次通信。

2.如权利要求1所述的方法，其特征在于，计算所述第一密文的所述第一MAC值的步骤包括：

将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第一MAC值；

计算所述第二密文的所述第二MAC值的步骤包括：

将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第二MAC值。

3.如权利要求1所述的方法，其特征在于，所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值的步骤之后，所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值的步骤之前，所述方法还包括：

当所述第六MAC值和所述第五MAC值不相同时，所述服务器终止与所述客户端的通信。

4.如权利要求1所述的方法，其特征在于，所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值的步骤之后，所述方法还包括：

当所述第六MAC值和所述第五MAC值不相同时，所述客户端终止与所述服务器的通信。

5.如权利要求1所述的方法，其特征在于，所述方法还包括：

当所述第九MAC值与所述第七MAC值不相同时，所述服务器终止与所述客户端的通信。

6.如权利要求1所述的方法，其特征在于，所述方法还包括：

当所述第十MAC值与所述第八MAC值不相同时，所述客户端终止与所述服务器的通信。

7.一种SSL连接的通信装置，其特征在于，所述装置包括：

请求消息发送单元，用于客户端向服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数；

响应消息返回单元，用于所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数；

第一处理单元，用于所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值，将所述第一MAC值发送给所述服务器；

第二处理单元，用于所述服务器接收到所述第一MAC值后，生成第四随机数，使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文，计算所述第二密文的MAC值，将该MAC值记为第二MAC值，将所述第二MAC值发送给所述客户端；

所述第一处理单元还用于当所述客户端接收到所述第二MAC值后，将所述第一密文发送给所述服务器；

所述第二处理单元还用于当所述服务器接收到所述第一密文后，计算所述第一密文的MAC值，记为第三MAC值，当所述第三MAC值与所述第一MAC值相同时，使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数，将所述第二密文发送给所述客户

端；

所述第一处理单元还用于当所述客户端接收到所述第二密文后，计算所述第二密文的MAC值，记为第四MAC值，当所述第四MAC值与所述第二MAC值相同时，使用所述服务器证书的公钥对所述第二密文进行解密以得到所述第四随机数，根据所述第一随机数、第二随机数以及第三随机数，使用预设的密钥导出函数计算出一会话主密钥，记为第一会话主密钥，使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第五MAC值，将所述第五MAC值发送给所述服务器；

所述第二处理单元还用于所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第六MAC值发送给所述客户端，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥；

所述第一处理单元还用于当所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立；

第三处理单元，用于客户端使用第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值，将所述第七MAC值发送给服务器；

第四处理单元，用于服务器接收到所述客户端的第七MAC值后，使用所述第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值，将所述第八MAC值发送给客户端；

所述第三处理单元还用于所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器；

所述第四处理单元还用于所述服务器接收到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据，并将所述第四密文发送给所述客户端；

所述第三处理单元还用于所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八MAC值相同时，对所述第四密文进行解密以得到所述服务器数据，从而完成一次通信。

8.如权利要求7所述的装置，其特征在于，计算所述第一密文的所述第一MAC值的步骤包括：

第一处理单元包括：

第一MAC值计算单元，用于将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第一MAC值；

第二处理单元包括：

第二MAC值计算单元，用于将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第二MAC值。

# SSL连接的建立方法以及基于SSL连接的通信方法及装置

## 技术领域

[0001] 本发明属于通信安全领域，尤其涉及一种SSL连接的建立方法以及基于SSL连接的通信方法及装置。

## 背景技术

[0002] 安全套接层(Secure Sockets Layer，缩写为SSL)协议主要用于网页(Web)服务的数据加密方面，以保证用户和服务器之间Web通信的数据安全。SSL协议可分为两层：SSL记录协议(SSL Record Protocol)：建立在可靠的传输协议(如TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL握手协议(SSL Handshake Protocol)：建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

[0003] 现有SSL握手协议需要公钥基础设施(Public Key Infrastructure，缩写为PKI)的支持，PKI的安全性依赖证书的安全性，而证书的安全性由证书的可信性和有效性来保证。使用证书前，需要检查证书撤销列表来确定证书的有效性，但事实上，通过证书撤销列表或者在线证书状态协议的有效性检测，并不能实时的提供有效性保证，客户端不能实时的得到这样的服务，因此，容易受到中间人攻击。

## 发明内容

[0004] 本发明实施例的目的在于提供一种SSL连接的建立方法以及基于SSL连接的通信方法及装置，旨在解决由于现有SSL协议中客户端和服务器之间的数据通信容易受到中间人攻击，导致客户端和服务器之间通信数据安全性降低的问题。

[0005] 本发明实施例是这样实现的，一方面，提供了一种SSL连接的建立方法，所述方法包括下述步骤：

[0006] 客户端向服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数；

[0007] 所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数；

[0008] 所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值，将所述第一MAC值发送给所述服务器；

[0009] 所述服务器接收到所述第一MAC值后，生成第四随机数，使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文，计算所述第二密文的MAC值，将该MAC值记为第二MAC值，将所述第二MAC值发送给所述客户端；

[0010] 所述客户端接收到所述第二MAC值后，将所述第一密文发送给所述服务器；

[0011] 所述服务器接收到所述第一密文后，计算所述第一密文的MAC值，记为第三MAC值，当所述第三MAC值与所述第一MAC值相同时，使用所述服务器证书的私钥对所述第一密文进

行解密以得到所述第三随机数，将所述第二密文发送给所述客户端；

[0012] 所述客户端接收到所述第二密文后，计算所述第二密文的MAC值，记为第四MAC值，当所述第四MAC值与所述第二MAC值相同时，使用所述服务器证书的公钥对所述第二密文进行解密以得到所述第四随机数，根据所述第一随机数、第二随机数以及第三随机数，使用预设的密钥导出函数计算出一会话主密钥，记为第一会话主密钥，使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第五MAC值，将所述第五MAC值发送给所述服务器；

[0013] 所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第六MAC值发送给所述客户端，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥；

[0014] 所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立。

[0015] 一方面，提供了一种SSL连接的建立装置，其特征在于，所述装置包括：

[0016] 请求消息发送单元，用于所述客户端向所述服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数；

[0017] 响应消息返回单元，用于所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数；

[0018] 第一处理单元，用于所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值，将所述第一MAC值发送给所述服务器；

[0019] 第二处理单元，用于所述服务器接收到所述第一MAC值后，生成第四随机数，使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文，计算所述第二密文的MAC值，将该MAC值记为第二MAC值，将所述第二MAC值发送给所述客户端；

[0020] 所述第一处理单元还用于当所述客户端接收到所述第二MAC值后，将所述第一密文发送给所述服务器；

[0021] 所述第二处理单元还用于当所述服务器接收到所述第一密文后，计算所述第一密文的MAC值，记为第三MAC值，当所述第三MAC值与所述第一MAC值相同时，使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数，将所述第二密文发送给所述客户端；

[0022] 所述第一处理单元还用于当所述客户端接收到所述第二密文后，计算所述第二密文的MAC值，记为第四MAC值，当所述第四MAC值与所述第二MAC值相同时，使用所述服务器证书的公钥对所述第二密文进行解密以得到所述第四随机数，根据所述第一随机数、第二随机数以及第三随机数，使用预设的密钥导出函数计算出一会话主密钥，记为第一会话主密钥，使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第

四随机数的MAC值，记为第五MAC值，将所述第五MAC值发送给所述服务器；

[0023] 所述第二处理单元还用于所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第六MAC值发送给所述客户端，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥；

[0024] 所述第一处理单元还用于当所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立。

[0025] 一方面，提供了一种基于前述建立的SSL连接的通信方法，所述方法包括：

[0026] 所述客户端使用所述第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值，将所述第七MAC值发送给服务器；

[0027] 所述服务器接受到所述客户端的第七MAC值后，使用所述第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值，将所述第八MAC值发送给客户端；

[0028] 所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器；

[0029] 所述服务器接受到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据，并将所述第四密文发送给所述客户端；

[0030] 所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八MAC值相同时，对所述第四密文进行解密以得到所述服务器数据，从而完成一次通信。

[0031] 一方面，提供了一种基于SSL连接的通信装置，所述装置包括：

[0032] 第三处理单元，用于客户端使用第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值，将所述第七MAC值发送给服务器；

[0033] 第四处理单元，用于服务器接受到所述客户端的第七MAC值后，使用所述第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值，将所述第八MAC值发送给客户端；

[0034] 所述第三处理单元还用于所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器；

[0035] 所述第四处理单元还用于所述服务器接受到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据，并将所述第四密文发送给所述客户端；

[0036] 所述第三处理单元还用于所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八MAC值相同时，对所述第四密文进行解密以得到所述服务器数据，从而完成一次通信。

[0037] 本发明实施例在客户端和服务器之间建立SSL连接的过程中引入联锁机制，客户端和服务器首先分别收到密文数据对应的MAC值，再收到密文数据，之后分别计算收到加密

后消息密文数据的MAC值，通过对比判断是否有中间人攻击，从而保证了后续生成的会话主密钥的安全性，有效地避免了中间人攻击。

## 附图说明

[0038] 图1是本发明实施例一提供的SSL连接的建立方法的实现流程图；

[0039] 图2是本发明实施例二提供的SSL连接的建立装置的结构图；

[0040] 图3是本发明实施例三提供的基于SSL连接的通信方法的实现流程图；以及

[0041] 图4是本发明实施例四提供的基于SSL连接的通信装置的结构图。

## 具体实施方式

[0042] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0043] 以下结合具体实施例对本发明的具体实现进行详细描述：

[0044] 实施例一：

[0045] 图1示出了本发明实施例一提供的SSL连接的建立方法的实现流程，详述如下：

[0046] 在步骤S101中，客户端向服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数。

[0047] 在本发明实施例中，客户端可以是浏览器，也可以是其他可连接到Web服务的专用客户端。当客户端连接到服务器时，向服务器发出建立SSL连接的请求消息，该请求消息中包括客户端最高可支持的SSL协议的版本号、会话标识、客户端支持的密码套件列表、压缩算法列表和用作产生密钥的随机数等参数，在这里将该随机数记为第一随机数。

[0048] 在步骤S102中，所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数。

[0049] 在本发明实施例中，第二随机数由服务器生成，以用于后续的主密钥的生成，在具体实施例中，服务器证书和第二随机数可以分别发送。为了简化通信过程，优选地，生成的第二随机数和服务器证书在一个响应消息中发送给客户端，从而减少握手过程中的通信次数。另外，服务器消息中还可以包括服务器根据接收的SSL版本号选择的SSL版本号、从客户端的密码套件列表中选择的一个密码套件、从客户端的压缩算法列表中选择的压缩方法。

[0050] 在步骤S103中，所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值。

[0051] 在本发明实施例中，客户端接收到响应消息后，请求服务器证书的证书授权中心(Certificate Authority,CA)对服务器证书进行认证，以保证服务器证书的有效性和安全性。认证成功后，客户端生成一随机数，将该随机数记为第三随机数，客户端使用服务器证书的公钥对包含第三随机数的消息进行加密以得到一密文，将该密文记为第一密文，计算第一密文的消息鉴别码(Message Authentication Code,MAC)值，将该MAC值记为第一MAC值，最后客户端将第一MAC值发送给服务器。

[0052] 其中，在计算第一密文的MAC值时，客户端将服务器证书的公钥作为密钥，使用服

务器发送过来的响应消息中选择的(即客户端与服务器协商得到的)单向散列函数对第一密文进行运算,从而得到第一MAC值。

[0053] 在步骤S104中,所述客户端将所述第一MAC值发送给所述服务器。

[0054] 在步骤S105中,所述服务器接收到所述第一MAC值后,生成第四随机数,使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文,计算所述第二密文的MAC值,将该MAC值记为第二MAC值。

[0055] 在本发明实施例中,同样地,服务器可将服务器证书的公钥作为密钥,使用其选择的单向散列函数计算所述第二MAC值。

[0056] 在步骤S106中,所述服务器将所述第二MAC值发送给所述客户端。

[0057] 在步骤S107中,所述客户端接收到所述第二MAC值后,将所述第一密文发送给所述服务器。

[0058] 在步骤S108中,所述服务器接收到所述第一密文后,计算所述第一密文的MAC值,记为第三MAC值,当所述第三MAC值与所述第一MAC值相同时,使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数。

[0059] 在步骤S109中,所述服务器将所述第二密文发送给所述客户端。

[0060] 在本发明实施例中,同样地,服务器将服务器证书的公钥作为密钥,使用其选择的单向散列函数计算所述第三MAC值。之后,服务器比较所述第三MAC值是否与所述第一MAC值相同,当所述第三MAC值与所述第一MAC值相同时,使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数,将所述第二密文发送给所述客户端。当所述第三MAC值和所述第一MAC值不相同时,所述服务器终止与所述客户端的通信,以保证服务器与客户端的通信安全。

[0061] 在步骤S110中,所述客户端接收到所述第二密文后,计算所述第二密文的MAC值,记为第四MAC值,当所述第四MAC值与所述第二MAC值相同时,使用所述服务器证书的公钥对所述第二密文进行解密以得到所述第四随机数,根据所述第一随机数、第二随机数以及第三随机数,使用预设的密钥导出函数计算出一会话主密钥,记为第一会话主密钥,使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值,记为第五MAC值。

[0062] 在步骤S111中,所述客户端将所述第五MAC值发送给所述服务器。

[0063] 在本发明实施例中,密钥导出函数根据步骤S101和S102中客户端和服务器协商确定的密码套件列表进行设置。

[0064] 在本发明实施例中,在步骤S103的客户端将第一MAC值发送给服务器的过程中,如果中间人截获第一MAC值后,只能虚构一个MAC值发送给服务器,而当步骤S107中客户端将第一密文发送给服务器时,由于中间人之前已经对第一MAC进行了伪造,当接收到第一密文时,解密获得消息后,也不也能再发送第一密文的内容,因此,中间人只能向服务器发送之前伪造出第一MAC的消息内容。同样,中间人截获服务器发送给客户端的第二MAC值和第二密文后,也只能虚构对应的MAC值和密文,这样,使得客户端和服务器的通信内容被打乱,客户端和服务器发现异常后终止会话,从而有效防止了中间人攻击。

[0065] 在步骤S112中,所述服务器根据所述第一随机数、第二随机数以及第三随机数,使用所述预设的密钥导出函数计算出一会话主密钥,记为第二会话主密钥,使用所述第二会

话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥。

[0066] 在步骤S113中，所述服务器将所述第六MAC值发送给所述客户端，

[0067] 在本发明实施例中，当所述第六MAC值和所述第五MAC值相同时，表明在前述通信中，并未受到中间人的攻击，SSL连接建立过程中的通信消息是完全、可靠的。当所述第六MAC值和所述第五MAC值不相同时，服务器终止与所述客户端的通信，以保证服务器的安全。

[0068] 在步骤S114中，所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立。

[0069] 在本发明实施例中，当客户端通过比较确定所述第六MAC值和所述第五MAC值不相同时，客户端终止与所述服务器的通信，以保证客户端的安全。在本发明实施例中，若SSL连接成功建立后，则所述第一会话密钥与所述第二会话密钥相同。

[0070] 本发明实施例在客户端和服务器之间建立SSL连接的过程中引入联锁机制，客户端和服务器首先分别收到密文数据对应的MAC值，再收到密文数据，之后分别计算收到加密后消息密文数据的MAC值，通过对比判断是否有中间人攻击，从而保证后续生成的会话主密钥的安全性，有效地避免了中间人攻击。

[0071] 实施例二：

[0072] 图2示出了本发明实施例二提供的SSL连接的建立装置2的结构，为了便于说明，仅示出了与本发明实施例相关的部分，其中，SSL连接的建立装置2包括下述单元：

[0073] 请求消息发送单元2101，用于所述客户端向所述服务器发送建立SSL连接的请求消息，所述请求消息包含生成的第一随机数；

[0074] 响应消息返回单元2201，用于所述服务器向所述客户端返回所述请求消息的响应消息，所述响应消息包含服务器证书以及生成的第二随机数；

[0075] 第一处理单元2102，用于所述客户端通过公钥基础设施对所述服务器证书进行认证，认证成功后，使用所述服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算所述第一密文的MAC值，将该MAC值记为第一MAC值，将所述第一MAC值发送给所述服务器；

[0076] 第二处理单元2202，用于所述服务器接收到所述第一MAC值后，生成第四随机数，使用所述服务器证书的私钥对包含所述第四随机数的消息进行加密以得到第二密文，计算所述第二密文的MAC值，将该MAC值记为第二MAC值，将所述第二MAC值发送给所述客户端；

[0077] 所述第一处理单元2102还用于当所述客户端接收到所述第二MAC值后，将所述第一密文发送给所述服务器；

[0078] 所述第二处理单元2202还用于当所述服务器接收到所述第一密文后，计算所述第一密文的MAC值，记为第三MAC值，当所述第三MAC值与所述第一MAC值相同时，使用所述服务器证书的私钥对所述第一密文进行解密以得到所述第三随机数，将所述第二密文发送给所述客户端；

[0079] 所述第一处理单元2102还用于当所述客户端接收到所述第二密文后，计算所述第二密文的MAC值，记为第四MAC值，当所述第四MAC值与所述第二MAC值相同时，使用所述服务

器证书的公钥对所述第二密文进行解密以得到所述第四随机数，根据所述第一随机数、第二随机数以及第三随机数，使用预设的密钥导出函数计算出一会话主密钥，记为第一会话主密钥，使用所述第一会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第五MAC值，将所述第五MAC值发送给所述服务器；

[0080] 所述第二处理单元2202还用于所述服务器根据所述第一随机数、第二随机数以及第三随机数，使用所述预设的密钥导出函数计算出一会话主密钥，记为第二会话主密钥，使用所述第二会话主密钥计算所述请求消息、所述响应消息、所述第一密文以及所述第四随机数的MAC值，记为第六MAC值，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值和所述第五MAC值相同时，将所述第六MAC值发送给所述客户端，将所述第二会话主密钥设置为与所述客户端进行后续通信的主密钥；

[0081] 所述第一处理单元2102还用于当所述客户端接收到所述第六MAC值后，比较所述第六MAC值与所述第五MAC值，当所述第六MAC值与所述第五MAC值相同时，将所述第一会话主密钥设置为与所述客户端进行后续通信的主密钥，从而完成所述SSL连接的建立。

[0082] 在具体的实施例中，所述请求消息发送单元2101和所述第一处理单元2102可位于客户端中，所述响应消息返回单元12和所述第二处理单元2202可位于服务器中，以用于在客户端和服务器之间建立SSL连接。

[0083] 具体地，所述第一处理单元2102可包括：

[0084] 第一MAC值计算单元21021，用于将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第一MAC值；

[0085] 所述第二处理单元2202可以包括：

[0086] 第二MAC值计算单元22021，用于将所述服务器证书的公钥作为密钥，使用所述响应消息中选择的单向散列函数计算所述第二MAC值。

[0087] 本发明实施例提出了一种SSL连接的建立装置，该装置在客户端和服务器之间建立SSL连接的过程中引入了联锁机制，客户端和服务器首先分别收到利用服务器公钥或私钥加密后消息密文数据对应的MAC值，再收到加密后消息密文数据，之后分别计算收到加密后消息密文数据的MAC值，通过对比判断是否有中间人攻击，从而保证了后续生成的会话主密钥的安全性，有效地避免了中间人攻击。

[0088] 实施例三：

[0089] 图3示出了本发明实施例三提供的基于实施一建立的SSL连接的通信方法的实现流程，详述如下：

[0090] 在步骤S301中，客户端使用第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值。

[0091] 在步骤S302中，客户端将所述第七MAC值发送给服务器。

[0092] 在本发明实施例中，待传送的客户端数据段可以为客户端待发送的请求信息或数据。当通过本发明实施例一中的方法建立SSL连接后，客户端和服务器之间开始进行通信。首先使用客户端生成的第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，之后，使用SSL连接建立过程中与服务器协商的单向散列函数对第三密文进行运算，得到第三密文的MAC值。

[0093] 在步骤S303中，所述服务器接受到所述客户端的第七MAC值后，使用所述第二会话

主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值。

[0094] 在步骤S304中，所述服务器将所述第八MAC值发送给客户端。

[0095] 在本发明实施例中，待发送的服务器数据段可以为服务器发送给客户端的响应消息或数据。

[0096] 在步骤S305中，所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器。

[0097] 在步骤S306中，所述服务器接受到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据。

[0098] 在步骤S307中，所述服务器将所述第四密文发送给所述客户端。

[0099] 在步骤S308中，所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八MAC值相同时，对所述第四密文进行解密以得到所述服务器数据，从而完成一次通信。

[0100] 在本发明实施例中，为了进一步提高客户端和服务器之间通信的安全性，在SSL连接的建立过程和数据传输过程中分别引入了联锁机制。如果在SSL连接的过程中有中间人的存在，会使得客户端和服务器生成的会话密钥不同，而本发明实施例中在后续数据传输的通信再使用联锁机制，同样由于中间人接收到MAC值后，不能获得原消息，只能进行伪造，使得客户端和服务器接收数据混乱，这样，中间人攻击可以更被容易地发现，同时，也不需要过多地改变基于SSL连接的通信模型。

[0101] 实施例四：

[0102] 图4示出了本发明实施例四提供的基于SSL连接的通信装置4的结构，为了便于说明，仅示出了与本发明实施例相关的部分。

[0103] 在本发明实施例中，基于SSL连接的通信装置4包括本发明实施例二中SSL连接的建立装置2的各个单元，在这里不再对SSL连接的建立装置2的各个单元进行描述。除了包括SSL连接的建立装置2的各个单元之外，所述通信装置4还包括：

[0104] 第三处理单元2103，用于客户端使用第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算所述第三密文的MAC值，记为第七MAC值，将所述第七MAC值发送给服务器。

[0105] 第四处理单元2203，用于服务器接受到所述客户端的第七MAC值后，使用所述第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算所述第四密文的MAC值，记为第八MAC值，将所述第八MAC值发送给客户端。

[0106] 所述第三处理单元2103还用于所述客户端接收到所述第八MAC值后，将所述第三密文发送给所述服务器。

[0107] 所述第四处理单元2203还用于所述服务器接受到所述第三密文后，计算所述第三密文的MAC值，记为第九MAC值，当所述第九MAC值与所述第七MAC值相同时，对所述第三密文进行解密以得到所述客户端数据，并将所述第四密文发送给所述客户端。

[0108] 所述第三处理单元2103还用于所述客户端计算所述第四密文的MAC值，记为第十MAC值，当所述第十MAC值与所述第八MAC值相同时，对所述第四密文进行解密以得到所述服

务器数据，从而完成一次通信。

[0109] 在具体的实施例中，所述第三处理单元2103位于客户端中，所述第四处理单元2203位于服务器中。

[0110] 在本发明实施例中，为了进一步提高客户端和服务器之间通信的安全性，在SSL连接的建立过程和数据传输过程中分别引入了联锁机制。如果在SSL连接的过程中有中间人的存在，会使得客户端和服务器生成的会话密钥不同，而本发明实施例中在后续数据传输的通信再使用联锁机制，同样由于中间人接收到密文和MAC值后，不能获得原消息，只能进行伪造，使得客户端和服务器接收数据混乱，这样，中间人攻击可以更被容易地发现，同时，也不需要改变基于SSL连接的通信模型。

[0111] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

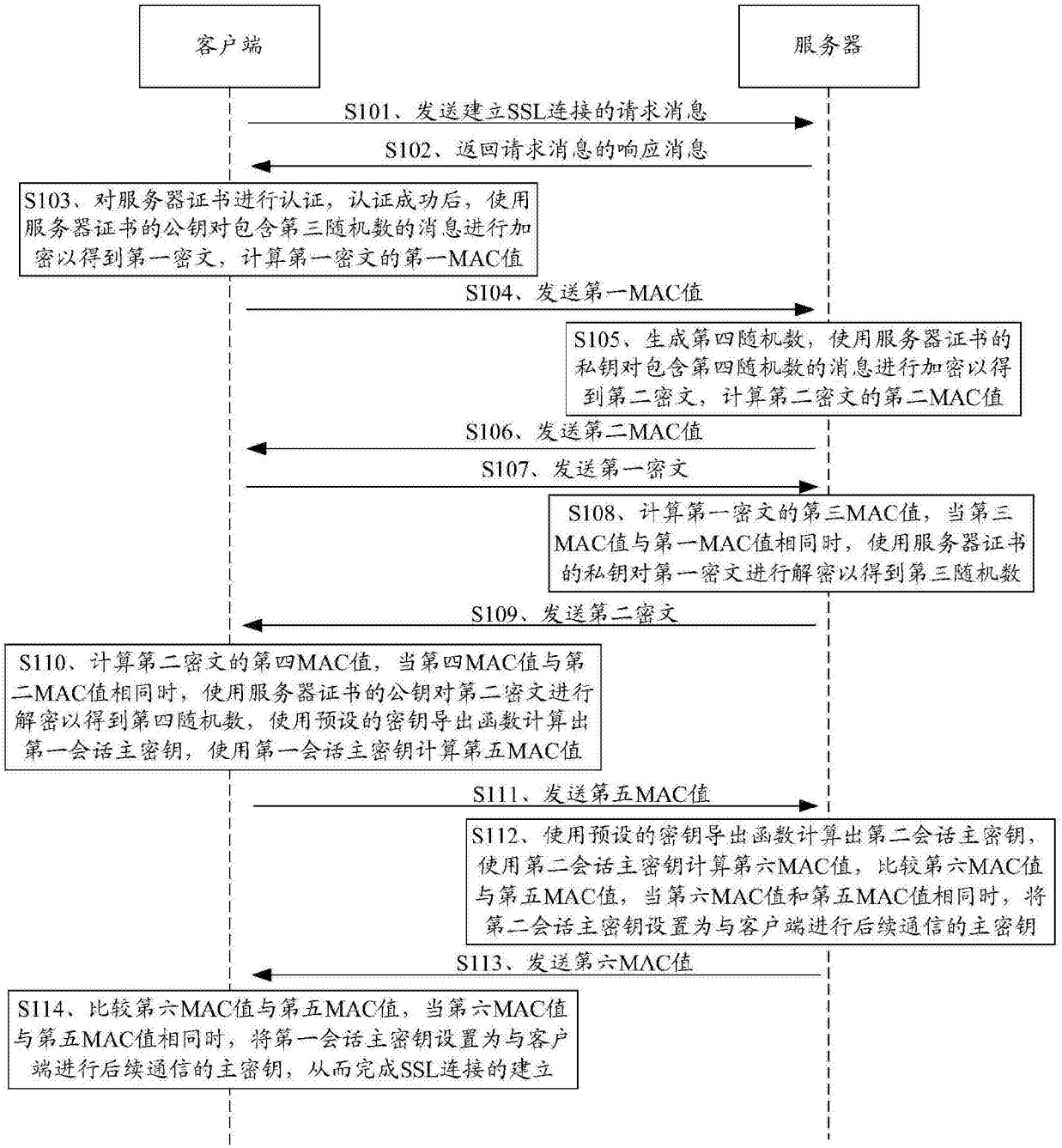

客户端
服务器
S101、发送建立SSL连接的请求消息
S102、返回请求消息的响应消息
S103、对服务器证书进行认证，认证成功后，使用服务器证书的公钥对包含第三随机数的消息进行加密以得到第一密文，计算第一密文的第一MAC值
S104、发送第一MAC值
S105、生成第四随机数，使用服务器证书的私钥对包含第四随机数的消息进行加密以得到第二密文，计算第二密文的第二MAC值
S106、发送第二MAC值
S107、发送第一密文
S108、计算第一密文的第三MAC值，当第三MAC值与第一MAC值相同时，使用服务器证书的私钥对第一密文进行解密以得到第三随机数
S109、发送第二密文
S110、计算第二密文的第四MAC值，当第四MAC值与第二MAC值相同时，使用服务器证书的公钥对第二密文进行解密以得到第四随机数，使用预设的密钥导出函数计算出第一会话主密钥，使用第一会话主密钥计算第五MAC值
S111、发送第五MAC值
S112、使用预设的密钥导出函数计算出第二会话主密钥，使用第二会话主密钥计算第六MAC值，比较第六MAC值与第五MAC值，当第六MAC值和第五MAC值相同时，将第二会话主密钥设置为与客户端进行后续通信的主密钥
S113、发送第六MAC值
S114、比较第六MAC值与第五MAC值，当第六MAC值与第五MAC值相同时，将第一会话主密钥设置为与客户端进行后续通信的主密钥，从而完成SSL连接的建立

图1

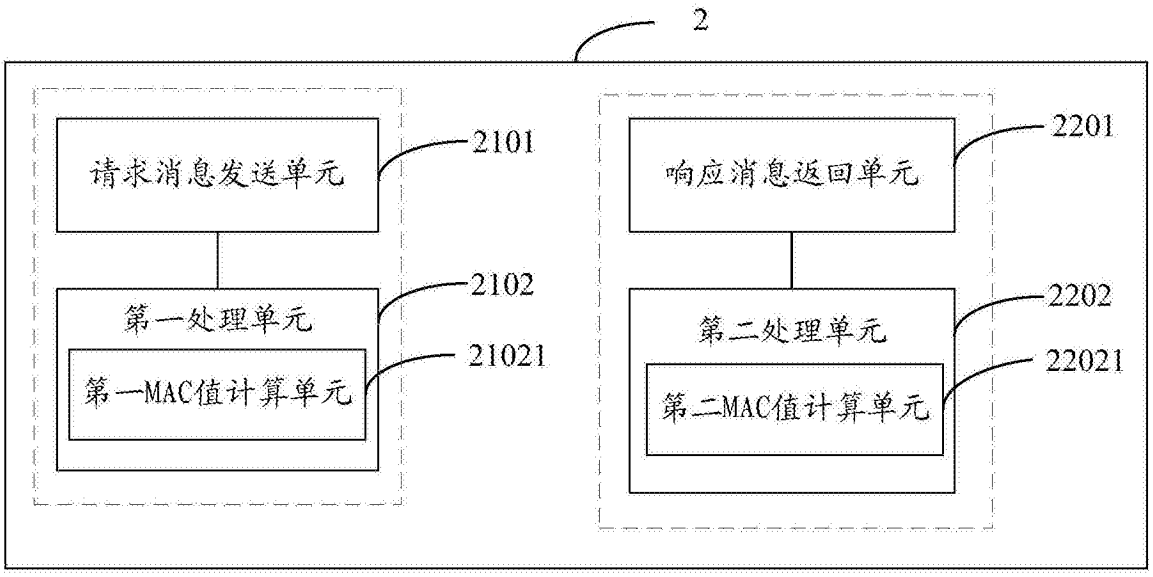

2
请求消息发送单元
2101
第一处理单元
2102
第一MAC值计算单元
21021
响应消息返回单元
2201
第二处理单元
2202
第二MAC值计算单元
22021

图2

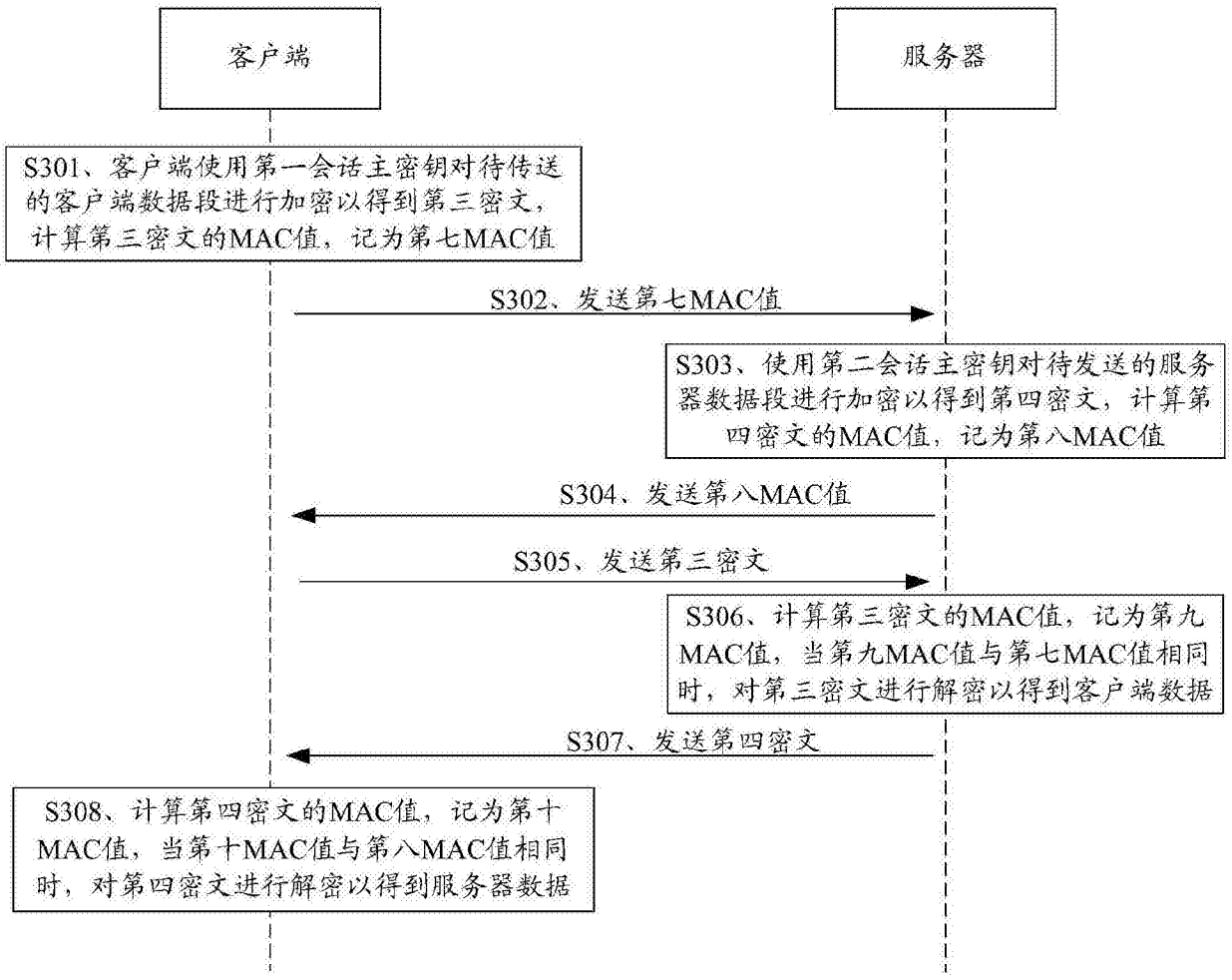

客户端
服务器
S301、客户端使用第一会话主密钥对待传送的客户端数据段进行加密以得到第三密文，计算第三密文的MAC值，记为第七MAC值
S302、发送第七MAC值
S303、使用第二会话主密钥对待发送的服务器数据段进行加密以得到第四密文，计算第四密文的MAC值，记为第八MAC值
S304、发送第八MAC值
S305、发送第三密文
S306、计算第三密文的MAC值，记为第九MAC值，当第九MAC值与第七MAC值相同时，对第三密文进行解密以得到客户端数据
S307、发送第四密文
S308、计算第四密文的MAC值，记为第十MAC值，当第十MAC值与第八MAC值相同时，对第四密文进行解密以得到服务器数据

图3

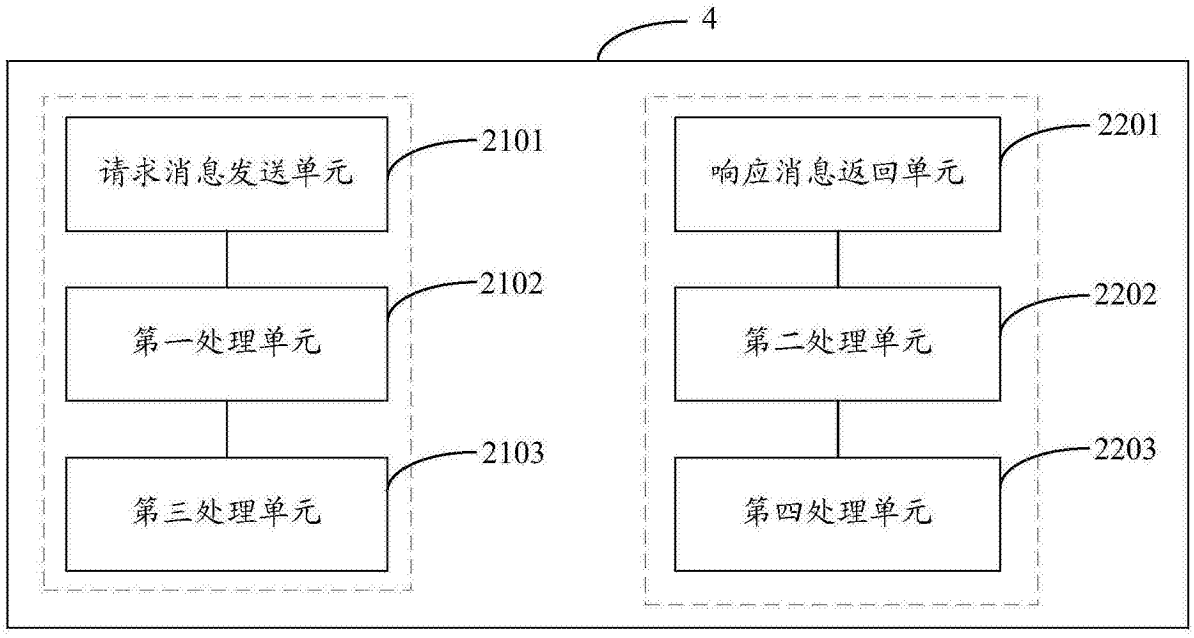

4
请求消息发送单元
2101
第一处理单元
2102
第三处理单元
2103
响应消息返回单元
2201
第二处理单元
2202
第四处理单元
2203

图4