安全即时通信软件设计文档

------信息安全课程设计

09 信息安全 陈新宇 董颖 蒋轩

安全即时通信软件设计文档

------信息安全课程设计

一、 项目名称：

安全即时通信软件

二、 开发背景：

随着计算机网络技术突飞猛进的发展，即时通信已成为目前互联网上最为流行的通信方式，深受广大网民的喜爱。无论是国内的腾讯 QQ 还是微软的 MSN Messenger，都拥有相当大的用户群。即时通信软件给人们带来了极大的便利，使人们可以随时随地地和亲朋好友进行在线交流和沟通，它拉近了人与人之间的距离，丰富了人们的精神生活，正逐渐成为人们生活和工作中不可或缺的一部分。虽然即时通信软件层出不穷，但是大部分免费的即时通信软件都不开源，因此用户对于其安全状况一无所知，不能完全信赖，尤其对于重要隐私信息的传送。

本项目将利用现有的网络通信技术、数据库技术和信息安全技术，设计并实现一个新的安全网络即时通信软件。它在原有的即时通信系统的基础上，对用户进行身份验证，对通信内容进行加密，保证数据通信的即时性和安全性，同时，在局域网内使用还可以节省外网流量，提供信息与文件的快速可靠共享，为人们提供了更加安全值得信赖的即时通信平台。

三、 基本要求：

机密性（Confidentiality）：任何未授权者都无法理解经过加密得消息。

完整性（Integrity）：可以检测存储介质或传输过程中对加密消息的任何更改或讹误。

不可抵赖性（Nonrepudiation）：发送方不能抵赖先前发送了加密消息。

身份验证（Authentication）：发送方和接收方能够彼此确认对方的身份以及消息的起源和目的地。

四、 功能概述：

身份验证

身份验证是指在计算机和网络系统中，确认操作者身份的过程，也就是证实用户的真实身份与其所生成的身份是否符合的过程。本软件将通过对称和非对称加密算法组合实现身份验证，获得许可的用户方可登录系统与好友进行安全通信。

密钥协商

服务器与客户端或者客户端之间，在进行通信之前，需要安全协商二者进行后续加密通信时对称加密算法的会话密钥。

加密通信

- 安全文字通信

该功能模块是安全即时通信系统中最重要的一部分。用户在对话窗口的文字编辑区域输入想要发送的内容，加密后将消息发送给服务器，由服务器转发。

◆ 安全文件传送

用户选择要发送的文件，传送前采用 AES 加密机制，加密后将文件发送请求发送给服务器，由服务器转发给接收方。

◆ 安全语音通信

客户端将对另一客户端的语音请求加密后发送给服务器，服务器将请求转发给目的客户端，该客户端接受请求后两个客户端之间方可进行加密的语音通信。

◆ 安全视频通信

随着人们生活水平的提高，仅仅是文字和语音聊天已不能满足人们在线交流的需要，因此安全视频通信是即时通信系统应尽力完善的一个功能，系统将客户端之间的视频通信内容加密，安全地通过网络传输视频数据。

五、 整体架构：

在 Internet 上的聊天程序一般都是以服务器提供服务端连接响应，使用者通过客户端程序登录到服务器，就可以与登录在同一服务器上的用户交谈，这是一个面向连接的通信过程。因此，该即时通信软件要在 TCP/IP 环境下，实现服务器端和客户端两部分结构。

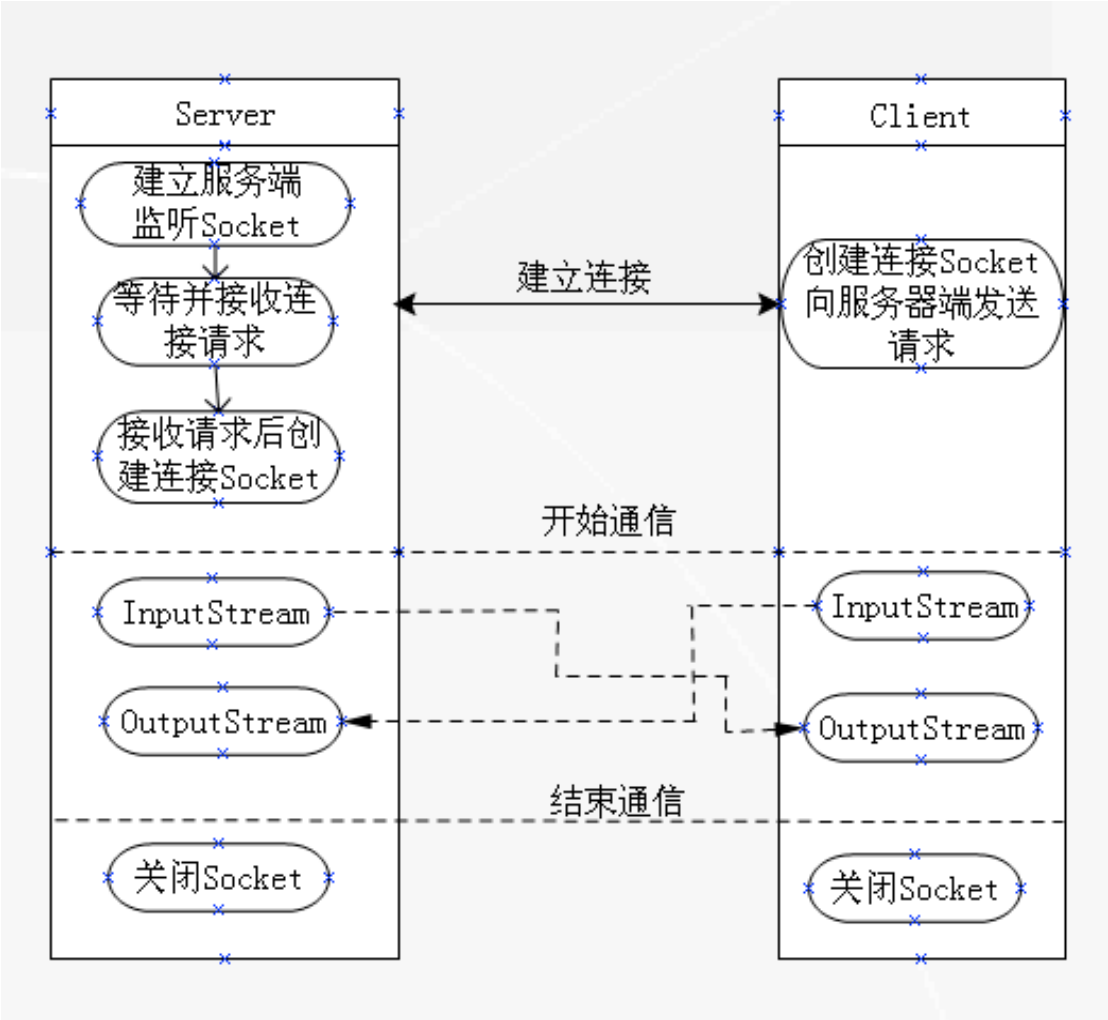


图 1 系统实现原理图

该安全即时通信软件采用 C/S 模式设计，主要包括客户端、服务器和数据库服务器三层，客户端提供用户注册账号、用户登录、安全通信等服务，服务器用来对注册登录的用户进行管理以及对客户端发送的请求信息做出相应处理，数据库服务器存放用户相关的用户表和好友表。它们之间的关系如图 1 所示：

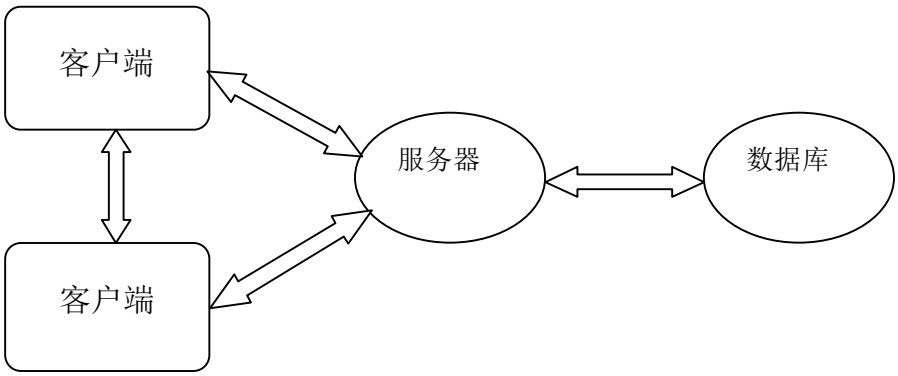


图 2 系统模型

服务器与客户端之间采用 TCP 协议进行可靠通信，使服务器可以随时掌控客户端的在线状态和运行情况。两个要求通信的客户端之间采用 UDP 协议直接进行通信。其总体结构如图 2 所示：

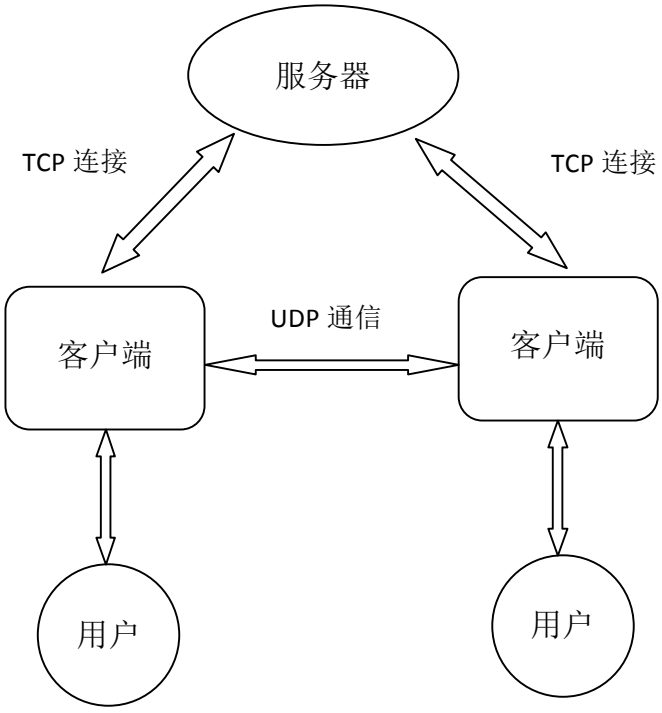


图 3 系统总体结构

八、功能层次图：

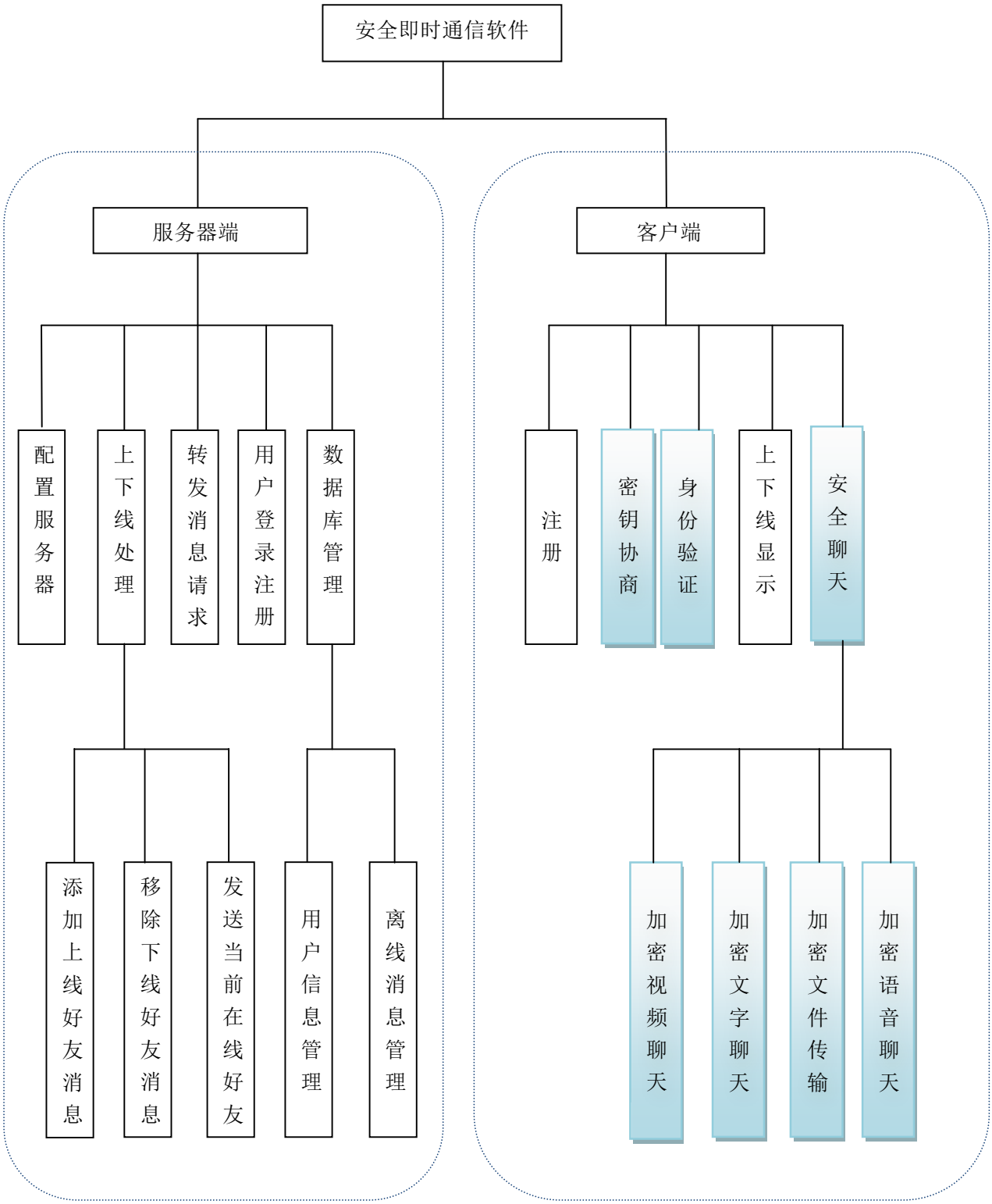


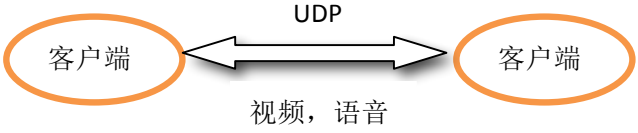
图 4 功能模块

九、详细设计：

1. 通信协议设计

TCP是面向连接的传输层协议，提供双向同时通信和可靠的数据传输。客户端和服务器之间使用的就是TCP协议。TCP每一条连接上的通信是一对一的，它提供错误控制，对乱序到达的报文进行重新排序，具有高可靠性，确保传输数据的正确性，不出现丢失或乱序。TCP采用字节流方式，即以字节为单位传输字节序列，具有紧急数据传送功能。由于该即时通信软件安全性要求很高，故客户端与服务器之间采用TCP协议就行加密后的通信。

UDP是无连接的传输层协议，UDP报文不需要确认，由于附加的控制信息少，传输效率比较高。UDP协议用来在互联网中提供包交换，它提供了向另一个用户程序发送信息的最简便的协议机制。在发送数据报文段之前不需要建立连接，它不支持拥塞控制，网络出现拥塞时就简单地丢掉数据单元，支持一对多、一对一、多对多和多对一的交互通信，因而具有资源消耗小，处理速度快的优点。UDP的首部很简单，只有8个字节，由源端口号、目的端口号、长度及校验和4个字段组成，每个字段都是2个字节。视频和语音通信很大程度上会受到网络状况的影响，故采用UDP协议进行加密后的，因为它们即使偶尔丢失一两个数据包，也不会对接收结果产生太大影响。

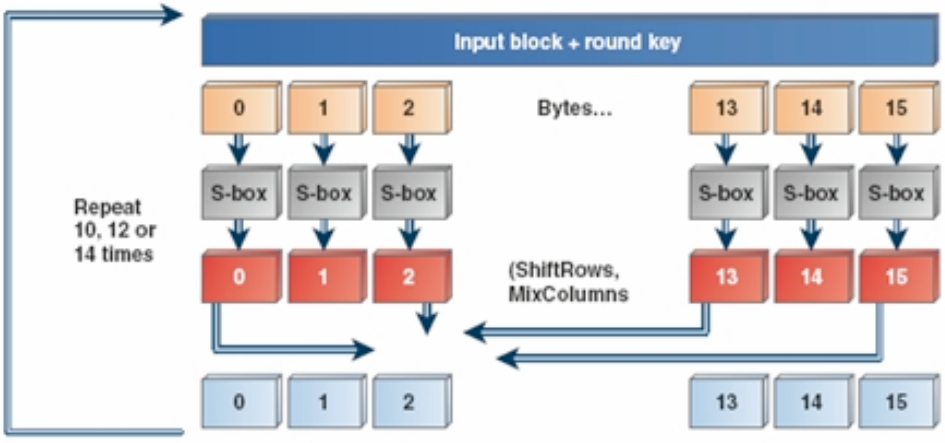


2. 加密算法

2.1 对称加密算法

对称密码体制以分组密码为重点。分组密码算法通常由密钥扩展算法和加密（解密）算法两部分组成。密钥扩展算法将 b 字节用户主密钥扩展成 r 个子密钥。加密算法由一个密码学上的弱函数 f 与 r 个子密钥迭代 r 次组成。混乱和密钥扩散是分组密码算法设计的基本原则。抵御已知明文的差分和线性攻击，可变长密钥和分组是该体制的设计要点。

AES 是美国国家标准技术研究所 NIST 旨在取代 DES 的 21 世纪的加密标准。AES 的基本要求是，采用对称分组密码体制，密钥长度的最少支持为 128、192、256，分组长度 128 位，算法应易于各种硬件和软件实现。



本软件将采用 AES 这种高级数据加密标准作为对称加密算法，用来加密通信内容。AES 加密数据块和密钥长度可以是 128 比特、192 比特、256 比特中的任意一个。AES 加密有很多轮的重复和变换。大致步骤如下：1、密钥扩展（KeyExpansion），2、初始轮（Initial Round），3、重复轮（Rounds），每一轮又包括：字节替换（SubBytes）、行变换（ShiftRows）、列混淆（MixColumns）、密钥加（AddRoundKey），4、 最终轮（Final Round），最终轮没有 MixColumns。

2.2 非对称加密算法

在公开密钥密码体制中，加密密钥（即公开密钥）PK 是公开信息，而解密密钥（即秘密密钥）SK 是需要保密的。加密算法 E 和解密算法 D 也都是公开的。虽然秘密密钥 SK 是由公开密钥 PK 决定的，但却不能根据 PK 计算出 SK。正是基于这种理论，1978 年出现了著名的 RSA 算法，它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA 密钥至少为 500 位长，一般推荐使用 1024 位。

本软件的公钥加密算法采用 RSA，RSA 是被研究得最广泛的公钥算法，其安全性依赖于大数分解，从提出到现在的三十多年里，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

2.3 哈希算法

本软件的设计中，用户密码需要用一种不可逆的加密算法保存。加密性强的散列一定是不可逆的，这就意味着通过散列结果，无法推出任何部分的原始信息。任何输入信息的变化，哪怕仅一位，都将导致散列结果的明显变化。 单向散列函数一般用于产生消息摘要，密钥加密等，常见的有 MD5（Message Digest Algorithm 5）和 SHA（Secure Hash Algorithm）。

SHA 是一种数据加密算法，现在已成为公认的最安全的散列算法之一，并被广泛使用。该算法输入报文的长度不限，将输入流按照每块 512 位（64 个字节）进行分块，并产生 20 个字节的信息摘要的输出。 SHA-1 是不可逆的、防冲突，并具有良好的雪崩效应。

SHA 与 MD5 的比较 ：

- **对强行攻击的安全性：**最显著和最重要的区别是 SHA 摘要比 MD5 摘要长 32 位，因此 SHA 对强行攻击有更大的强度。
- **对密码分析的安全性：**由于 MD5 的设计，易受密码分析的攻击，SHA 显然不易受这样的攻击。
- **速度：**在相同的硬件上，SHA的运行速度比MD5慢。

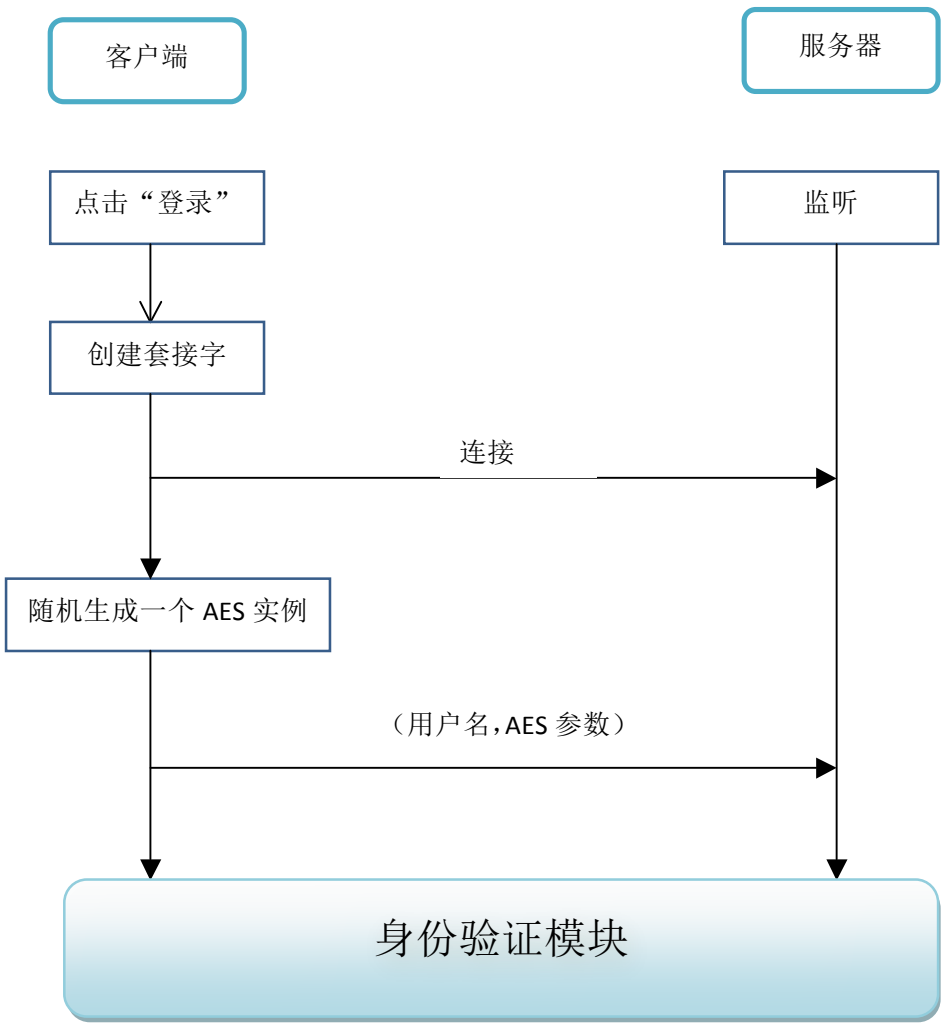
综合以上所述，本软件采用安全性更高的SHA散列算法来保存用户密码。

3. 核心安全模块设计

3.1 密钥协商模块

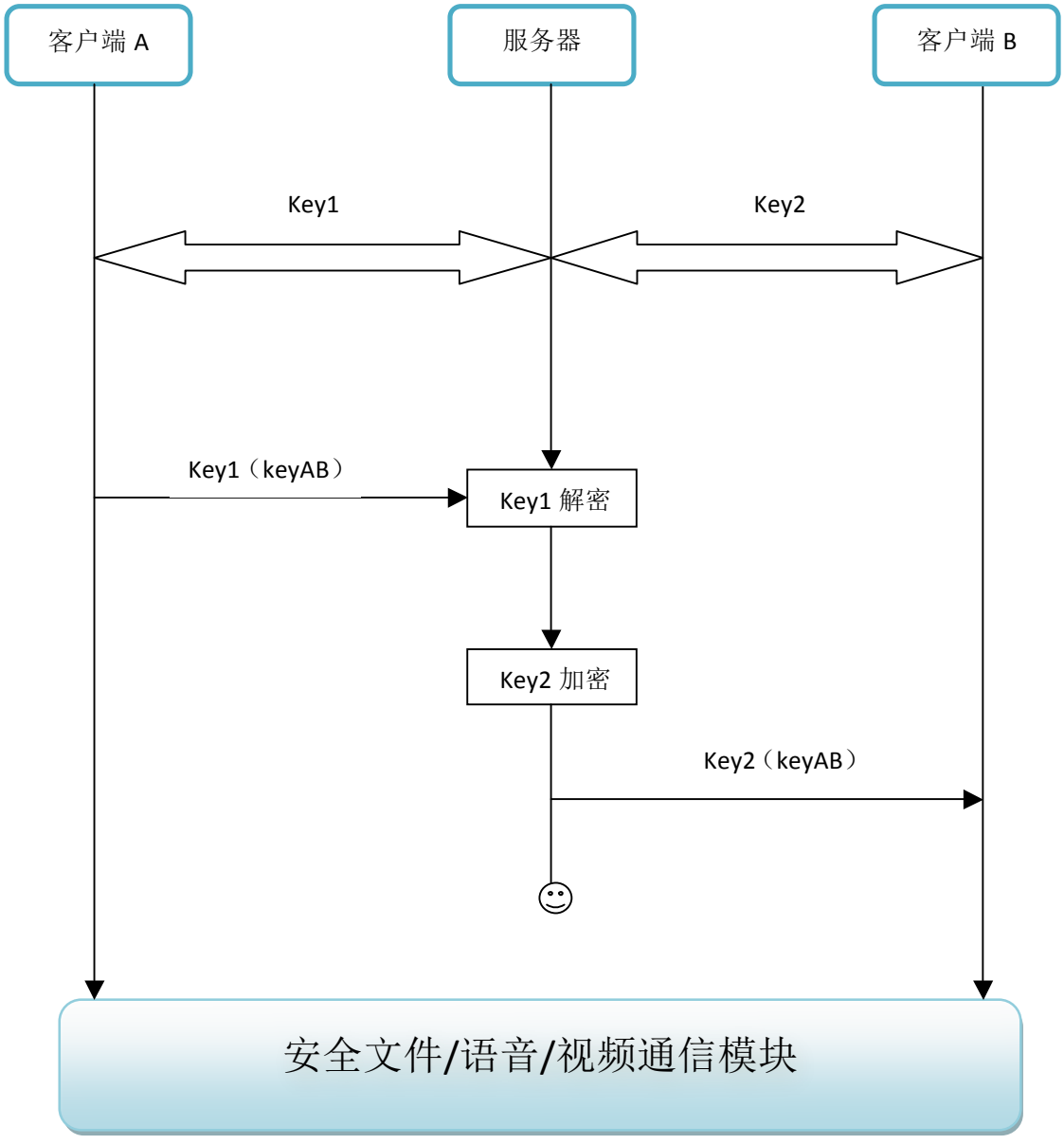
- **客户与服务器**

用户在登录窗口输完用户名以及密码，点击“登录”按钮后，触发创建套接字并连接服务器事件，连接建立后，随机生成一个加密算法 AES 的实例，并将用户名以及生成 AES 参数一起发送给服务器，其中，AES 参数中包含该客户端与服务器进行通信会话的私钥，然后进入身份验证模块。



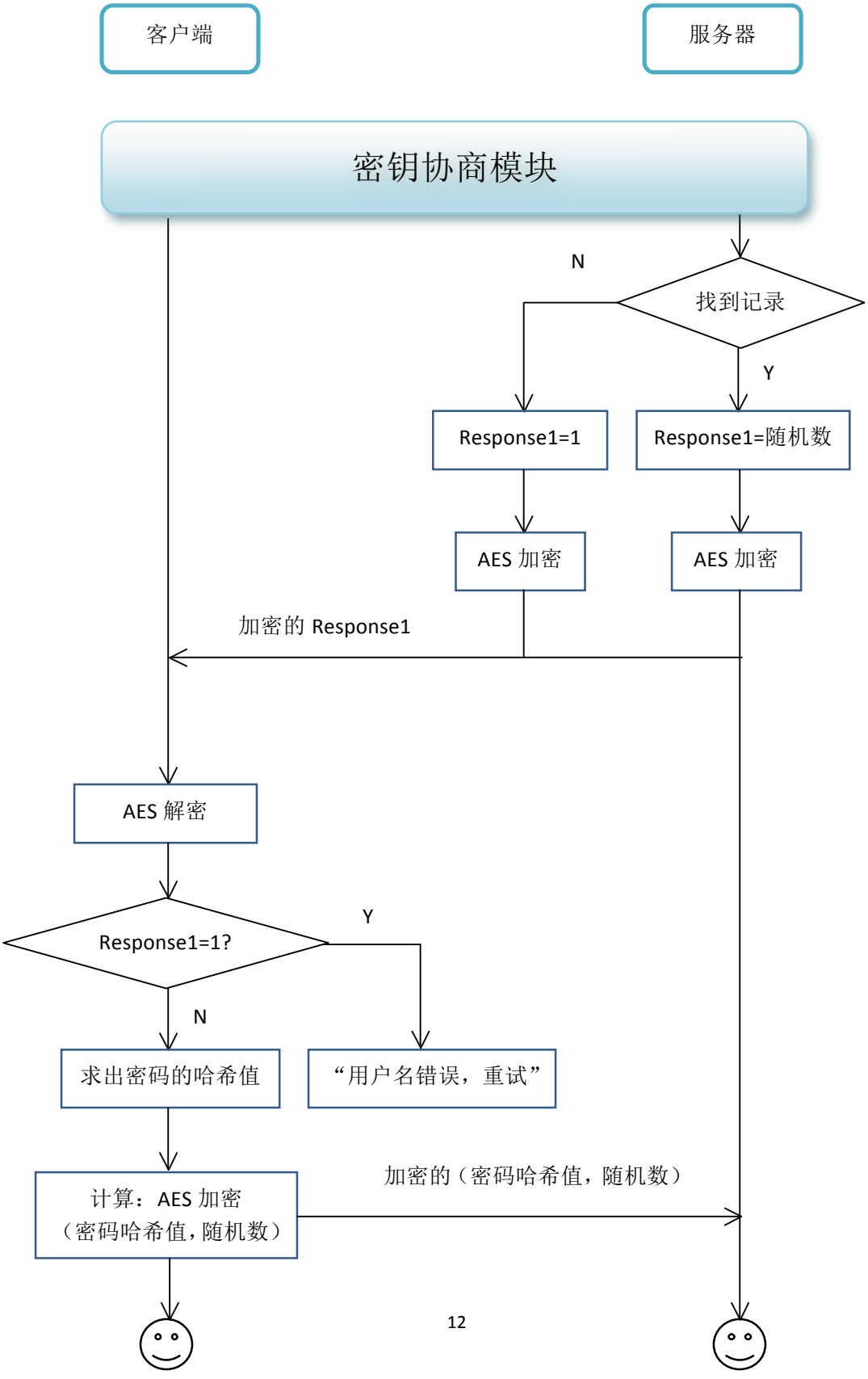
- **客户端之间**

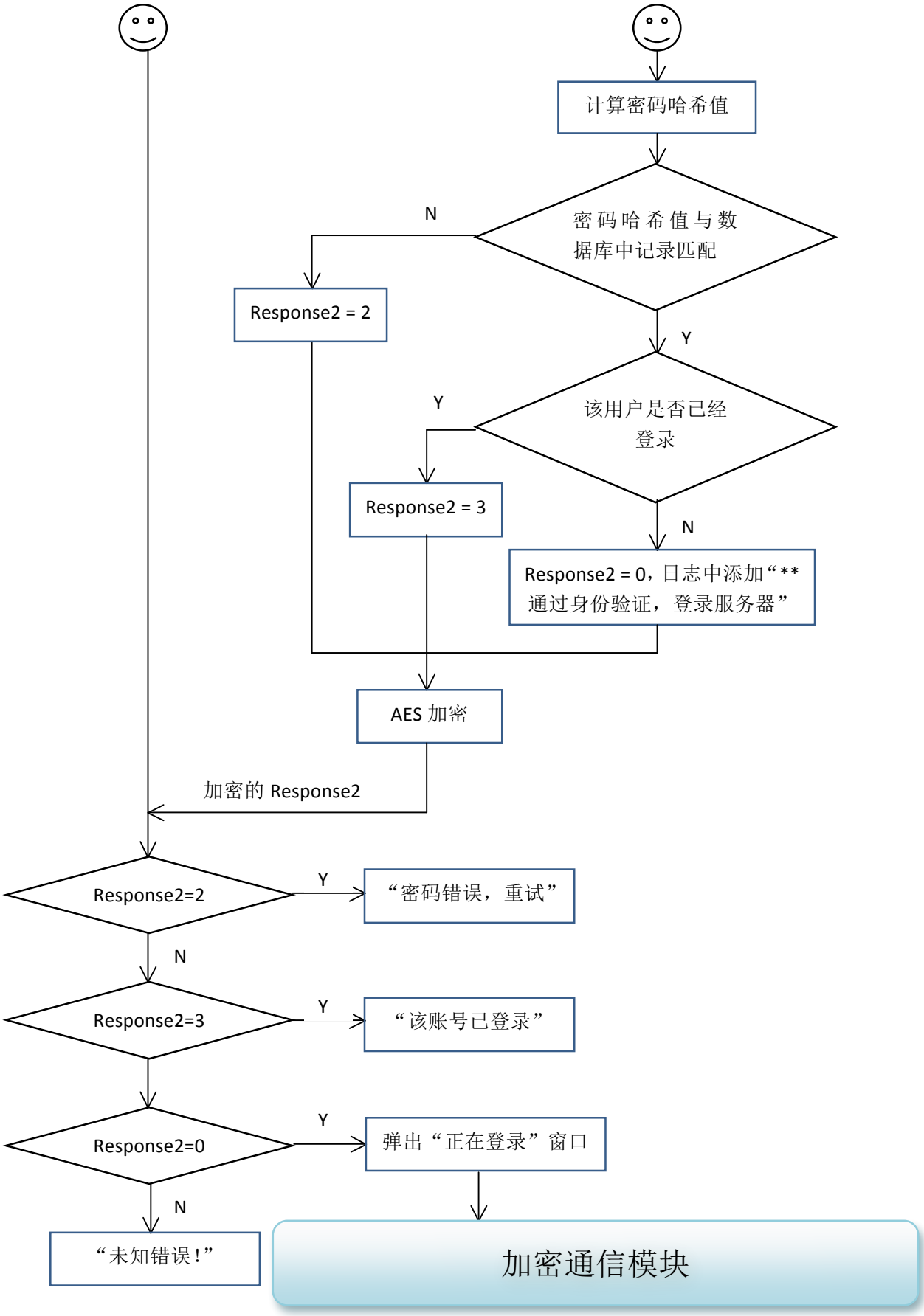
视频或语音请求的接收方客户端向服务器发出自己随机生成的 AES 实例的参数，其中包含会话密钥，服务器再转发给视频或者语音的请求发送方，待其收到会话密钥后客户端之间便可用该密钥进行加密通信。



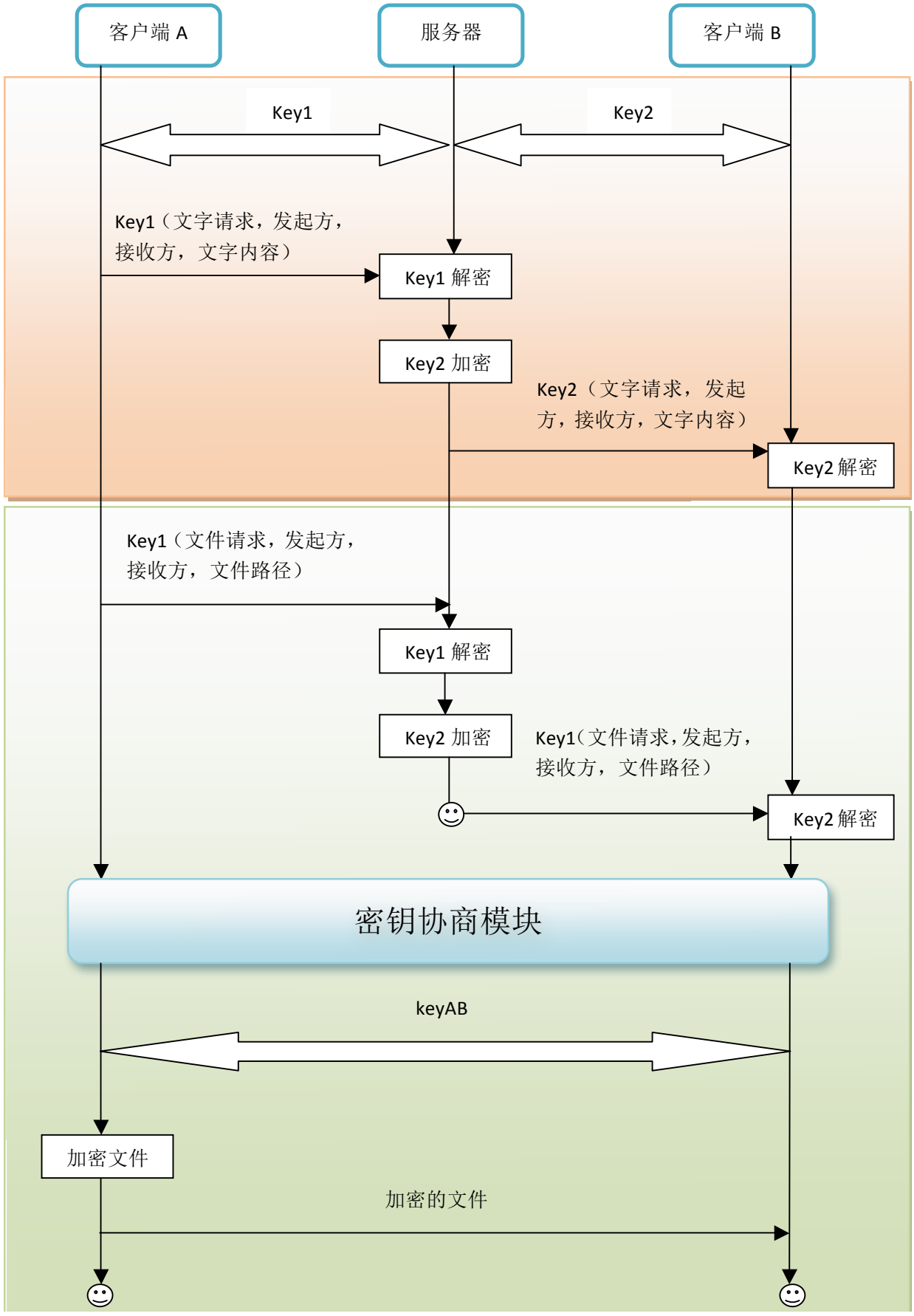
3.2 身份验证模块

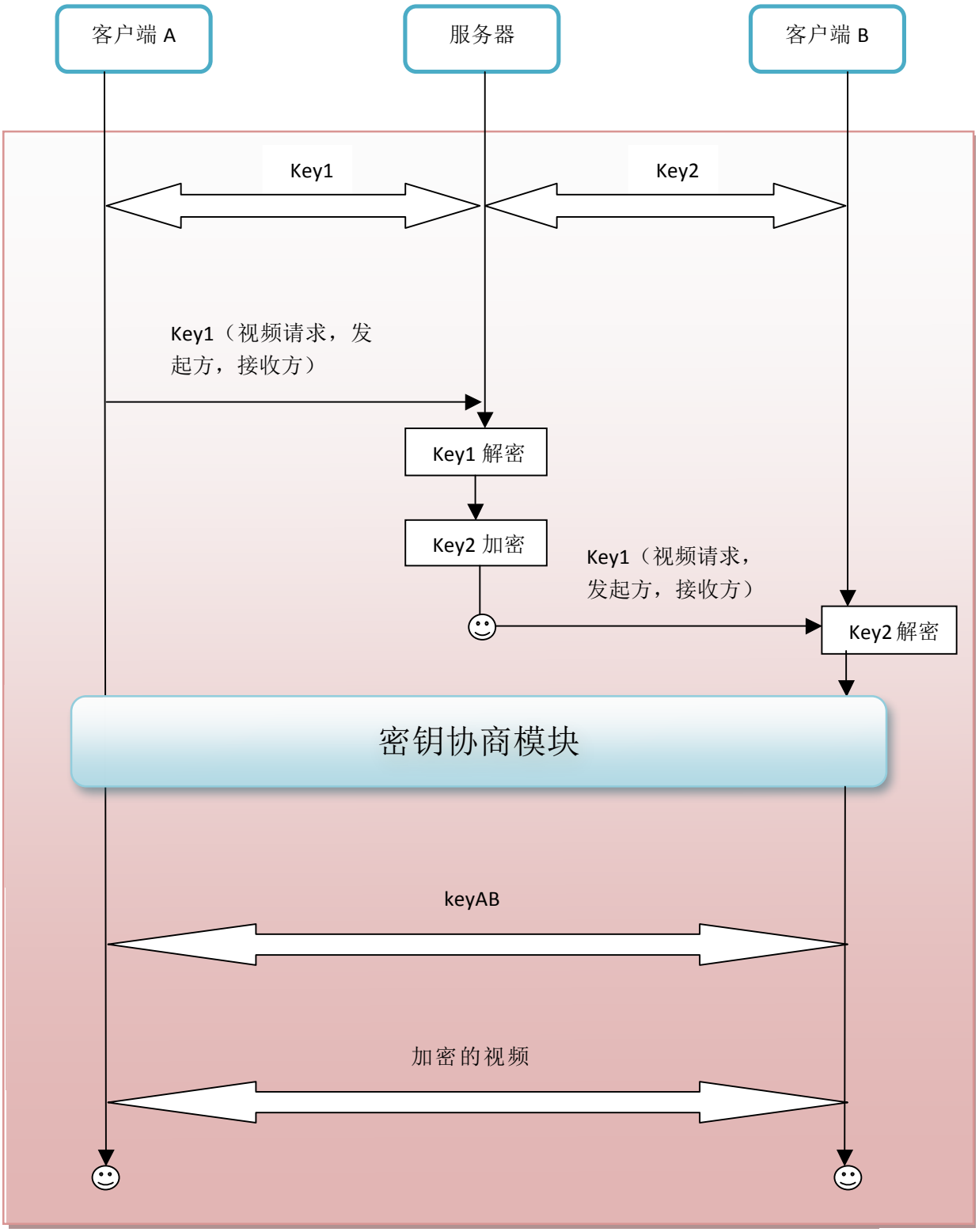
用户登录时先输入账号和密码，客户端与服务器建立连接，以挑战应答方式向服务器发送用户的登录信息，服务器在数据库中查找是否有该用户信息，若信息一致，则登陆成功。




计算密码哈希值
密码哈希值与数据库中记录匹配
N
Response2 = 2
Y
该用户是否已经登录
Y
Response2 = 3
N
Response2 = 0，日志中添加“** 通过身份验证，登录服务器”
AES 加密
加密的 Response2
Response2=2
Y
“密码错误，重试”
N
Response2=3
Y
“该账号已登录”
Response2=0
Y
弹出“正在登录”窗口
N
“未知错误!”
加密通信模块

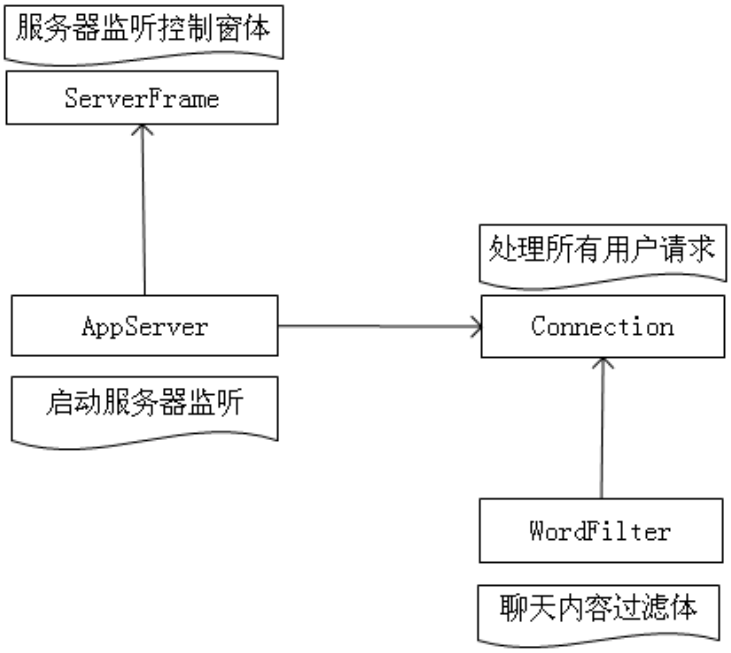
3.2 安全通信模块


客户端 A
服务器
客户端 B
Key1
Key2
Key1（文字请求，发起方，接收方，文字内容）
Key1 解密
Key2 加密
Key2（文字请求，发起方，接收方，文字内容）
Key2 解密
Key1（文件请求，发起方，接收方，文件路径）
Key1 解密
Key2 加密
Key1（文件请求，发起方，接收方，文件路径）
Key2 解密
密钥协商模块
keyAB
加密文件
加密的文件


客户端 A
服务器
客户端 B
Key1
Key2
Key1（视频请求，发起方，接收方）
Key1 解密
Key2 加密
Key1（视频请求，发起方，接收方）
Key2 解密
密钥协商模块
keyAB
加密的视频

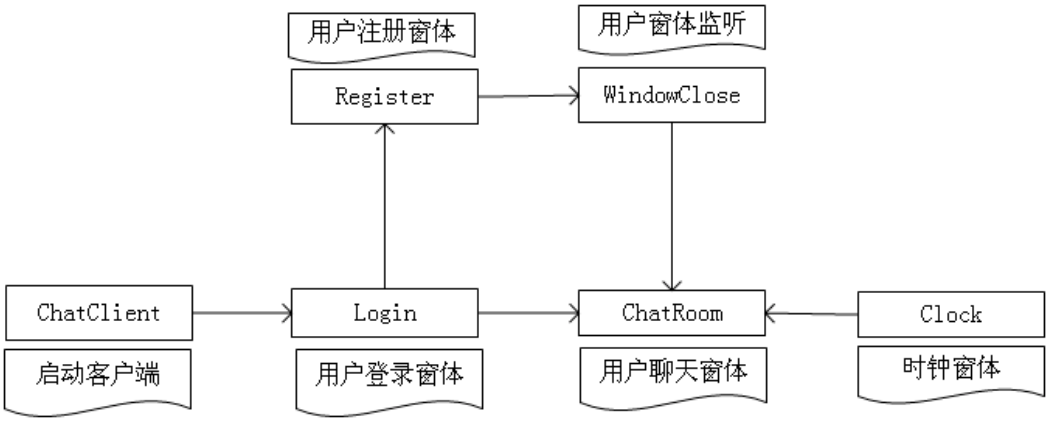
文件传输以及文字聊天以 TCP 为通信基础，防止信息丢失，传输过程实时显示在对应的窗口，可以实现同时传输多个文件到不同客户，也可以同时接收多个客户传来的文件，还可以自发自收传送文件，发送方和接收方都显示传输进度。

4． 服务器端结构



服务器主要完成建立连接、监听客户和操作数据库这 3 个功能。服务器首先得建立一个 Socket 连接，通过 TcpListener 不断侦听是否有客户端连接或者断开连接。服务器是一个信息发送中心，所有客户端的请求信息都发送到服务器，再由服务器根据要求做出相应处理并发送反馈信息。后台用数据库进行数据存取，数据库的数据操作包括写入用户信息，查找客户信息（密码哈希值）。

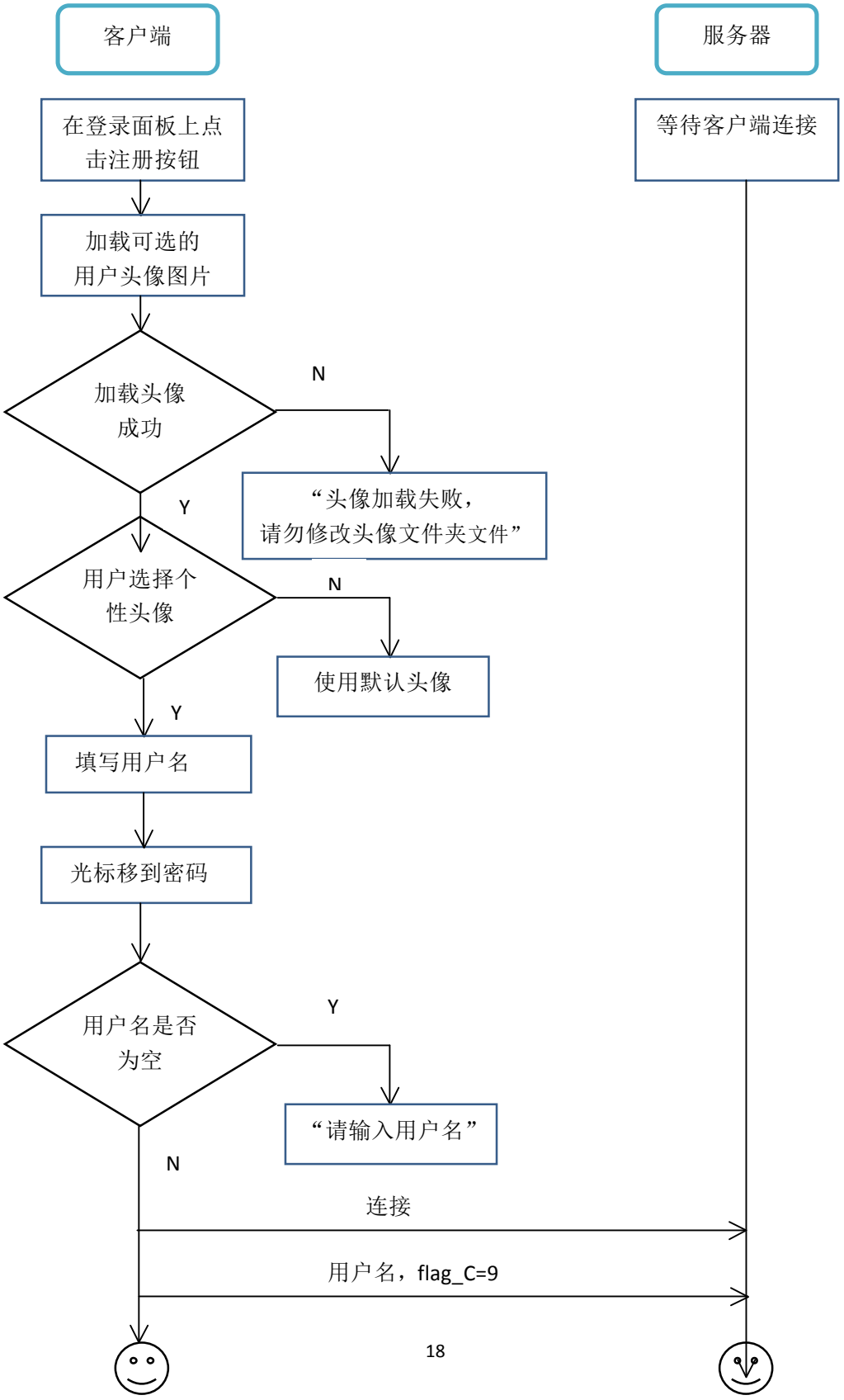
5.客户端结构

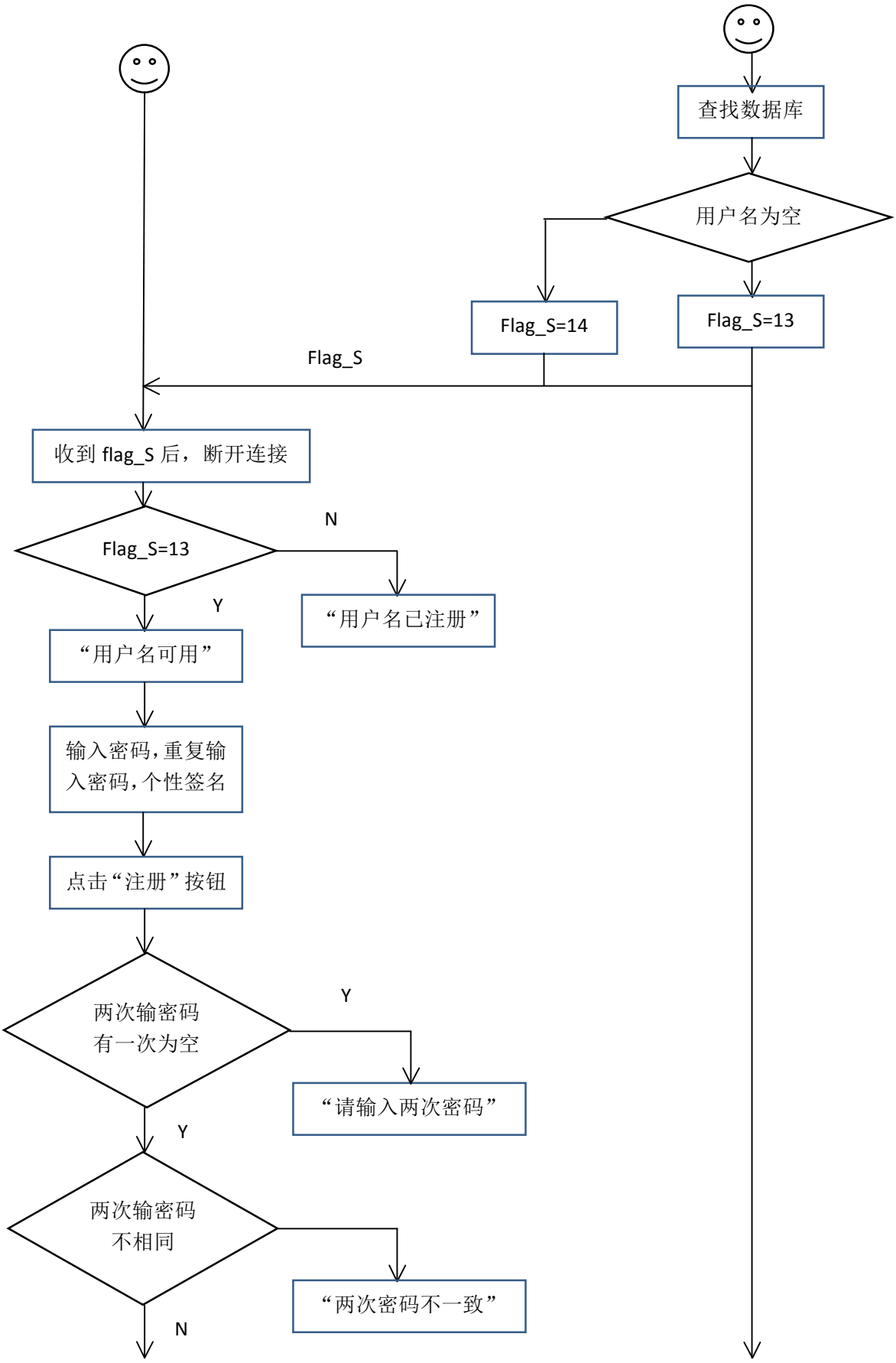


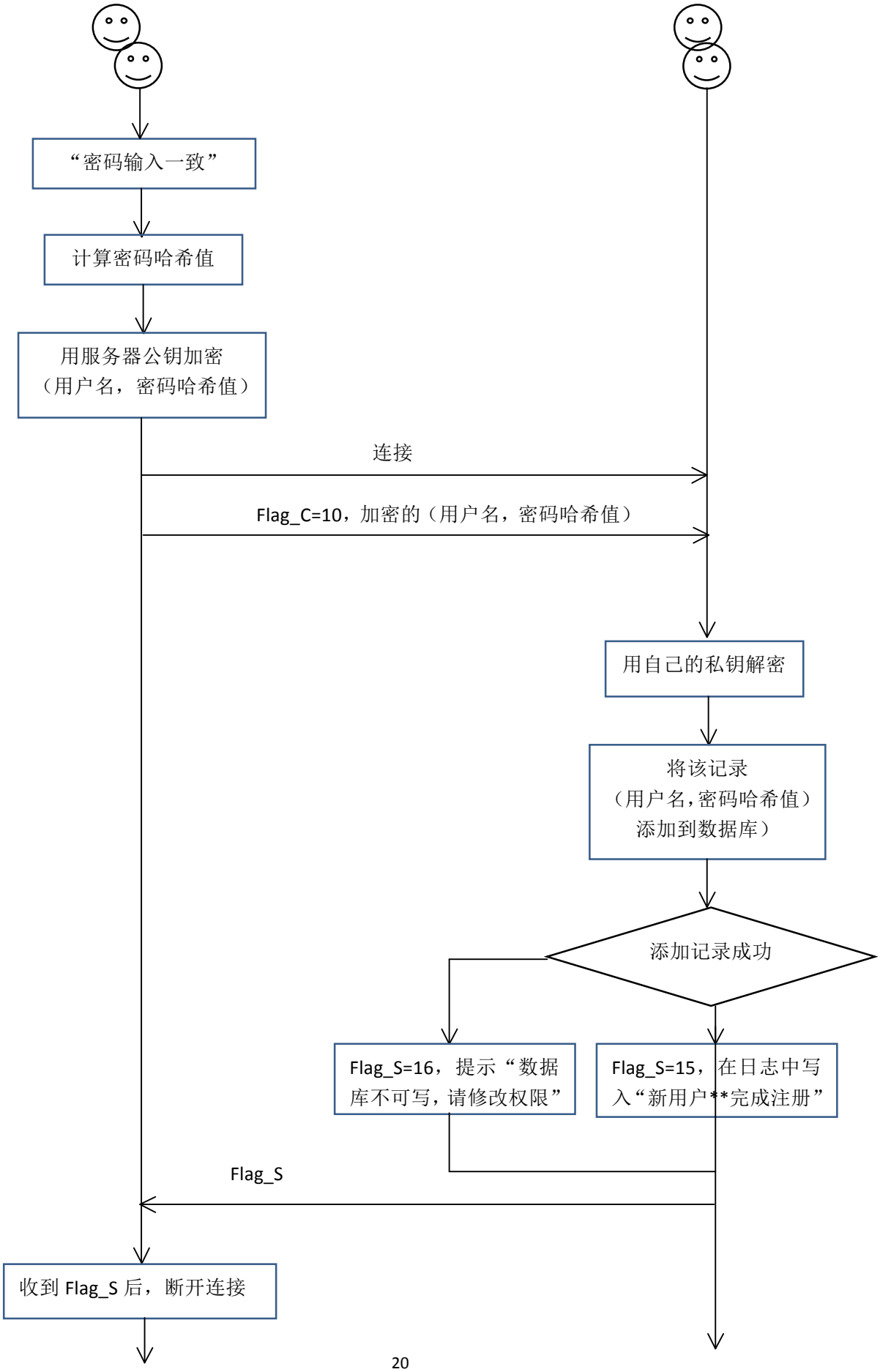
客户端需要完成账号注册、用户登陆、以及加密通信这 4 个功能。客户端可以查看好友的信息，添加好友后会给对方发送消息窗口，等待对方验证。两个客户端之间通过 UDP 协议进行直接通信，因而好友之间可以进行文字，语音，视频聊天和文件传输等。

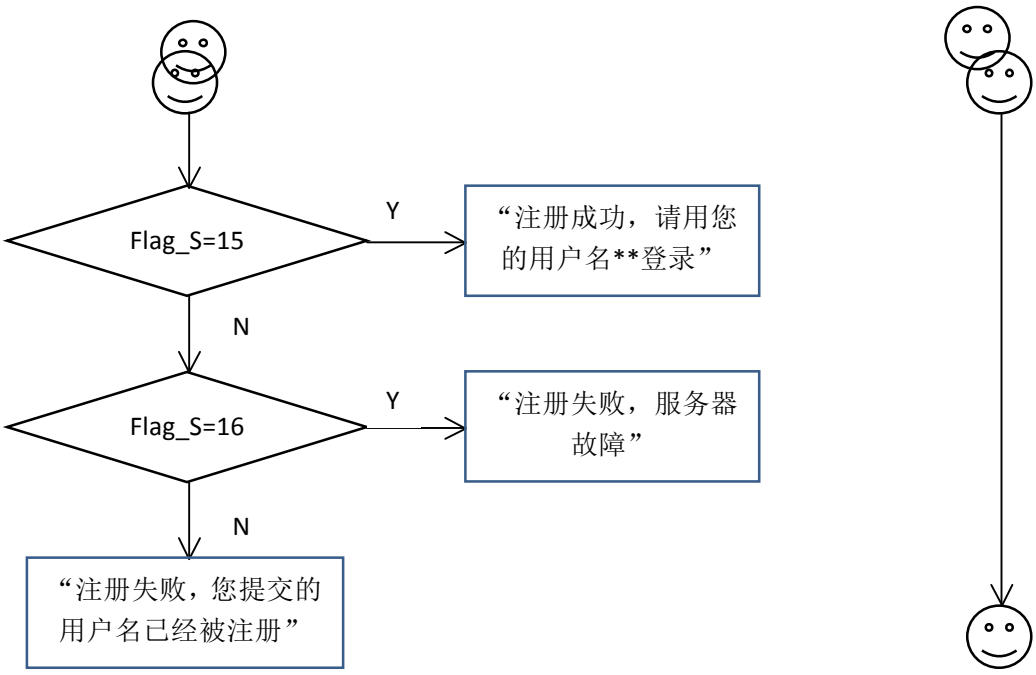
6. 其他模块

6.1 注册模块



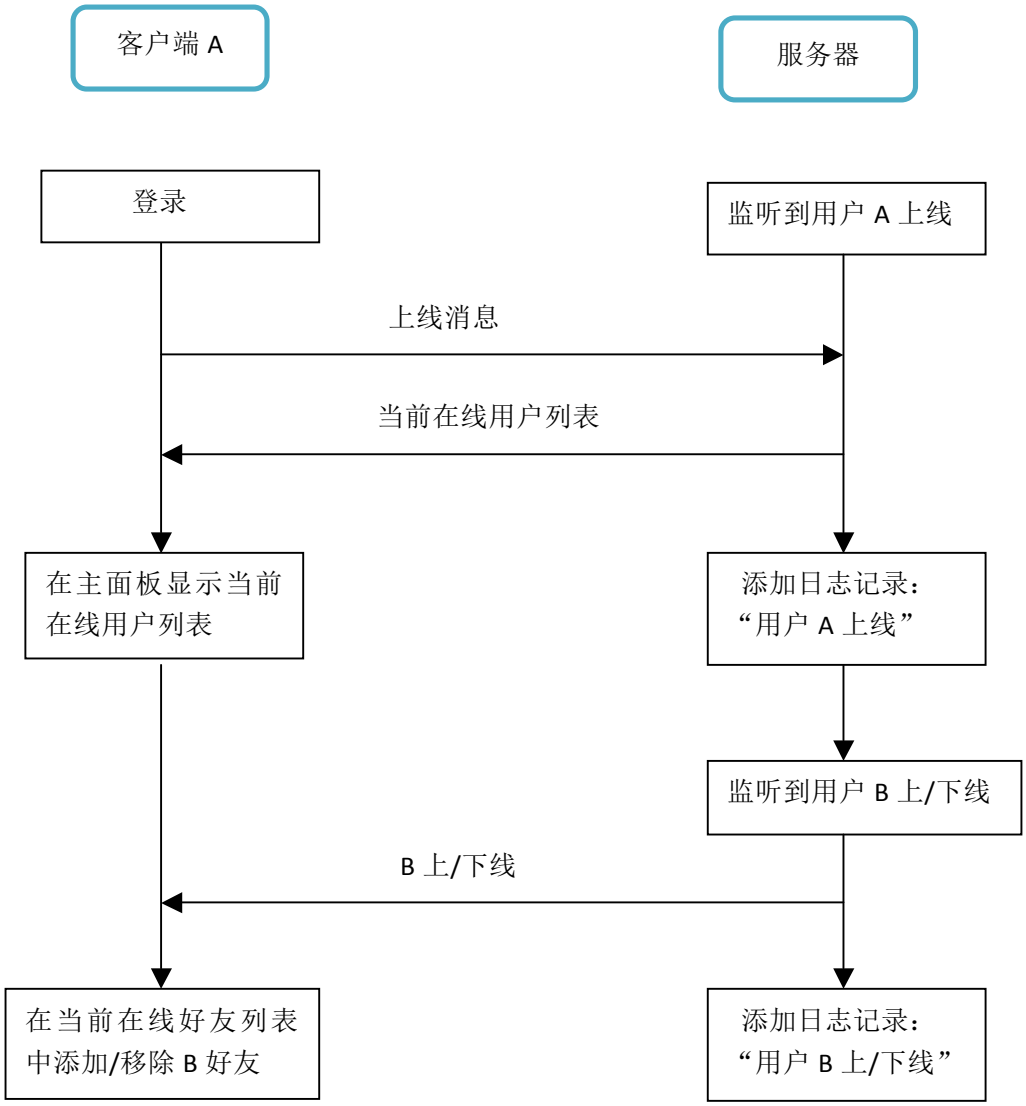

查找数据库
用户名为空
Flag_S=14
Flag_S=13
Flag_S
收到 flag_S 后，断开连接
Flag_S=13
N
“用户名已注册”
Y
“用户名可用”
输入密码，重复输入密码，个性签名
点击“注册”按钮
两次输密码有一次为空
Y
“请输入两次密码”
Y
两次输密码不相同
“两次密码不一致”
N


“密码输入一致”
计算密码哈希值
用服务器公钥加密
（用户名，密码哈希值）
连接
Flag_C=10，加密的（用户名，密码哈希值）
用自己的私钥解密
将该记录
（用户名，密码哈希值）
添加到数据库）
添加记录成功
Flag_S=16，提示“数据库不可写，请修改权限”
Flag_S=15，在日志中写入“新用户**完成注册”
Flag_S
收到 Flag_S 后，断开连接



当用户注册账号时，客户端与服务器建立连接，并向服务器发送新用户的申请信息，接收来自服务器的反馈信息进行注册。

6.2 其它循环消息处理


客户端 A
服务器
登录
监听到用户 A 上线
上线消息
当前在线用户列表
在主面板显示当前在线用户列表
添加日志记录：“用户 A 上线”
监听到用户 B 上/下线
B 上/下线
在当前在线好友列表中添加/移除 B 好友
添加日志记录：“用户 B 上/下线”

9. 数据库设计

数据库是安全网络即时通信系统的后台，存放着所有用户的信息，在安全网络即时通信系统中有着极其重要的作用。数据库设计的好坏直接影响到整个系统的运行效率。一个良好的数据库设计，可以提高数据信息的存储效率，保证数据信息的一致性和完整性。而且一个设计合理的数据库结构有助于程序的实现。本系统选用 SQL Server 2000 作为后台数据库。

本系统需要两张数据库表分别用来存放用户的注册信息以及用户的好友资料。在 SQL Server 2000 上新建一个名为 test 的数据库，并在 test 中建立两张数据库表：用户的基本信息表（表名 userio）和用户的好友表（表名 u_id）。

字段名称	数据类型	长度	主键	说明	允许空
username	nvarchar	100	✓	用户昵称	否
password	nvarchar	100		密码	是
headPic	int	4		用户头像编号	否
selfIntro	nvarchar	200		个性签名	是
offlineMsg	nvarchar	MAX		离线消息	是
pubKey	nvchar	1000		公钥	是
priAndPubKey	nvchar	1000			是

采用数据库的目的是保存用户的基本信息及好友信息，为用户之间的通信提供相关的数据服务，例如用户登录时，在登录窗口中输入用户账号和密码后，就需要和数据库中已有的用户信息进行比较，如果一致则登录成功，如果不一致则需要重新登录。基本的设计思路为首先建立一个用户基本信息表，这张表包括所有用户的详细信息，包括用户账号、用户昵称、密码、用户头像编号、在线状态等，当新用户注册时，将用户的基本信息记录该表内；在用户注册成功后，服务器就会自动生成一个该 用户的好友表，该表中存放着该用户添加的好友信息，在用户登录成功后，客户端主界面上的好友信息就来自用户的好友表，从而两个

在线的好友之间就可以进行通信了。