

# X509 加密社交系统实现

密码学大作业



严春伟  
1201213679  
互联网研发中心

王永庆  
1201213674  
现代数字信号处理实验室

2013 年 1 月 13 日

luzm	发放北京市在校生补贴 - 各班班长注意, 今天发放北京市在校生补贴, 该补贴主要是根据价格上涨时对学生食堂基本伙食进行补..
luzm	转发: 关于增设临时穿梭巴士的通知 - 关于增设临时穿梭巴士的通知 全院各单位: 因地铁7号线西丽湖站施工, 丽水路部分路段从..
李立华	Fw: 回复: 开题考评意见 - ----- Original ----- From: "雷总" <leik@pkusz.edu.cn>; Date: Tue, D
luzm	转发: 寒假留校学生统计表 - 各位同学, 接到校本部通知, 需要统计寒假留校生名单, 请各位打算寒假留校的同学把附件表格填好..
杨柳	信息工程学院12-13S21期末考试安排 - 各位同学: 2012-2013学年第一学期期末考试安排, 详见附件。其中政治课考试地点由教务..
杨柳	讲座通知: Ming Liu 博士 Swiss Federal Institute of Technology (ETH) Zurich, Switzerland - 各位同学: 我..
汇丰学生会	欢迎大家参加 "传承 * 跨越" ——汇丰商学院2013新年论坛 - 大家好~ 明天 (2012年12月23日) 将会在国际会议中心举行 "传承 ..
孙海峰	【新年论坛】"传承 * 跨越" 汇丰商学院2013新年论坛 - 主 办: 北京大学汇丰商学院 承 办: 北大汇丰EMBA校友会 时 间: 20..
luzm	领取镜湖之夜晚会抽奖券的通知 - 各班班长注意, 下午2点至3点根据上报名单到我处A-206领取晚会的抽奖券! 可凭抽奖券在晚会..
luzm	抽奖名单统计通知 - 还有部分班级没发抽奖名单我的, 今晚尽快发给我! 逾期不候! 没班级编制的直接给我报名! 请各班班长统计班
雷凯	Fw: ACM TechNews, Wednesday, December 19, 2012
杨柳	讲座通知: 讯程实业股份有限公司 (台湾) 高级经理罗达权先生 - 各位同学: 我院崔小乐老师邀请讯程实业股份有限公司 (台湾)
杨柳	讲座通知: 耐基梅隆大学电子及计算机工程学院李昕博士 - 各位同学: 我院林信南老师邀请耐基梅隆大学电子及计算机工程学院 ..
杨柳	Fw: 大学英语四六级考试准考证领取通知 - 各位同学: 关于四六级英语考试的事情请查阅以下邮件。如有问题, 请咨询教务处H-1..
luzm	转发: 2013年寒假学生火车票 订购通知-此件为准 - 各位同学好, 2013年寒假学生火车票往返票集中办理工作现已正式开始, 请各..
雷凯	Content Is King: Can Researchers Design an Information-Centric Internet?
luzm	转发: 关于公费医疗报销 - 2012年12月份公费医疗报销通知 各位同学: 2012年12月份的学生公费医疗报销工作从今日开始, 请..

图 1: 学校内公共邮箱内的邮件比较杂乱.

## 1 需求分析

在实际工作或者学习中, 特别是在企业或者学校中, 经常会有比较正式和重要的新闻和公告。目前现成的接受工具包括电子邮箱、即时通信 (IM)、社交网络 (人人网、QQ 等)。其中, 就我们学校环境来看, 用的比较多的包括邮箱 (企业邮箱, sz.pku.edu.cn), 以及班级群。但是通知公告嫁接在常规的信息工具之上会有一些不方便, 如图 1, 图 2.

图 1 是学校的公共邮箱, 很多正式的通知公告会由相关的职能部门发给每一位学生, 但是由于学生的身份并没有详细的划分, 总会有很多信息公告甚至垃圾邮件被盲目推送给并不相关的学生。

比如图中汇丰商学院的讲座信息也发送给了我们信息工程学院的学生, 相信大部分学生都不需要这样的信息。

图 2是我们班级群聊天记录一小部分的截图。

可以看到由于 QQ 群本身就是一个聊天交流的工具, 并不完全能够胜任通知的要求, 主要有两个原因:

1. 在老师发送通知之后, 一些与之无关的聊天讨论仍会继续, 这导致了正式的通知会很快淹没在无关的聊天刷屏中
2. QQ 本身只是一个聊天工具而已, 并不能将之与学校及其他机构正式的公告平台等同, 很多同学并不会每天上 QQ, 这降低了信息的传达效果。

考虑到这些, 我们尝试去实现一个专业公共的平台。

## 2 实现设想

我们实现的核心思想是, 实现一个平台, 能够将日常所需要的通告信息聚集起来, 对于我们学生, 一般的信息包括学校学院最新的新闻, 还有的就是通知公告。

我们实现了一个爬虫, 能够自动爬取深圳研究社官网 (<http://pkusz.edu.cn>), 信息工程学院 (<http://ece.pku.edu.cn>) 的首页新闻。

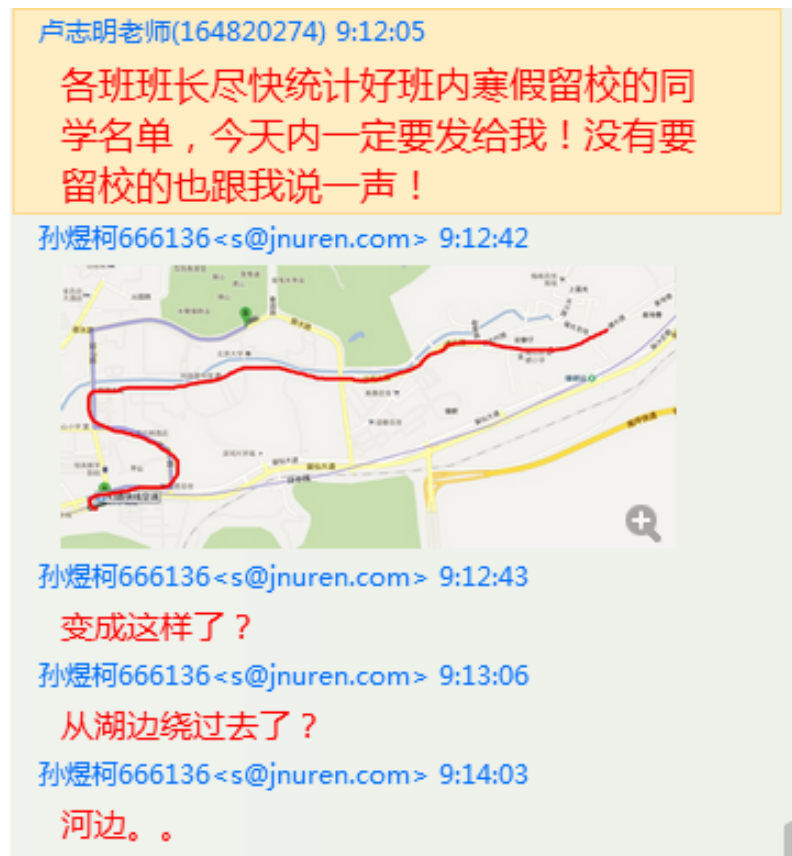


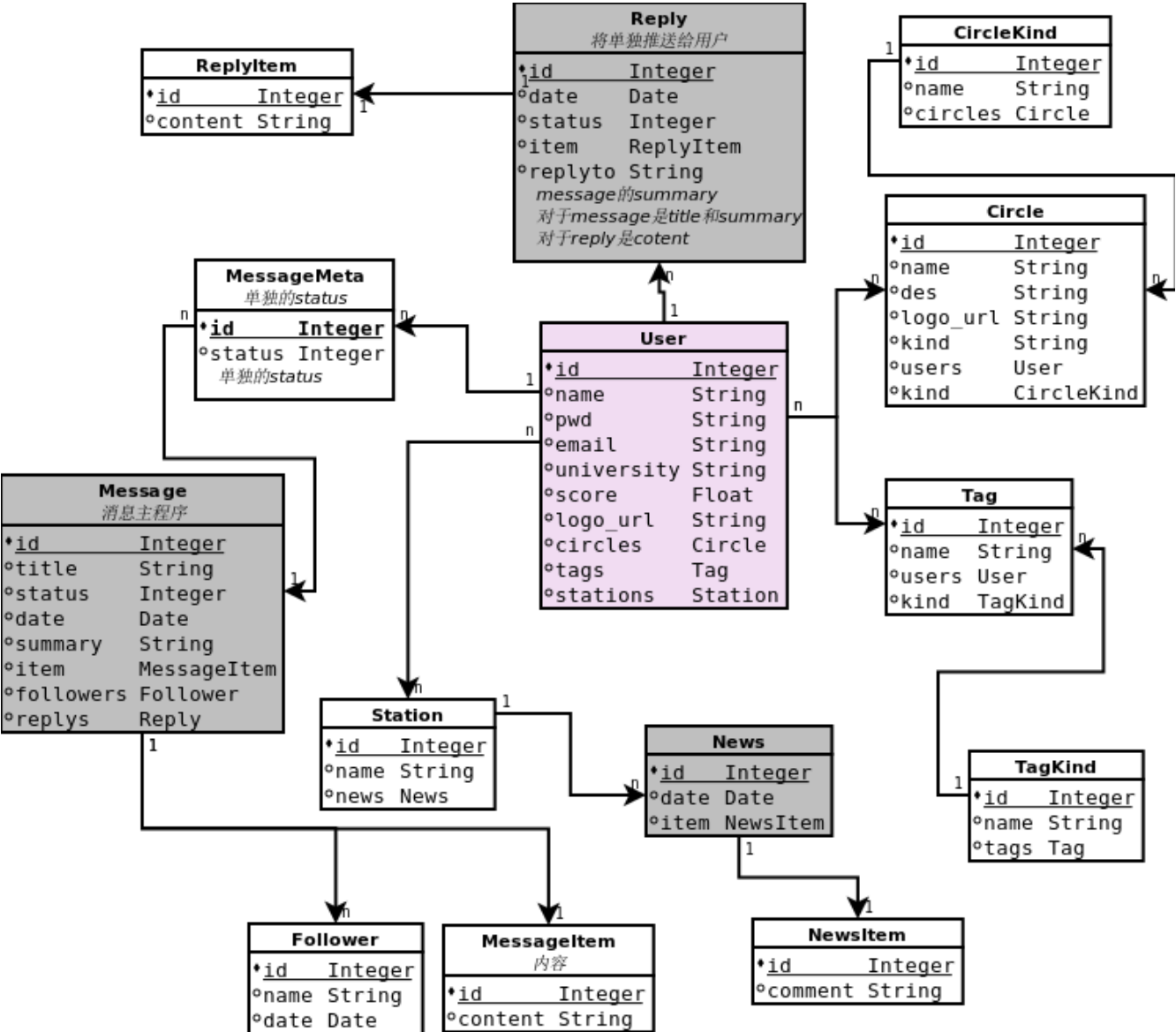
图 2: QQ 中的公告信息很容易淹没在无关的讨论中。

通过群组的概念将通知信息进行归类，用户可以添加或者退出群组来自由选择自己所需要的公告信息来源。同时，我们有限度地支持回复讨论的功能，并很注重将回复与正式的通告的区分。信息以推送的方式发送给每一位用户，为了方便了解用户对信息的回馈，我们实现了一个统计的功能，可以让信息推送人很方便地统计对信息公告感兴趣的用户（比如，推送一个活动或讲座的公告后，会有哪些用户有意愿参加）。

### 3 实现及环境

开发语言	Python2.7
网络框架	web.py
数据库	sqlite
爬虫框架	Scrapy
数据库操作框架	sqlalchemy
javascript 框架	jQuery
X509 实现	OpenSSL
运行环境	Linux Mint 14

4 数据库设计



5 X509 协议

6 运行演示

6.1 基本界面

6.2 功能演示

图 9表示的是我们从深圳研究生院网站以及信息工程学院网站抓取的最新的新闻。

图 11表示，我们实现了一个类似 QQ 群组的功能，不同的信息公告通过群组进行分类，筛选。用户选择了一个群组就相当于接受这个群组的信息公告。公告只能由该群组的拥有者推送出去，给每一位听众，听众的回馈会直接传达给管理者，但是不会被推送给其他用户。

图 12展示的是用户统计功能，通过图 5中的 Follow 按钮，用户可以对信息进行相关的回馈，比如讲



图 3: 首页



©All rights reserved by Swin Info Center | 关于我们 | 特色功能 | 联系合作

图 4: 群组



图 5: 推送的信息

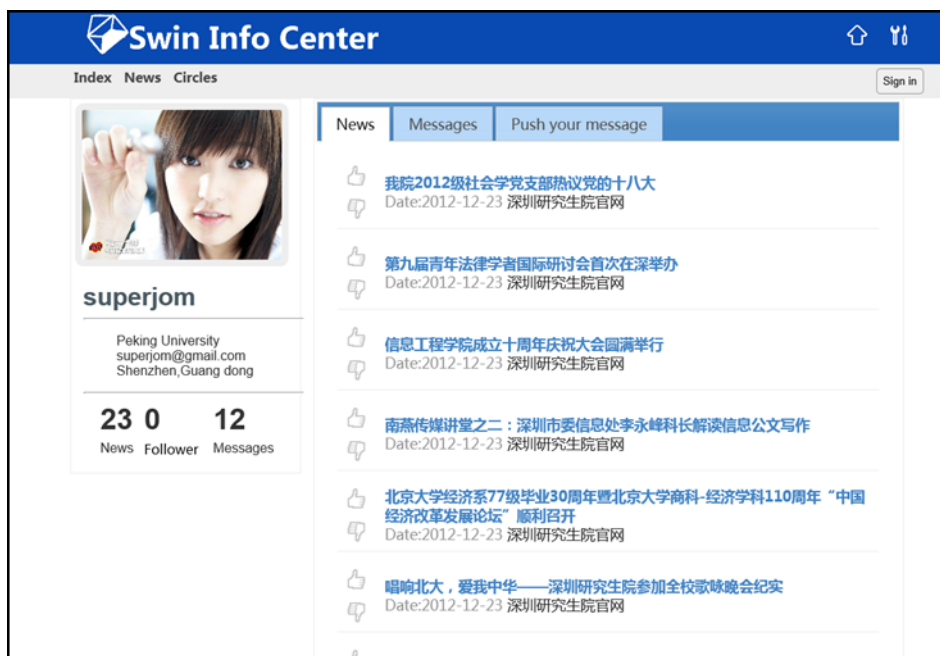


图 6: 爬取的新闻



图 7: 用 Google 浏览器 https 浏览本平台





图 8: 具体证书

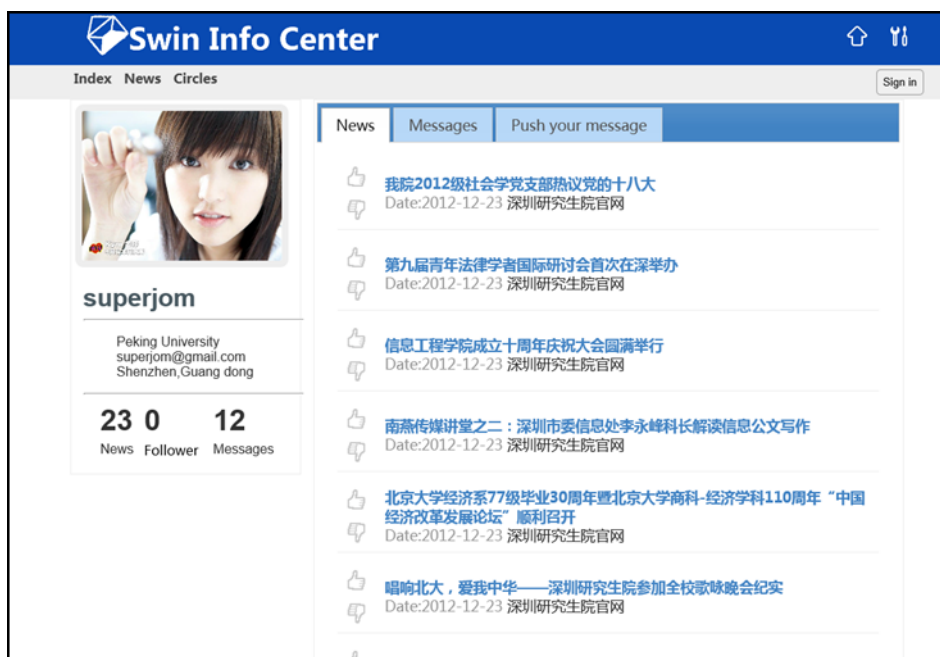


图 9: 新闻列表

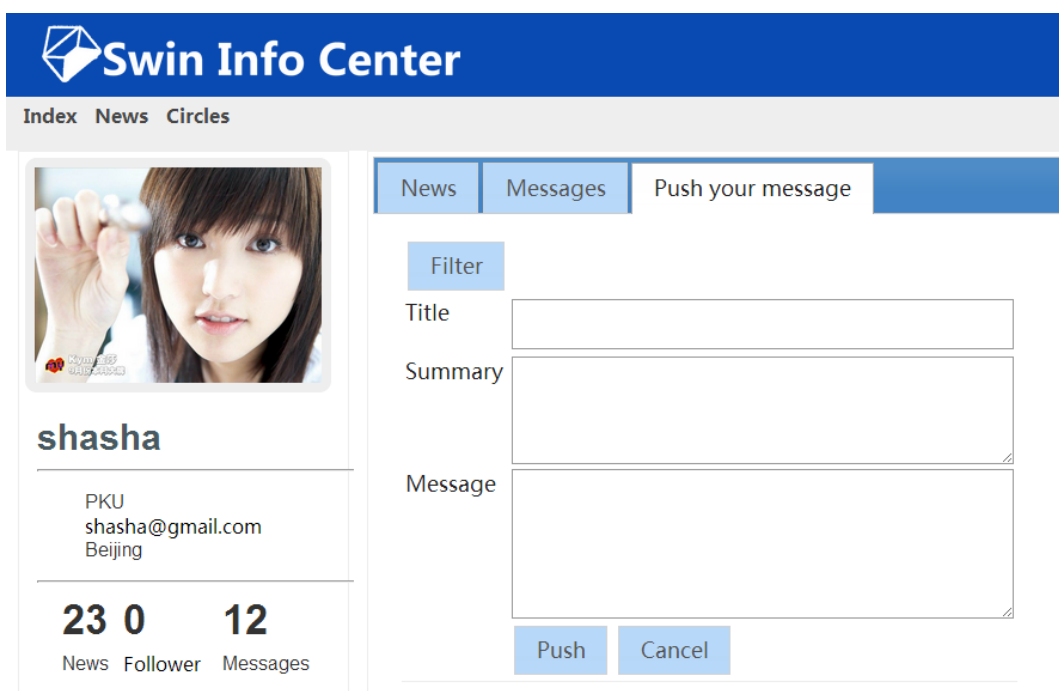


图 10: 信息推送



图 11: 推送群组选择

## Followers

讲座通知：台湾中山大学物理系特聘教授 张鼎张先生

Date:2013-01-13 研究生院

Followers:



shasha

图 12: 统计参加用户

座或者活动，点选 follow 按钮表示是要参加，信息的拥有者可以在自己的后台很方便地看到所有 Follow 的用户的列表，便于统计人数。