鹏程万里视频加密系统

用户手册

目录

1 引言.....2
1.1 编写目的.....2
1.2 术语和缩略词.....5
2 软件概述.....7
2.1 软件特点.....7
2.2 加密及认证流程.....8
2.3 软件运行.....9
2.4 系统要求.....9
3 系统使用.....10
3.1 注册登录.....10
3.2 主界面功能介绍.....12
3.2.1 选择项目.....12
3.2.2 视频加密信息填写.....13
3.2.3 加密设置.....13
3.2.3.1 快速加密.....14
3.2.3.2 编码加密.....14
3.2.4 认证模式.....14
3.2.4.1 网络认证模式.....14
3.2.4.2 离线认证模式.....14
3.2.5 答题设置.....14
3.2.5.1 不启用答题.....14
3.2.5.2 启用简单数学答题.....14
3.2.5.3 启用自定义答题.....15
3.2.5.3.1 添加问题.....16
3.2.5.3.2 编辑问题.....17
3.2.5.3.3 单选题、多选题、简答题.....17
3.2.5.3.4 回到上个问题、继续播放、关闭播放器.....17
3.2.5.3.5 保存问题.....18
3.2.5.4 绑定方式.....18
3.2.5.5 其他设置.....19
3.2.6 水印设置.....20
3.2.7 信息管理.....20
3.2.7.1 视频信息管理.....21
3.2.7.2 网络授权管理.....22
3.2.7.3 批量授权管理.....22
3.2.7.4 离线授权生成.....23
3.2.7.5 子账户管理.....24

1 引言

1.1 编写目的

在互联网教育培训兴起的时代，正版的视频教学正被盗版所侵害着，虽然国家对版权保护的要求越来越严，但仅仅靠版权保护还远远不够，法律不能即时解决我们的著作权问题，特别是视频教学的作者们看到自己的劳动成果，在淘宝上、网站上以白菜价的价格售出的时候，他们的心情可想而知。然而，市场上的加密器却显得无能为力，鹏程万里视频加密系统（以下简称“鹏程万里视频加密”）的开发者曾经也深受其害，所以要励志解决著作权保护问题，保护作者的劳动成果。

为解决视频加密后被破解提取或被翻录的问题，我们对目前市场上流行的视频加密软件进行了详细的调研，比如：金盾、超时代、金狮、狂牛、海海、飞星、金钻、鹏宝宝等等本地视频加密，还有云视频保护平台：保利威视、腾讯教育、百度教育、51CTO等等网页视频教育平台，都存在破解提取、翻录下载的问题。经过仔细研究我们发现这些加密软件都使用了相同的缓存加密的方法，就是说对视频文件直接进行简单的异或加密后再放到内存中进行解密播放，从而导致破解者可以直接读取内存数据进行破解提取。为解决这个问题，鹏程万里视频加密使用了微软公司的 DirectShow 系统对视频文件进行重新编码后，采用 AES 256 位高强度逐帧动态加密，加密后的文件直接送往视频渲染器进行播放，很好的解决了直接读取内存数据进行破解提取的问题，但这样还是远远不够安全，因此我们还采用了动态加密

技术，在传统文件加密中，采用的是静态加密，既两个相同的文件编码序列加密后的编码序列也是相同的，这样就给破解带来方便，鹏程万里视频加密采用动态加密技术，可以保证文件加密后的编码序列具有唯一性，既两个相同的文件编码序列加密后的编码序列是不相同的，就像您的指纹或虹膜一样具有唯一性；加密后的视频文件还同时具有哈希效验功能，这样就很好的解决了非法复制、破解和数据篡改的问题。

解决了视频文件被破解提取的问题后，我们开始研发防翻录系统，翻录几乎是上面所提到的视频加密软件及云视频保护平台的通病，那么为什么这些加密软件及平台对翻录程序的检测功能很弱呢？经过研究我们发现，他们使用的防翻录技术就是检测系统中是否运行了加密器中已经设定好的翻录软件库，如果翻录者使用了加密器翻录软件库中没有的翻录软件，或者使用一些特殊的手段，如隐藏录屏软件的进程或者使用视频采集卡等，那么这些加密器的防翻录功能就彻底失效了。为了解决视频被翻录的问题，鹏程万里视频加密采用了5种特殊的录屏检测方法，其中包含了系统内核检测和驱动检测视频采集卡的防翻录方法，采用内核检测后，隐藏录屏软件进程的翻录方法彻底失效，而且还防止了一些新出的录屏软件。接着我们又研究了使用视频采集卡进行翻录的问题，所谓的视频采集卡翻录，就是利用计算机的 HDMI 或 DVI 视频图像输出接口进行硬件采集图像数据的方法翻录视频，把视频翻录工作做到了计算机的外面，使得所有加密器的防翻录功能彻底失效，为了做到防止视频采集卡翻录，鹏程万里视频加

密的开发者经过几个月的研究，终于找到了解决方案，通过系统内核驱动来动态检测计算机的 HDMI 或 DVI 视频图像输出接口，对连接计算机的视频输出设备进行分析，然后锁定视频翻录设备信号，这样就可以做到防止视频采集卡翻录的行为了。除此之外，为了防止远程桌面等远程翻录行为，我们还加入了检测远控软件的功能，还有视频翻录黑化的功能，发现录屏行为自动封锁授权等功能，做到了真正的防翻录效果。

在软件开发的过程中，我们也调查了许多视频播放用户，因为他们也是视频被破解提取、翻录的主因，调查后我们发现，大部分播放用户都表示加密的视频播放不方便，而且有些加密软件需要关闭用户的所有进程，才能进行视频播放，极大地影响了用户的工作和学习，而且误报率很高，发现录屏后自动关闭该程序，造成用户数据丢失等问题，而且本地视频加密软件的绑定方式单一，用户更换计算机后无法进行播放，有些加密软件甚至重装操作系统后便无法进行播放，给加密者及播放用户带来不便。为此鹏程万里视频加密采用三种不同的绑定方式供加密者和播放用户进行选择，其中有一种是用户可以用自己的手机下载我们的APP，通过扫描播放器的二维码即可播放视频，极大地方便了用户的使用。在防翻录方面也做了相应的改进，如发现翻录行为后，播放器不会结束该程序，只是对用户进行友好的界面提示，如果用户执意翻录，播放器只会关闭自己，不会给用户带来麻烦，有用户在使用鹏程万里视频加密播放器时向我们表示：就像在使用 PotPlayer 等媒体播放器一样简单好用。在视频授权方面我们也提供

了多种授权方案供加密者选择，使用网络授权模式时，为了确保视频授权信不被截取，鹏程万里视频加密的服务端对授权信息也使用了RSA 2048 进行加密后，再发送到视频播放用户的播放器上，确保授权信息不被截取破译。如果加密者有自己的销售系统，如网站、公众号、小程序等，也可自行接入鹏程万里视频加密提供的授权API，从而实现无人值守的自动化视频销售系统，真正的实现了一劳永逸的加密授权方式。

1.2 术语和缩略词

DirectShow 是微软公司在 ActiveMovie 和 Video for Windows 的基础上推出的新一代基于 COM(Component Object Model)的流媒体处理的开发包，与 DirectX 开发包一起发布。DirectShow 使用一种叫 Filter Graph 的模型来管理整个数据流的处理过程，运用 DirectShow，我们可以很方便地从支持 WDM 驱动模型的采集卡上捕获数据，并且进行相应的后期处理乃至存储到文件中。这样使在多媒体数据库管理系统（MDBMS）中多媒体数据的存取变得更加方便。它广泛地支持各种媒体格式，包括 Asf、Mpeg、Avi、Dv、Mp3、Wave 等，为多媒体流的捕捉和回放提供了强有力的支持。

RSA（RSA algorithm）加密算法是一种非对称加密算法。在公开密钥加密和电子商业中 RSA 被广泛使用。RSA 是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。当时他们三人都在麻省理工学院工作。RSA 就是他们三人姓氏开头字母拼在一起组成的。
1973 年，在英国政府通讯总部工作的数学家克利福德·柯克斯（Clifford Cocks）在一个内部文件中提出了一个相同的算法，但他的发现被列入机密，一直到 1997 年才被发表。
对极大整数做因数分解的难度决定了 RSA 算法的可靠性。换言之，对一极大整数做因数分解愈困难，RSA 算法愈可靠。假如有人找到一种快速因数分解的算法的话，那么用 RSA 加密的信息的可靠性就肯定会极度下降。但找到这样的算法的可能性是非常小的。今天只有短的 RSA 钥匙才可能被强力方式解破。到目前为止，世界上还没有任何可靠的攻击 RSA

算法的方式。只要其钥匙的长度足够长，用 RSA 加密的信息实际上是不能被解破的。
1983 年麻省理工学院在美国为 RSA 算法申请了专利。这个专利 2000 年 9 月 21 日失效。由于该算法在申请专利前就已经被发表了，在世界上大多数其它地区这个专利权不被承认。

AES（Advanced Encryption Standard）高级加密标准，在密码学中又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院（NIST）于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

2 软件概述

2.1 软件特点

（1）支持所有视频文件：鹏程万里视频加密系统可加密mp4、avi、mkv、mpeg、flv、3gp、mov等所有视频文件格式。

（2）高强度加密算法：鹏程万里视频加密系统采用AES 256位高强度加密算法对视频文件进行逐帧动态加密。

（3）一机一码网络授权：经过加密后的视频文件需要绑定才能正常播放，网络授权可设定过期时间及播放次数，可随时随地收回授权。

（4）内核级防翻录：通过操作系统内核扫描屏幕录像软件，可防范非法手段运行录屏软件。

（5）驱动级视频采集卡检测：采用内核驱动的方式动态视频采集卡检测，只要插上视频采集卡设备就能精准检测，真正的防硬件翻录。

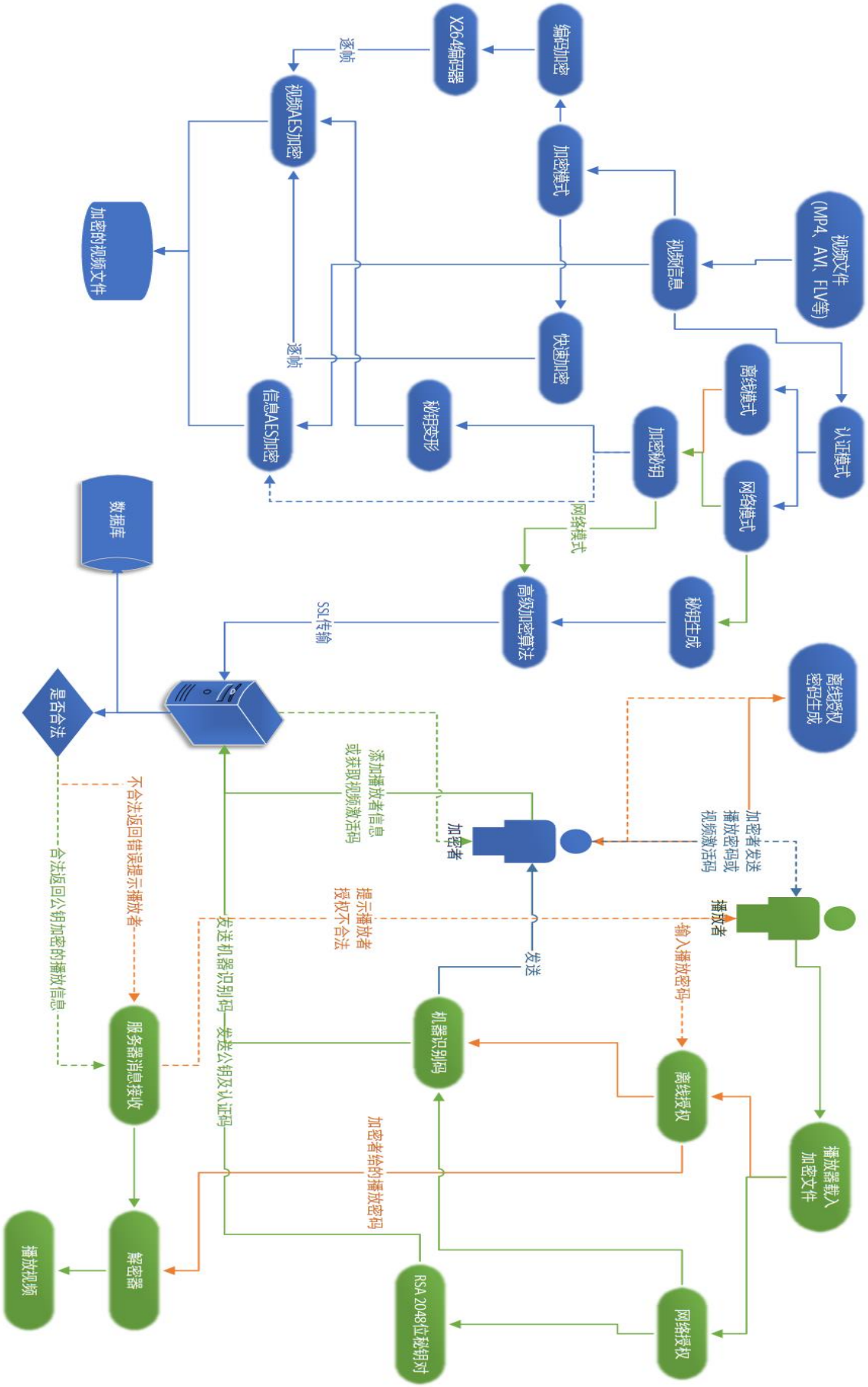
（6）视频互动答题系统：加密者可在加密视频时设置丰富的相关问题，目前可以设置简答题、单选题及多选题。

（7）智能防翻录：可检测所有主流屏幕录制软件及远程控制软件，发现翻录行为可自动封锁授权。

（8）录屏黑化：采用录屏黑化技术既截图、录屏、远控等截取图像操作均被黑化处理，确保视频不被非法窃取。

（9）高强度防破解：采用高级防破解技术，可以防止OD等任何调试程序对加密后的文件进行调试破解。

2.2 加密及认证流程


X264编码器
编码加密
逐帧
视频AES加密
加密模式
加密的视频文件
视频信息
视频文件
(MP4、AVI、FLV等)
逐帧
快速加密
高线模式
信息AES加密
秘钥变形
加密秘钥
认证模式
网络模式
数据库
网络模式
高级加密算法
秘钥生成
SSL传输
是否合法
高线授权
密码生成
添加播放者信息
或获取视频激活码
加密者
加密者发送
播放密码或
视频激活码
播放者
不合法返回错误提示播放者
提示播放者
授权不合法
发送机器识别码
发送
输入播放密码
合法返回公钥加密的播放信息
服务器消息接收
机器识别码
离线授权
播放器载入
加密文件
发送公钥及认证码
加密者给的播放密码
播放视频
解密器
RSA 2048位秘钥对
网络授权

2.3 软件运行

本系统运行在 PC 及其兼容机上，使用 Windows 7或以上版本号操作系统，在软件安装后，直接点击相应图标，就可以显示出软件的主菜单，进行需要的软件操作。

2.4 系统要求

Windows 7 及其以上版本
处理器(CPU)：1千兆赫(GHz)或更快的64位(x64)处理器
内存：1GB 内存
硬盘：100MB可用硬盘空间
显卡：带有WDDM 1.0或更高版本的驱动程序的DirectX 9图形设备，显存128MB。

3 系统使用

3.1 注册登录

双击软件图标，进入登录界面。

图 3-1 系统登录界面

如果没有账号，先注册账号。

图 3-2 系统注册界面

注册成功后，输入注册的账号密码即可成功登录，登录后即可看到个人信息和所拥有的对应授权。

图 3-3 软件界面

如果下方用户信息显示为试用用户，即没有对应授权，可联系QQ：453188961，购买对应授权。

3.2 主界面功能介绍

3.2.1 选择项目

选择一个需要加密的视频拖入或者添加进加密系统。

图 3-4 拖入或添加视频

3.2.2 视频加密信息填写

填写符合自己所需的视频信息。

图 3-5 视频加密信息填写

其中，视频编号（双击即可生成）和加密密钥（点击即可生成）是系统生成，不由用户填写，如用户填写会导致加密后的文件出错。

3.2.3 加密设置

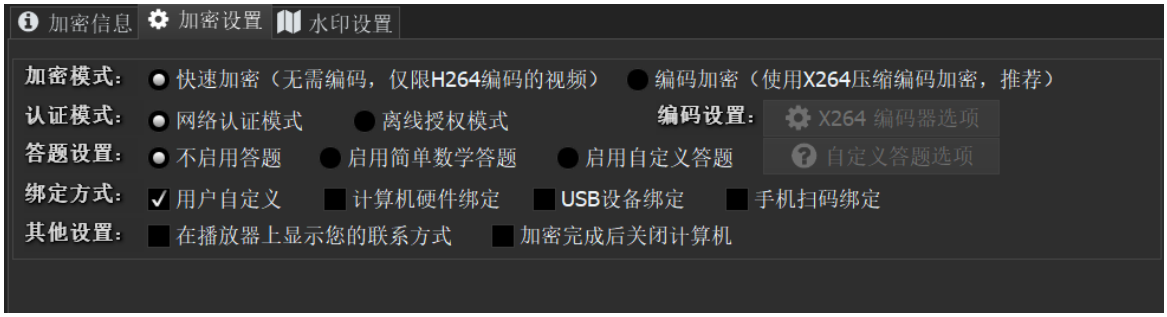


图 3-6 视频加密设置

3.2.3.1 快速加密

快速加密即不转换视频编码从而直接加密，此模式仅适用于 H264 编码的视频，如果其他编码的视频使用此模式，可能会导致加密后的视频在播放时出现黑屏等问题。

3.2.3.2 编码加密

编码加密是通过 X264 编码器对视频进行转换编码后，再进行加密，此模式可以支持所有视频的编码格式，具有输出文件小，视频质量清晰的特点，但加密速度较慢。详情可参考简单设置。

3.2.4 认证模式

3.2.4.1 网络认证模式

网络认证是将加密的视频信息上传至服务器进行保存，用户在播放时仅需将自己的计算机识别码提供给加密者，或者输入加密者提供的视频激活码，即可授权其播放。

3.2.4.2 离线认证模式

离线认证是将加密的视频信息不会上传至服务器进行保存，加密者需要自己保存视频的加密信息，用户在播放时需将自己的计算机识别码提供给加密者，加密者需要使用加密系统提供的密码生成工具，手动生成视频的播放密码，并将播放密码发送给用户，才能完成授权。

3.2.5 答题设置

3.2.5.1 不启用答题

选择不启用答题，视频会流畅的播放完毕。

3.2.5.2 启用简单数学答题

启用简单数学答题，会根据视频的长度在某一个时间段里弹出数学答题。

3.2.5.3 启用自定义答题

自定义答题，专门为教育机构所提供的互动功能。可根据课程关键点设置答题选项。启用时点击自定义答题选项即可打开设置界面。

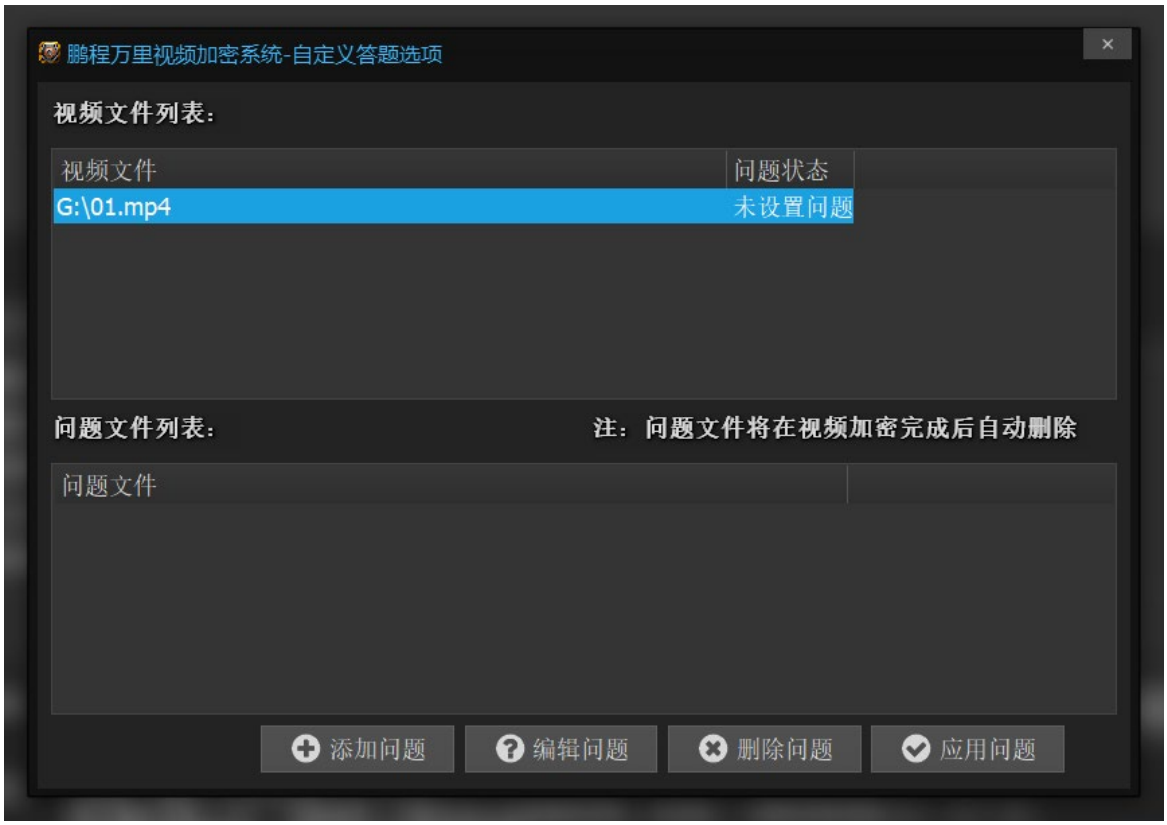


图 3-7 自定义答题选项界面

3.2.5.3.1 添加问题

选择需要添加问题的视频文件，然后选择添加问题即可打开设置界面。

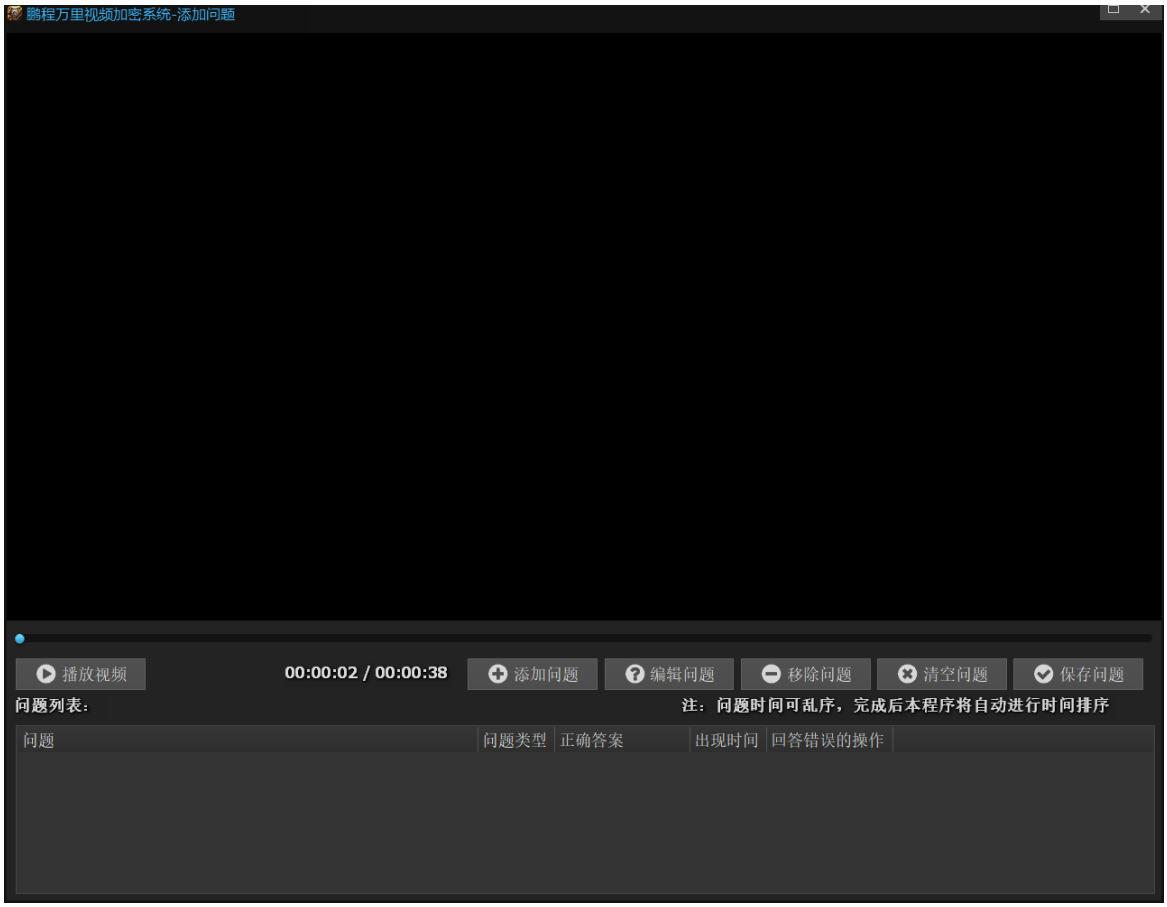


图 3-8 自定义答题设置界面

3.2.5.3.2 编辑问题

选择需要添加问题的时间轴，然后添加问题。输入符合视频相对应的互动问题。

图 3-9 自定义答题添加问题界面

3.2.5.3.3 单选题、多选题、简答题

单选题：

A、B、C、D仅有一个答案为正确答案。

多选题：

A、B、C、D为多选项正确答案。

简答题：

可根据问题填写课堂里所讲到的正确答案。

3.2.5.3.4 回到上个问题、继续播放、关闭播放器

回到上个问题：

用于一个视频有多个问题，回答错误返回到上个问题的时间轴，如果第一道题打错，则视频重新播放。

继续播放：

即使问题回答错误也将继续播放。

关闭播放器：

回答错误播放器将自动关闭。

3.2.5.3.5 保存问题

可根据视频所讲的关键点设置一个或者多个互动问题，点击添加，回到设置界面时，可根据问题进行修改，确认没问题点击保存问题即可。

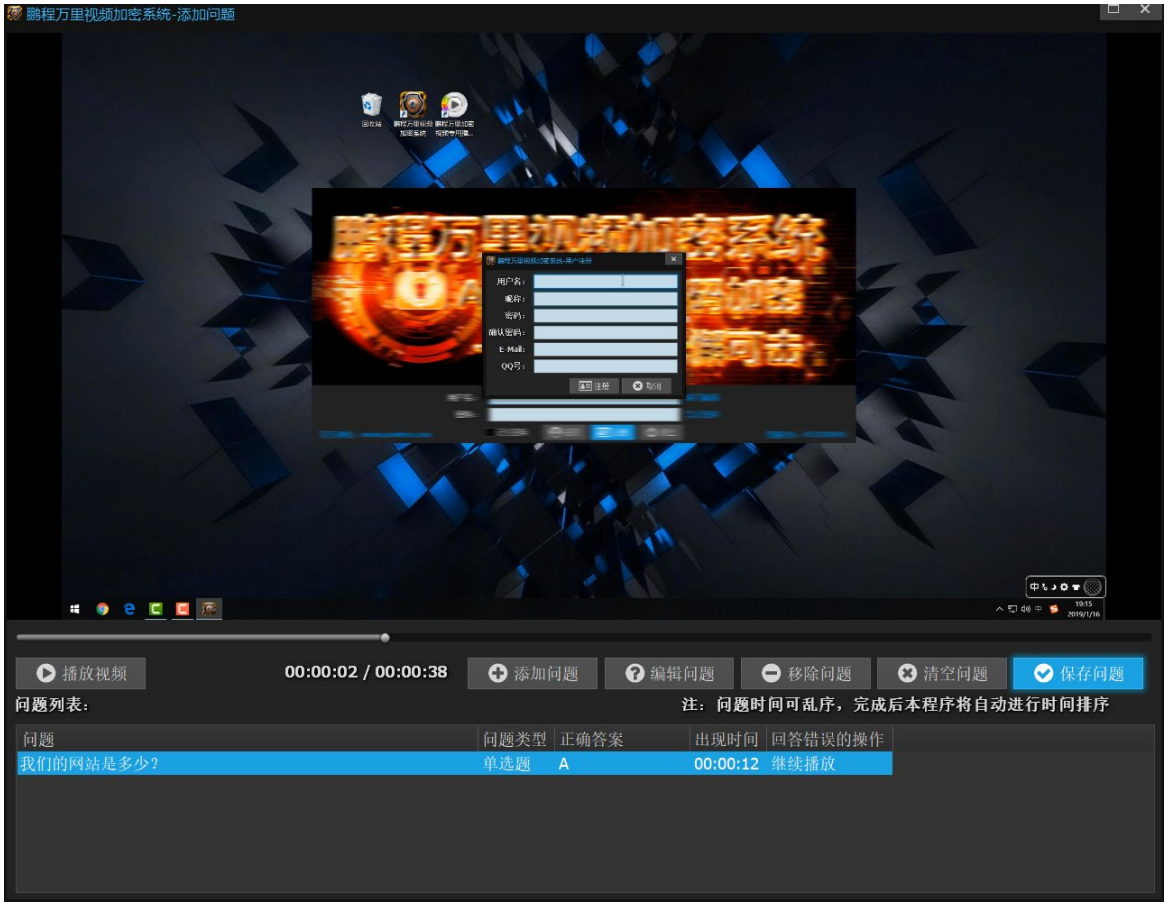


图 3-10 自定义答题添加问题界面

3.2.5.4 绑定方式

用户自定义：

将采用默认的所有绑定方式，包括计算机硬件绑定、USB设备绑定、手机扫码。

计算机硬件绑定：

通过计算机硬件ID（如CPU、网卡等）获取用户的识别码。

USB设备绑定：

支持一切正规带有USB存储的设备。例：U盘，移动硬盘，手机USB模式。

手机扫码：

用户通过扫描二维码的方式来获取视频的播放授权，方便需要经常变更计算机的用户。

3.2.5.5 其他设置

在播放器上显示您的联系方式，如实填写相对应的联系方式即可。

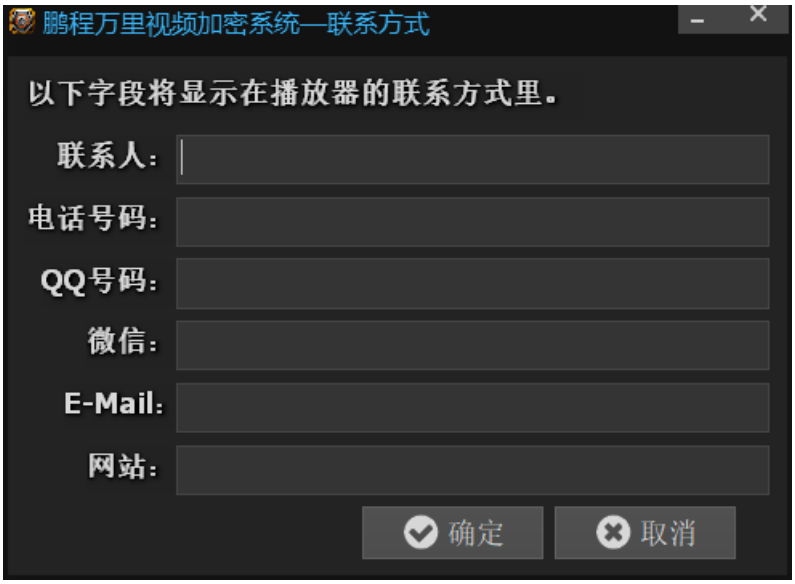


图 3-11 联系方式界面

加密完成后关闭计算机

方便用户忙碌时将视频信息添加完毕，加密过程不需要全程盯着，即使出门，视频加密完成后会自动关机。

3.2.6 水印设置

在播放器上显示动态水印，有效防止视频被翻录。水印设置可设置动态水印的字体、颜色、大小、显示方式等。

图 3-12 水印设置

3.2.7 信息管理

信息管理包含网络授权加密时的信息管理、网络授权管理、网络批量授权管理、离线授权生成器和子账户管理。

图 3-13 信息管理

3.2.7.1 视频信息管理

包含对视频加密信息的更新和删除功能。其中 添加到加密器 功能是为了方便加密者需要使用已使用过的视频加密信息，再次对为未加密的视频进行加密而设计的。特别提醒：删除视频加密信息将导致加密的视频无法正常播放。

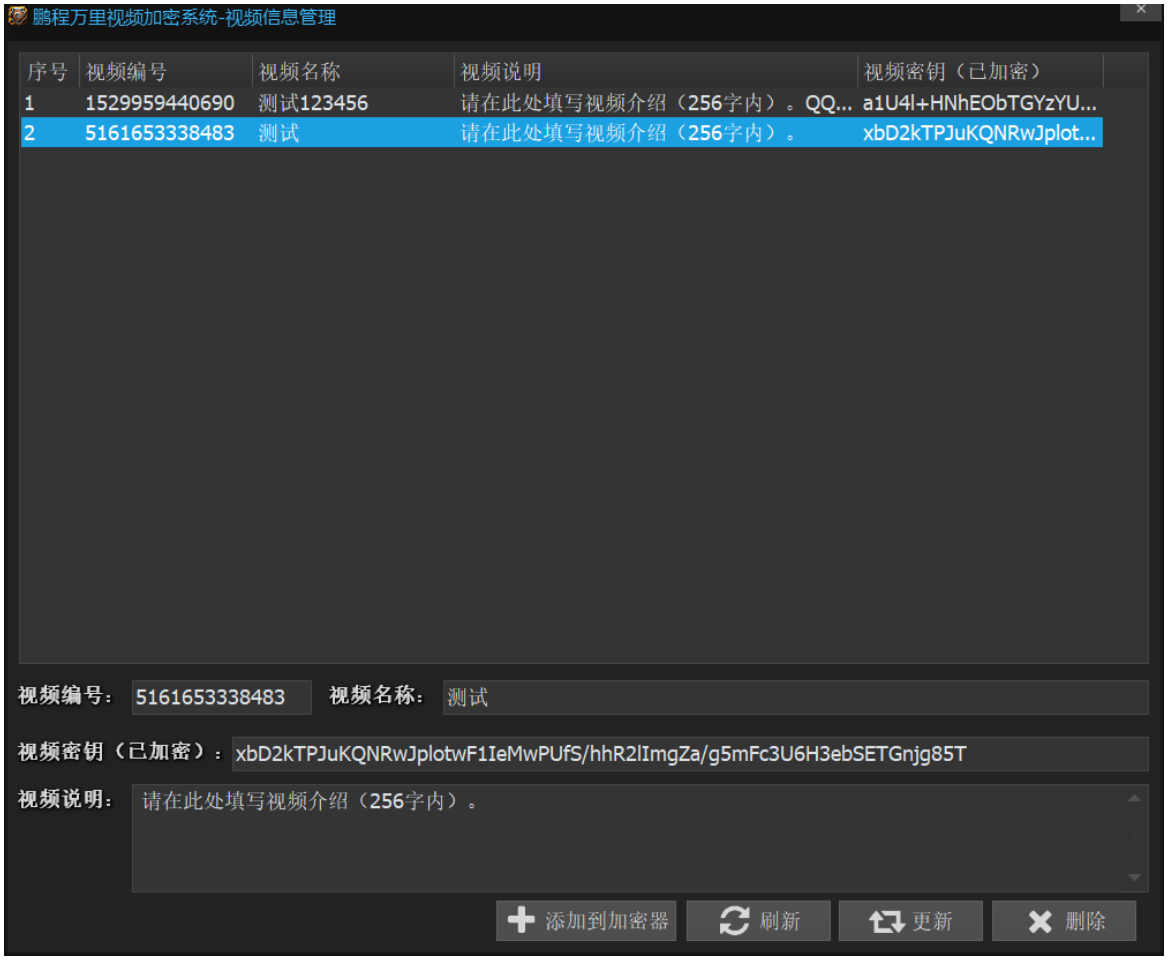


图 3-14 视频信息管理

3.2.7.2 网络授权管理

对使用网络授权模式加密的视频进行授权管理，其中包含对授权的添加、更新、查询、删除等操作。

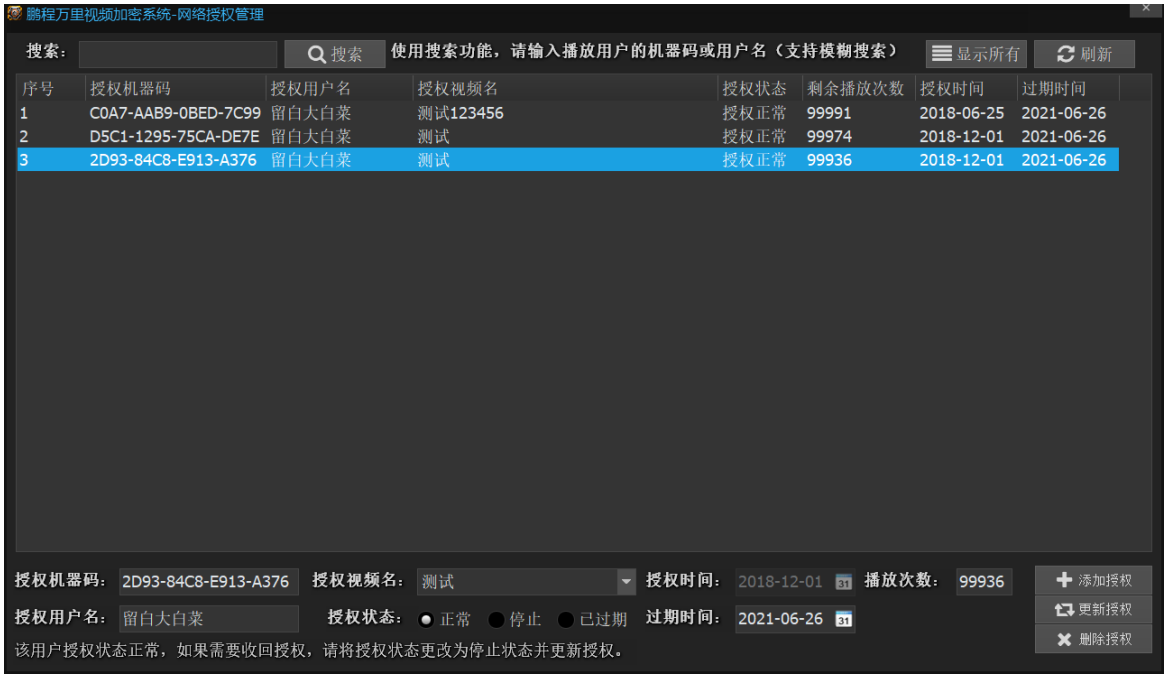


图 3-15 网络授权管理

3.2.7.3 批量授权管理

对使用网络授权模式加密的视频进行批量授权管理，其中包含对视频授权激活码的添加、导出、查询等操作。特别注意：视频激活码添加后不可删除。

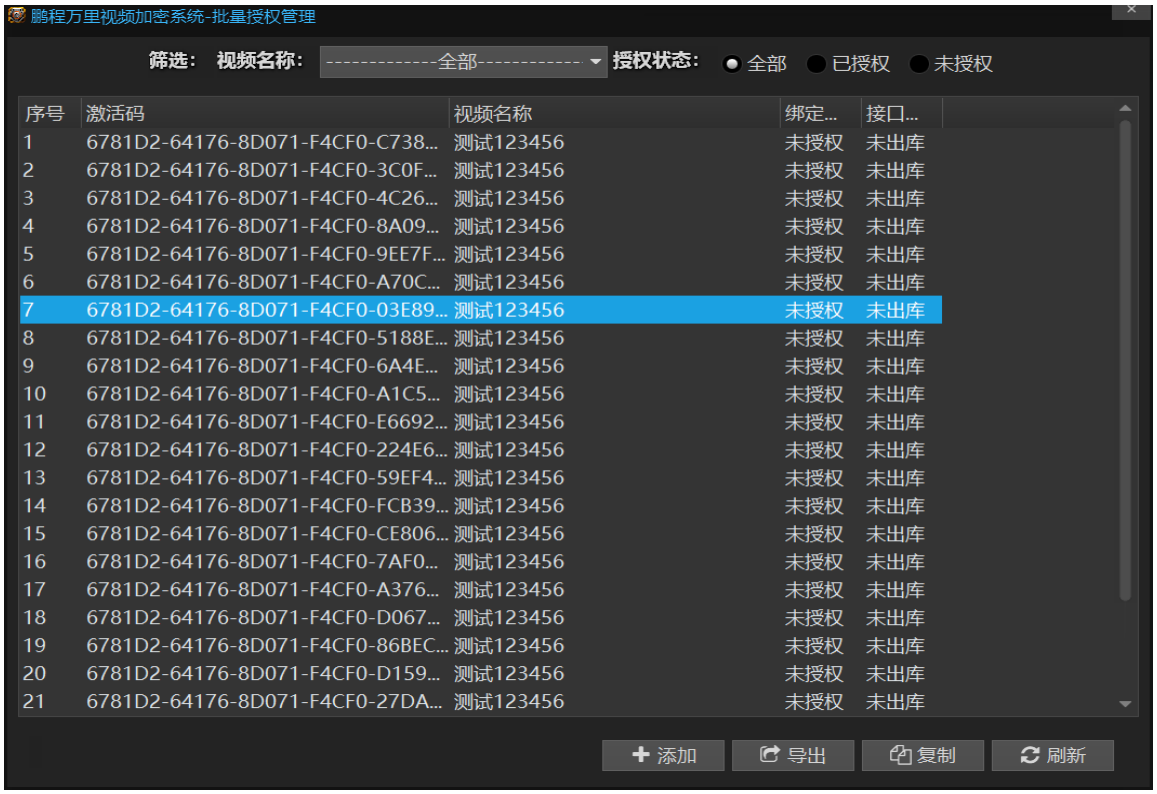


图 3-17 批量授权管理

3.2.7.4 离线授权生成

对使用离线授权模式加密的视频生成离线播放密码，使用时填写相关的信息及控制信息，点击 生成播放密码 即可生成离线播放密码，除此之外，还可以导出播放密码和生成注册机文件，方便用户和加密者使用。特别注意：离线授权不可回收。

图 3-18 离线授权生成

3.2.7.5 子账户管理

在使用网络授权版时，可以创建子账户，便于教育培训机构多名讲师使用。一个网络授权版的主账户最多可以创建10个子账户，子账户一旦创建便不可删除，只能通过停止子账户的功能停止使用。子账户只能使用网络授权模式加密视频，子账户的授权点数可自行分配，分配后将扣除主账户中相应的授权点数。也可以设置子账户的权限，查看子账户的授权等功能。

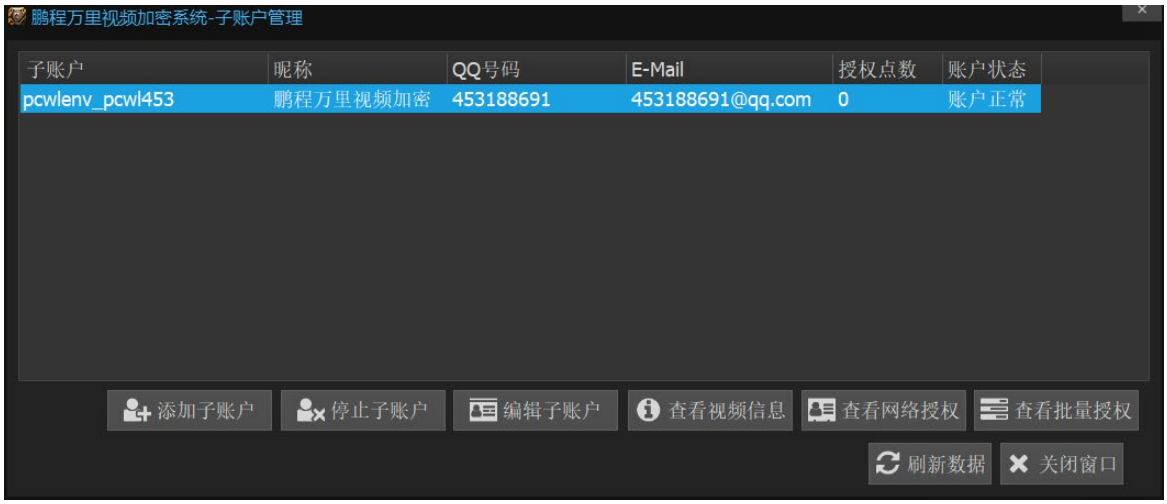


图 3-19 子账户管理