

<b>1 引言 .....</b>	<b>2</b>
1.1 编写目的.....	2
1.2 背景.....	2
1.3 定义.....	2
1.4 参考资料.....	2
<b>2 用途 .....</b>	<b>4</b>
2.1 功能.....	4
2.2 性能.....	4
2.2.1 精度.....	4
2.2.2 时间特性.....	4
2.2.3 灵活性.....	5
2.3 安全保密.....	错误!未定义书签。
<b>3 运行环境 .....</b>	<b>5</b>
3.1 硬设备.....	5
3.2 支持软件.....	6
3.3 数据结构.....	6
<b>4 使用过程 .....</b>	<b>6</b>
4.1 安装与初始化.....	6
4.2 输入.....	8
4.2.1 输入数据的现实背景.....	8
4.2.2 输入格式.....	8
4.2.3 输入举例.....	8
4.3 输出对每项输出作出说明.....	11
4.3.1 输出数据的现实背景.....	11
4.3.2 输出格式.....	11
4.3.3 输出举例.....	12
4.4 文卷查询.....	12
4.5 出错处理和恢复.....	12
4.6 终端操作.....	12

# 用户手册（GB8567——88）

## 1 引言

### 1.1 编写目的

编写这份用户手册旨在指导用户对软件的安装和使用进行了解以及使用。

### 1.2 背景

说明：

- a. 这份用户手册所描述的软件为一个在线聊天系统项目-----MaomaoChat
- b. 任务提出者：  
毛昌越

开发者：

毛昌越，姜佳豪

用户：

面向电脑用户、手机用户等互联网用户

### 1.3 定义

#### （1） Redis:

**Redis** is an open-source software project (sponsored by Redis Labs ) that implements data structure servers. It is networked, in-memory, and stores keys with optional durability.

#### （2） End-to-end encryption (E2EE):

**End-to-end encryption (E2EE)** is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation.

#### （3） Instant messaging:

**Instant messaging (IM)** is a type of online chat that offers real-time text transmission over the Internet.

#### （4） AES:

AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process.

## 1.4 参考资料

- a. [1]Daor J, Daemen J, Rijmen V. AES Proposal: Rijndael[J]. Vazirani: Efficient and Secure Pseudo-Random Number Generation. Proceedings, 25th IEEE FOCS, 1999.
- b. [2]Daemen J, Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard[J]. Springer-Verlag, 2002.
- c. [3] Wolkerstorfer J, Oswald E, Lamberger M. An ASIC Implementation of the AES SBoxes[C]// The Cryptographer's Track at the Rsa Conference on Topics in Cryptology. Springer-Verlag, 2002:67-78.
- d. [4] Feldhofer M, Dominikus S, Wolkerstorfer J. Strong Authentication for RFID Systems Using the AES Algorithm[M]// Cryptographic Hardware and Embedded Systems – CHES 2004. Springer Berlin Heidelberg, 2004:357-370.
- e. [5] Biryukov A, Khovratovich D. Related-Key Cryptanalysis of the Full AES-192 and AES-256[M]// Advances in Cryptology – ASIACRYPT 2009. Springer Berlin Heidelberg, 2009:1-18.
- f. [6] Canright D. A Very Compact S-Box for AES[J]. Lecture Notes in Computer Science, 2005, 3659:441-455.
- g. [7] Moradi A, Poschmann A, Ling S, et al. Pushing the Limits: A Very Compact and a Threshold Implementation of AES[C]// International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Springer-Verlag, 2011:69-88.
- h. [8] Manavski S A. CUDA Compatible GPU as an Efficient Hardware Accelerator for AES Cryptography[C]// IEEE International Conference on Signal Processing and Communications. IEEE, 2007:65-68.

## 2 用途

### 2.1 功能

- 用户注册
- 用户登录
- 添加好友
- 删除好友
- 添加群组
- 删除群组
- 创建群组
- 添加频道
- 删除频道
- 创建频道
- 发送文本消息
- 接收文本消息
- 发送离线消息
- 接收离线消息

### 2.2 性能

#### 2.2.1 精度

输入要求:

用户输入的信息等不能包含非法字符以及 SQL 注入等恶意操纵。

输出要求:

消息的发送与接收应该尽量即时。

所有字符使用 utf-8 作为编码，方便国际化的问题。

#### 2.2.2 时间特性

a. 响应时间:

并行处理软件客户端的相应时间应小于 3 秒。

b. 更新处理时间:

此软件的更新处理时间无要求。

c. 数据的转换和传送时间:

正常的网络状态下，消息数据转换和传送的时间应小于 3 秒

d. 登录时间：

登录时间应小于 5 秒

### 2.2.3 灵活性

a. 客户端变化：

针对多种浏览器进行适配，允许用户使用浏览器访问网页端，也允许使用移动端客户端使用软件。

b. 可移植性：

移植到 Windows、Mac OS、Linux 等系统的工作量较小。

c. 界面需求的变化，

当界面需要重新设计时，由于软件使用 MVC 设计，只需修改界面对应的 View 即可。

d. 国际化要求：

软件界面应具支持有多种语言，同时软件使用 utf-8 作为编码模式，方便在不同语言的平台上使用。

## 3 运行环境

### 3.1 硬设备

客户端程序硬件要求

a. 接入网络，支持 WebKit 的浏览器

预期可拓展的模块：

b. 具有音频输入输出功能

c. 数位板或压感笔输入

服务器设备：

a. 带宽大于 100M

b. 处理器 arm 或 x86/64

c. 内存大于 1G

## 3.2 支持软件

操作系统:

Windows, Linux, MacOS, Android, iOS, Windows Phone

程序语言:

TypeScript

编译系统:

IntelliJ IDEA, Webstorm

数据库:

MySQL

服务器端语言:

Java

服务器程序

Nginx, Tomcat

## 3.3 数据结构

本软件需要 MySQL 作为数据库。

# 4 使用过程

## 4.1 安装与初始化

程序作为 Web 应用程序，故用户可以直接访问在线页面 [maomaochat.tech](http://maomaochat.tech)



图 4-1-1：引导页面

滑动页面或点击跳过，完成引导页

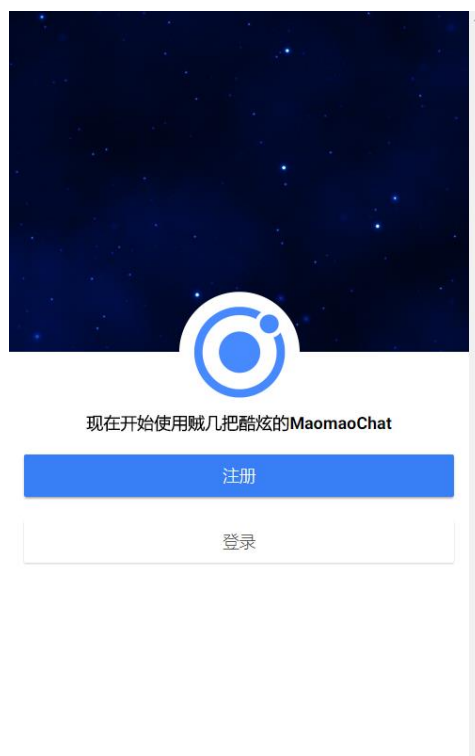


图 4-1-2：欢迎页面

进入欢迎页后，进行登录或注册即可开始使用

## 4.2 输入

本软件对输入数据和参量无准备要求。

### 4.2.1 输入数据的现实背景

表 4-2-1-1：输入情况表

情况	频度	来源	输入媒体	限制	质量管理	支配
用户发送消息	频繁	普通用户	键盘或鼠标	需要登录	无	保留
用户接收消息	频繁	普通用户	键盘或鼠标	需要登录	无	保留
用户登录	随机	普通用户	键盘或鼠标	需要密码	无	保留
用户注册	随机	普通用户	键盘或鼠标	无	无	保留

### 4.2.2 输入格式

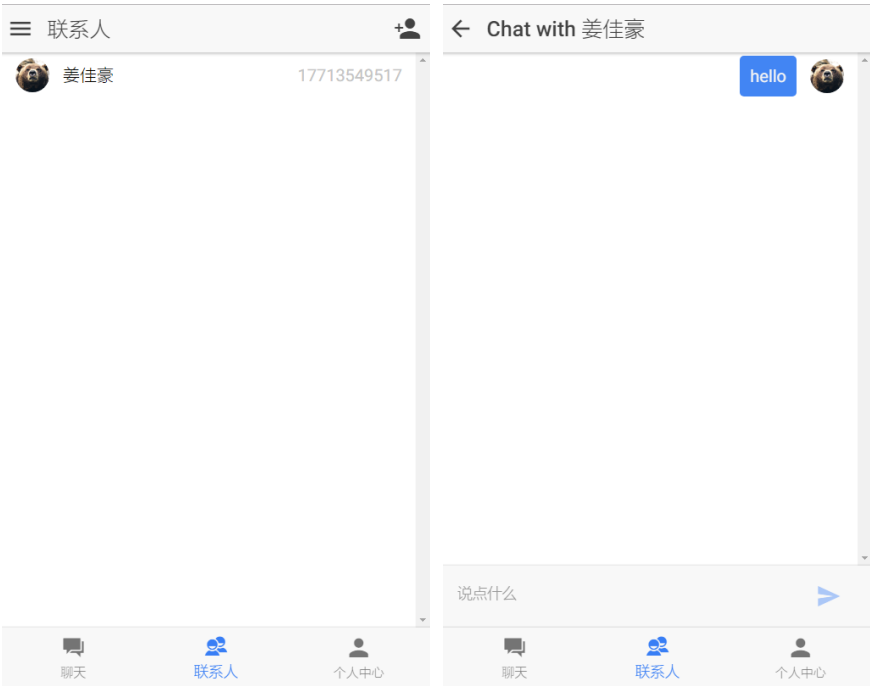
表 4-2-2-1：输入格式表

长度	格式基准	标号	顺序	标点	词汇表	省略和重复	控制
无限制	字符串	Text	无	无	无	无	无

### 4.2.3 输入举例

聊天：

点击联系人，再点击对应的用户，进入聊天界面即可开始聊天





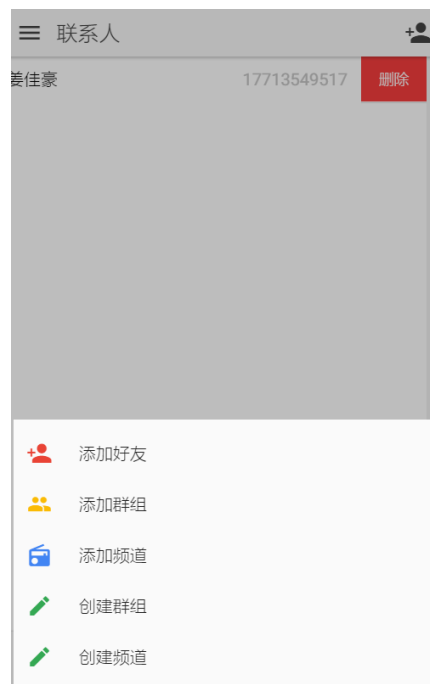
删除好友：

在联系人界面，左滑对应的用户条目，选择删除即可



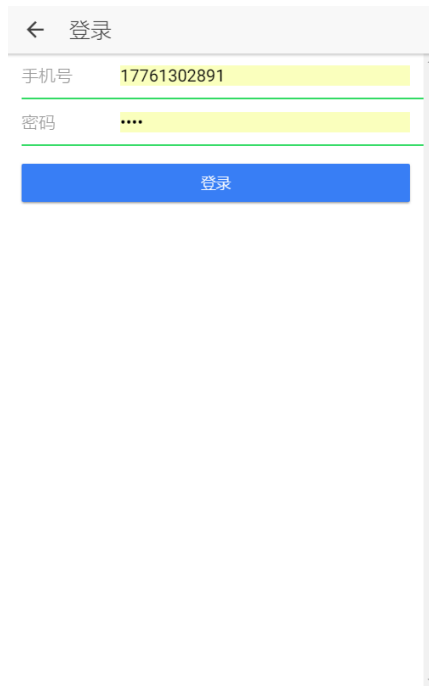
添加好友，群组，频道，创建群组，频道：

点击右上角的添加按钮，按界面提示进行操作即可



用户登录等：

在欢迎页面点击登陆按钮，进入登陆界面后按界面提示操作即可登陆

A screenshot of a mobile application's login screen. At the top, there is a header bar with a back arrow and the text '登录'. Below this, there are two input fields: '手机号' (Phone Number) containing '17761302891' and '密码' (Password) containing four dots. A blue button labeled '登录' is positioned below the password field. The entire form is enclosed in a light gray border with a vertical scrollbar on the right side.

← 登录

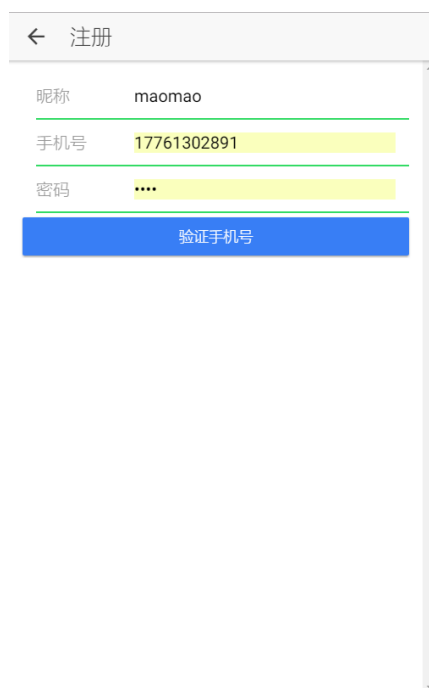
手机号 17761302891

密码 ....

登录

注册：

在欢迎页面点击注册按钮，进入注册界面后按界面提示操作即可登陆

A screenshot of a mobile application's registration screen. At the top, there is a header bar with a back arrow and the text '注册'. Below this, there are three input fields: '昵称' (Nickname) containing 'maomao', '手机号' (Phone Number) containing '17761302891', and '密码' (Password) containing four dots. A blue button labeled '验证手机号' is positioned below the password field. The entire form is enclosed in a light gray border with a vertical scrollbar on the right side.

← 注册

昵称 maomao

手机号 17761302891

密码 ....

验证手机号

退出登录：

在页面左侧右滑，在侧栏菜单中点击退出登录即可



4.3 输出对每项输出作出说明

4.3.1 输出数据的现实背景

表 4-3-1-1：输出数据表

使用	频度	媒体	质量管理	支配
显示消息给用户	频繁	屏幕显示	无	废弃
显示用户信息	随机	屏幕显示	无	废弃

4.3.2 输出格式

首部	主体	尾部
无	书籍内容	无
无	笔记内容，发送者 ID，	无
文件首部	书籍文件	文件结束符
无	用户信息	无

### 4.3.3 输出举例



图 4-3-3-1：消息显示

## 4.4 文卷查询

本软件对文件查询无相关要求。

## 4.5 出错处理和恢复

用户的网络突然中断时，软件有一定概率出现崩溃情况，此时用户可以重新打开本软件方可正常使用。

## 4.6 终端操作

本软件客户端无需终端操作