

1. 科技竞赛奖



获奖证书

张政宁、王凯月、崔含笑、杜阿美、胡锦涛、郑瑞丽、王月坤 你们的作品《基于伪随机置换的云外包隐私集合比较系统》荣获2017年“挑战杯”河南师范大学学生课外学术科技作品竞赛**二**等奖

指导老师：张恩

特颁此证

共青团河南师范大学委员会
二零一七年四月

证明

2014 级 计算机与信息工程学院
学号：1408114042 王凯月 在 2017 “挑战杯”大学生课外学术科技作品竞赛中获得省级三等奖，特此证明。

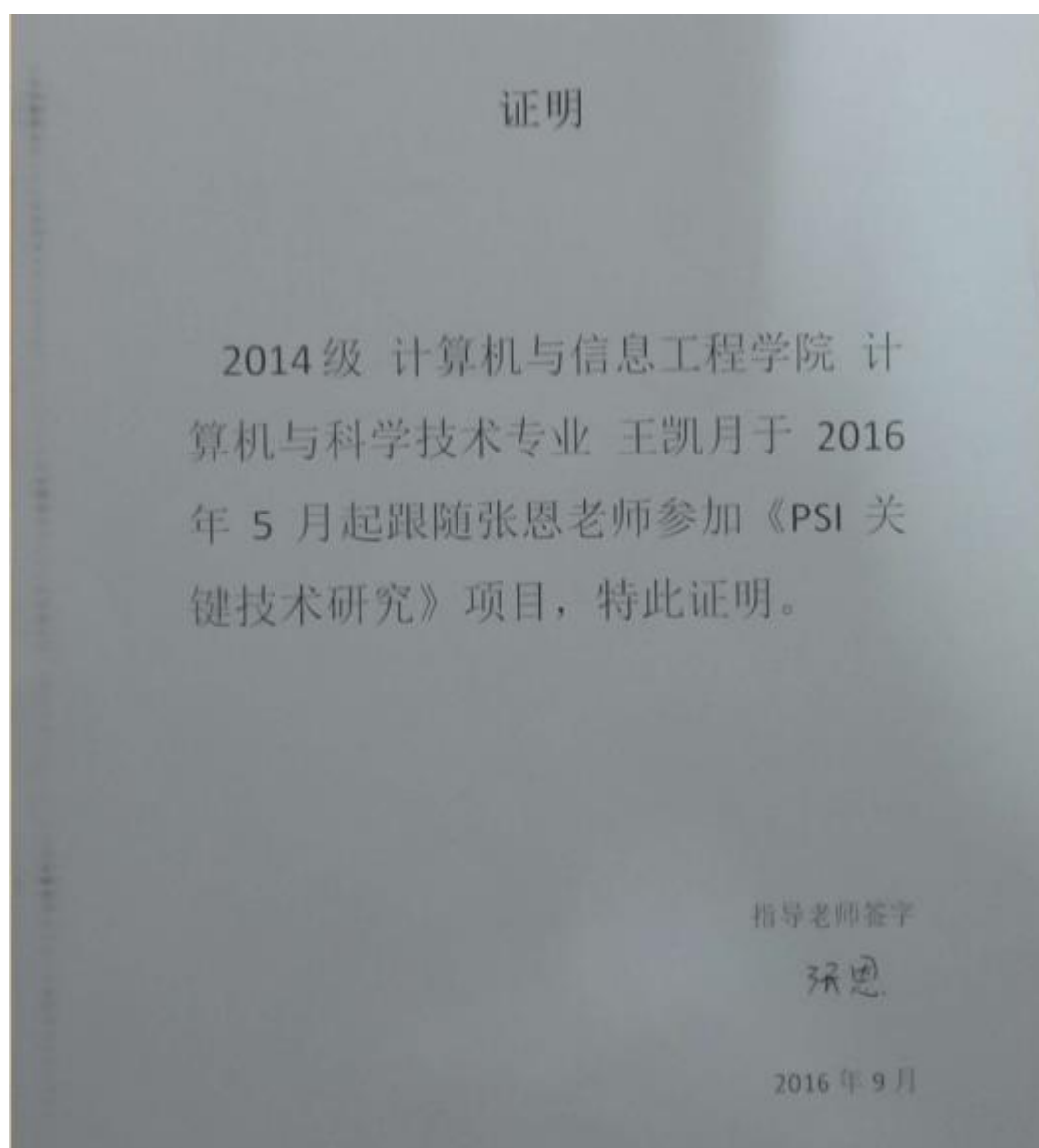
指导老师签字

张恩

2017 年 9 月

2017 年“挑战杯”省级三等奖证明（由于证书还未发放）

2.科研项目



大学生创新项目证明

中华人民共和国国家版权局 计算机软件著作权登记证书

证书号： 软著登字第1930877号

软件名称： 社交隐私匹配系统
V1.0

著作权人： 河南师范大学

开发完成日期： 2017年04月20日

首次发表日期： 2017年04月21日

权利取得方式： 原始取得

权利范围： 全部权利

登记号： 2017SR345593

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

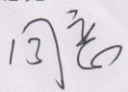
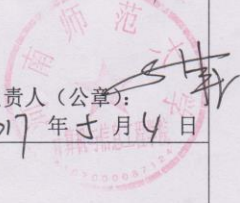
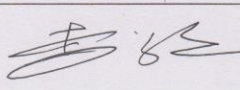


No. 01787780



软件著作权登记证书

河南师范大学职务软件著作权申请审批表

拟申请软件名称及版本	社交隐私匹配系统 V1.0		
拟申请类型	计算机软件著作权		
申请人姓名	张恩	所在部门	计算机与信息工程学院
参与软件开发的学生名单	张政宁、王月坤、王凯月、胡锦涛、崔含笑、杜阿美、郑瑞丽		
文献检索调研、创造性、应用前景等情况说明（本栏不够可加页填写）			
<p>在信息和互联网技术时代，人们更加注重信息的安全性和隐私性。许多应用场景（电子拍卖、社交网络、军事、金融商业等）需要在互不信任的参与者之间共享隐私数据或对隐私数据进行操作。因此设计出通过协同计算求交集数据并保证隐私安全的社交隐私匹配系统。该系统在很多应用前景下有极大的潜力。</p> <p>针对当前隐私泄露问题，该系统运用伪随机函数、混淆填充、洗牌算法对数据进行处理，保证了用户隐私数据的安全性，可以使用户之间进行安全的联系人信息匹配，达到了隐私保护的效果。社交隐私匹配系统是为方便寻找通讯录共同联系人而生成的一套系统。在该管理系统中，可以准确有效地寻找通讯录共同联系人电话号码，即以列表形式显示出来。更重要的是，通过输入密钥，生成密文在服务端进行比对，在客户端解密出相同信息，使得各自的信息不被泄露，因此更加安全可靠，这个过程利用计算机技术方便快速完成。</p> <p>本计算机软件开发为职务开发，知识产权属于河南师范大学所有。根据《著作权法》的规定，开发人员享有此软件的署名权，河南师范大学享有除署名权以外的其他著作权利。其著作权利由河南师范大学统一管理，任何其他单位和个人（包括开发人员）都不得擅自处置，如有违反，视为侵权，并追究其法律责任和经济责任。</p>			
		申请人: 张恩 2017年 5 月 4 日	
申请人所在部门意见		部门负责人（公章）: 2017 年 5 月 4 日	
			
科研处初审意见		部门负责人（公章）: 年 月 日	
学校审查意见		主管校长（公章）: 年 月 日	
			

软件著作权申请审批表

3.发表的期刊

1)基于伪随机置换的朋友发现系统

无线互联科技杂志社



稿件录用通知

王凯月，张政宁，杜阿美，崔含笑，胡锦涛：

来稿《基于伪随机之置换的朋友发现系统》已收悉，经本刊编辑部审阅，拟在本刊 2017 年 7 月予以刊发。

《无线互联科技》于 2004 年创办，经国家新闻出版总署批准，由江苏省科学技术厅主管、江苏省科学技术情报研究所主办。

《无线互联科技》为中国核心期刊（遴选）期刊、江苏省优秀期刊，被 CNKI、维普、万方、龙源等多家数据库收录。中国标准连续出版物号：ISSN 1672-6944，CN 32-1675/TN。

特此通知！

《无线互联科技》杂志社

2017 年 5 月 25 日

基于伪随机置换的朋友发现系统

王凯月, 张政宁, 杜阿美, 崔含笑, 胡锦涛

(河南师范大学 计算机与信息工程学院, 河南 新乡 453007)

摘 要:近年来,随着移动社交软件的迅速发展,便携式移动终端已经渗透到人们生活的方方面面。在这些软件中,人们经常用到其中的一项功能——朋友发现。但是目前这个功能对于用户并不安全,大量隐私信息被云服务商所获取。针对此现象,文章基于目前隐私集合比较的现状,运用伪随机置换和安全多方计算协议并加以改进,设计出基于伪随机置换的朋友发现系统。本系统使用户找到他们集合的交集而且不泄露除交集以外的信息,具有一定推广价值。

关键词:移动社交;伪随机置换;隐私保护;朋友发现

在信息技术和互联网技术日新月异的今天,社交网络服务越来越多地被人们使用,如微信和MSN等。每个人的朋友圈也在日益扩大,朋友的朋友在社会中也发挥着重要作用。不仅体现在就业市场上,还有其他业务,如房地产市场或产品推荐。社交网络的高聚类系数^[1]进一步表明,朋友的朋友是我们社会和情感环境的重要组成部分,并且可能成为我们直接的朋友。本文认为,一个共同的朋友至少表明两个人之间存在着潜在的“匹配”关系。

假如两个陌生人在街上相遇时,他们想要确定是否有共同的朋友,因此需要比较他们手机的联系人。我们针对此问题进行研究。与此同时,隐私保护受到大家越来越多的关注。如今,市场上开发的移动社交软件都或多或少地存在隐私泄露的问题。据DCC(互联网数据中心和360互联网安全中心联合发布的《2014年下半年Android手机隐私安全报告》)数据显示^[2],软件漏洞、系统漏洞、云端网络漏洞等都是Android手机用户隐私泄露的几大问题。如何在开放的网络环境下保障移动社交软件用户的数据安全存储和计算,成为非常紧迫和严峻的问题。

本文针对移动社交软件在生活中出现的隐私安全问题,设计出了基于安全多方计算(Secure Multi-Party Computation, SMC)和伪随机置换(Pseudo Random Permutation, PRP)的朋友发现系统。该系统在提高效率的基础上,使用了恶意模型以保证用户个人隐私的安全。

1 预备知识

1.1 SMC协议

SMC是指在分布式网络环境中,多个参与方在不泄露自己信息的情况下,将自己的信息作为输入,来共同计算某个函数^[3]。计算结束后,各个参与者在无法知道其他参与者的输入信息的情况下可以获得正确的计算结果。SMC最早是由YAO^[4]提出,主要是为了在一组互不信任的参与者间进行合作计算。EMILIANO等^[5]进一步完善SMC理论,为其理论奠定了基础。随后,GOLDREICH等^[6]提出计算任意函数的安全多方计算协议,并对其系统地做出了总结,提出了半诚实模型下SMC的安全性定义。

定义1 半诚实模型下安全证明法^[7]

设 $f: \{0,1\}_n^* \times \dots \times \{0,1\}_n^* \rightarrow \{0,1\}_n^* \times \dots \times \{0,1\}_n^*$, 其 $f(x_1, x_2, \dots, x_n)$ 是 $f(x_1, x_2, \dots, x_n)$ 的第 i 个元素。定义 $f_i(x_1, x_2, \dots, x_n) = \{f_j(x_1, x_2, \dots, x_n) \mid j = 1, 2, \dots, i\}$, 其中, $i = \{i_1, i_2, \dots, i_t\} \subseteq \{1, 2, \dots, n\}$ 。设 Π 为计算 f 的 n 方协议。若输入为 $\bar{x} = \{x_1, x_2, \dots, x_n\}$ 时,第 i 方执行 Π 的过程中得到信息序列 $(x_i, r_1, n_1', n_2', \dots, n_{i-1}')$,记为 $\text{VIEW}_i[\Pi](\bar{x})$ 。其中 r_i 表示第 i 方产生的随机数; n_j' 表示第 i 方收到第 j 个信息。协议 Π 执行完后,参与者 i 的输出结果记为 $\text{OUTPUT}_i[\Pi](\bar{x})$ 。对于确定性功能函数 f ,仅当存在概率多项式时间算法,有:

$$\{S(x_i, (x_1, x_2, \dots, x_n), f_i(\bar{x}), \text{VIEW}_i[\Pi](\bar{x}))\}_{x_i \in \{0,1\}_n^*, \bar{x} \in \{0,1\}_n^*} \approx \{\text{VIEW}_i[\Pi](\bar{x}), \text{OUTPUT}_i[\Pi](\bar{x})\}_{x_i \in \{0,1\}_n^*, \bar{x} \in \{0,1\}_n^*}$$

则称协议 Π 在半诚实模型下秘密的计算了 f 。该定义可以理解为对于半诚实的参与者,若能直接利用输入与协议的输出,通过模拟协议的执行过程来得到在过程中所能得到的所有信息,那么该协议就可以保证输入的隐私性。目前,在SMC领域内,GOLDREICH证明法是公认的安全性证明方式。

1.2 伪随机函数和伪随机置换

定义2 对于任意的攻击者 A , $F: \{0,1\}^k \times \{0,1\}^L \rightarrow \{0,1\}^L$ 是函数族,定义 A 的优势为:

$$\text{Adv}_A^{PRF}(t) = P_{\rho, K}[A(K, t) = 1] - P_{\rho, \tilde{F}}[A(\tilde{F}, t) = 1]$$

对任意整数 $t, q \geq 0$,令 $\text{Adv}_A^{PRF}(t, q) = \text{Adv}_A^{PRF}(t)$

其中 t 是时间复杂度, q 是询问次数。若 $\text{Adv}_A^{PRF}(t, q)$ 是可以忽略的,则称 F 是伪随机函数。

如下例子所示:

设 $F: \{0,1\}^k \times \{0,1\}^L \rightarrow \{0,1\}^L$ 是函数族,具体定义为: $k = L/2$, 密钥 K 是 $L \times 4$ 阶比特矩阵:

$$K = \begin{bmatrix} K[1,1] & \dots & K[1,t] \\ K[2,1] & \dots & K[2,t] \\ \vdots & \ddots & \vdots \\ K[L,1] & \dots & K[L,t] \end{bmatrix}$$

作者简介:王凯月(1995—),女,河南新乡,本科。

输入 $x = x[1]x[2] \cdots x[l]$ 作为长度为 l 的比特串, 函数 $F(K, x)$ 的形式如下面所示:

$$F_x(x) = \begin{bmatrix} K[1,1] & \cdots & K[1,l] \\ K[2,1] & \cdots & K[2,l] \\ \vdots & \vdots & \vdots \\ K[l,1] & \cdots & K[l,l] \end{bmatrix} \begin{bmatrix} x[1] \\ x[2] \\ \vdots \\ x[l] \end{bmatrix}$$

具体有:

$$x[1] = K[1,1] \cdot x[1] \oplus K[1,2] \cdot x[2] \oplus \cdots \oplus K[1,l] \cdot x[l]$$

$$x[2] = K[2,1] \cdot x[1] \oplus K[2,2] \cdot x[2] \oplus \cdots \oplus K[2,l] \cdot x[l]$$

$$x[l] = K[l,1] \cdot x[1] \oplus K[l,2] \cdot x[2] \oplus \cdots \oplus K[l,l] \cdot x[l]$$

本文所采用的是伪随机置换方法, 即通过密钥的密码方法, 在加密变换时, 改变各个字符在明文序列中的位置, 使一段文字信息的顺序混乱, 以此来隐藏其要表达的信息。这种方法利用“随机排序”来编制密钥, 该方法由以下两点理由支持。

(1) 设 n 为明文字符的个数, 当 n 足够大时, 则有 $n!$ 个不同排列种数, 在如此庞大的数字中, 想要在不知道生成条件的状况下, 找到某个特定的排列, 需要进行 $\frac{n!}{2}$ 次搜索, 可见其巨大的复杂度。

(2) 可以让计算机程序自动生成“伪随机序列”^[30], 得到一个参数 k , 每一个 k 值唯一对应一个排列, 并且不同的排列需要不同的 k 值一一对应, 由此得到一个可逆的变换, 从而完成加密和解密的过程, 该方法能很好地抵抗破解是由于其取值范围的较大性。

2 基于伪随机置换朋友发现系统模型的建立

2.1 模型介绍

假设 Alice 和 Bob 是两个移动终端用户, 简单方案如下描述: 他们想在自身隐私不被泄露的条件下寻找手机通讯录里的共同好友, 并且返回共同的手机联系人。基于伪随机置换朋友发现系统模型如图1所示。

本系统的具体模型如下: 本系统由客户端与服务端组成, 用 Android 手机作为客户端, 电脑暂时作为一个服务端。在客户端基于 PRP 和 SMC 使用任意服务器模型, 对数据进行加密处理, 并通过 socket 通信将加密后的数据传至服务器。服务器经过密文对比后, 返回相同的密文, 然后在客户端进行密文解密后, 最终得到交集。本文使用手机联系人作为集合, 进行集合比较, 得到相同的手机联系人信息, 实现了上述的模型和方法, 保护了隐私信息。

整体系统由3个线程组成, 服务端和客户端相对应: (1) 服务端创建线程, 发送服务端的IP, 客户端接收该信息, 得到服务端的IP地址; (2) 服务端监听端口号5020, 等待客户的密文信息, 服务端不断监听5020端口, 得到两两客户端集合后, 与客户端建立端口号1994的TCP连接, 返回交集数据, 客户端提取手机联系人信息, 进行加密处理; (3) 服务端密文对比, 返回客户端结果, 客户端解密服务端返回信息并显示。

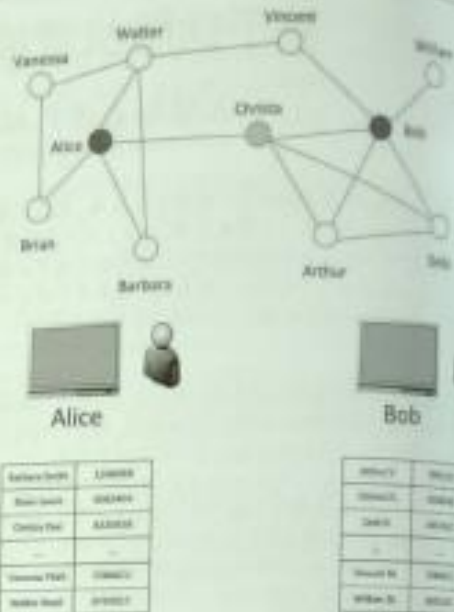


图1 基于伪随机置换朋友发现系统模型

2.2 模型分析

2.2.1 三要素服务器模型

以前的协议只能对半诚实的服务器保证安全, 因为服务器可以返回任意结果作为交集, 而客户端并不知道这是真正的交集。为了克服这一点, 本文作了如下改善:

设置和输入: 让 $F: \{0, 1\}^n \times U \rightarrow \{0, 1\}^n$ 为一个 PRP 和 $\lambda \geq 1$, P_1 和 P_2 分别将集合 $S_1 \subseteq U$ 和 $S_2 \subseteq U$ 作为输入, 而服务器有输出。

(1) P_1 选择集, 这样, 并把 P_1 发送他们; (2) P_2 检查是否正确, 否, 中止; (3) P_1 和 P_2 使用 F_{K_1} 构造一个随机排列; (4) 对于每一方, 发送集合 $T_i = \pi(F_{K_i}(S_i \cup \Delta_i))$ 到服务器, 且一个随机排列 $\Delta_i \subseteq D_i$; (5) 服务器返回交集 $J = T_1 \cap T_2$; 每一方 P_i 中止, 如果: (a) $D_i \subseteq F_{K_i}^{-1}(J)$ 或 $D_i \cap F_{K_i}^{-1}(J) \neq \emptyset$; 存在 $x \in S_i$, $x \notin F_{K_i}^{-1}(J)$ 和 $x \notin F_{K_i}^{-1}(J)$; (7) 每一方计算并返回 $(F_{K_i}^{-1}(J) \cap D_i)^c$ 。

2.2.2 洗牌算法

洗牌算法是对一组起始数列中的各个元素的位置进行重新调整, 以此得到新的数列。结合本文背景, 应用的洗牌算法如下:

已知有 N 个联系人, 在洗牌前将联系人信息放在数组 $array[N]$ 中, $0 \leq i < N$; 对随机数发生器进行初始化, 随机数 $(1-i)$ 之间的一个联系人, 与 $array[i]$ 交换; (减); 如果 $i < N$, 则跳到步骤2; 完成洗牌。

因为在该算法中, 本文将余下的联系人中的最后一个位置调整到刚刚抽掉的位置上, 而不是按抽掉的联系人位置部分全部前移, 所以在时间以及空间复杂度上都有一定的表现。

3 结语

针对当前朋友发现系统存在的隐私泄露问题,本文运用伪随机函数、混淆填充、洗牌算法对数据进行处理,保证了用户隐私数据的安全性,使其可以抵御社交网络的各种攻

击,使用户之间进行安全的信息匹配,达到了隐私保护的效果。在隐私保护越来越成为热点的趋势下,如何降低隐私保护方法的计算复杂度,提高服务质量,都有待进一步研究。

[参考文献]

- [1]LUCIANODA FC, OSVALDO N, OLIVEIRA JR, et al. Analyzing and modeling real-world phenomena with complex networks: a survey of applications[J]. *Advances in Physics*, 2011 (3): 329-412.
- [2]慕雨平.浅谈如何正确处理群众文化两个效益的关系[J]. *华章*, 2011 (1): 210-211.
- [3]GOLDWASSER S. Multi party computations: past and present[C]. *Washington: Proceedings of the 16th annual ACM symposium on principles of distributed computing*, 1997: 21-24.
- [4]YAO AC. Protocols for secure computations[C]. *Washington: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, 2008: 160-164.
- [5]EMILIANO D C, GENE T. Experimenting with fast private set intersection[J]. *Trust and Trustworthy Computing*, 2012 (7): 55-73.
- [6]GOLDREICH O, MICALI S, WIGDERSON A. A completeness theorem for protocols with honest majority[C]. *New York: Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, 1987: 218-229.
- [7]GOLDREICH O. Secure multi-party computation [EB/OL]. (1998-04-10) [2017-07-10]. <http://www.wisdom.weizman.ac.il/oded/pp.html>.
- [8]RAINER A, RUEPPEL. 计算机数据保护——序列密码的分析与设计[M]. 吕佩尔, 译. 北京: 人民邮电出版社, 1988.
- [9]WADE T, LAWRENCE CW. 密码学概论[M]. 邹红霞, 译. 北京: 人民邮电出版社, 2004.
- [10]DAVID S. 数据保密与安全[M]. 蔡建, 梁志敏, 译. 北京: 清华大学出版社, 2005.
- [11]ROGAWAY P, BELLARE M, BLACK J, et al. OCB: a block-cipher mode of operation for efficient authenticated encryption[J]. *Acm Transactions on Information & System Security*, 2001 (3): 196-205.

Friend find system based on pseudo random permutation

Wang Kaiyue, Zhang Zhengning, Du A'mei, Cui Hanxiao, Hu Jinguang

(Computer and Information Engineering College of Henan Normal University, Xinxiang 453007, China)

Abstract: In recent years, with the rapid development of mobile social software, portable mobile terminals have penetrated into all aspect of people's lives. In these software, people often use one of these functions——friend find. But this function is insecure for subscribers currently, vast quantities of privacy information is obtained by cloud service providers. Aiming at this phenomenon, the paper based on the current situation of comparison of privacy collections, friend find system based on pseudo random permutation is designed by using pseudo random permutation and secure multi-party computation protocol to improve. The system allows users to find the intersection of their collection and do not disclose information other than the intersection, with a certain value to promote.

Key words: mobile social; pseudo random permutation; privacy protection; friend find

4.其他类奖项

荣誉证书

王凯月 同志：

在河南省第八届翻译竞赛（笔译类英语非专业组）中荣获 三等奖，特颁发此证书，以资鼓励。



二〇一六年十二月九日