DOI：10.7652/xjtuxb201702003

支持加密搜索的定向息票安全投放框架

蒋精华[1,2]，桂小林[1]，郑宜峰[2,4]，张学军[1,3]，袁星亮[2,4]，王聪[2,4]
(1.西安交通大学电子与信息工程学院，710049，西安；2.香港城市大学计算机科学系，999077，香港；
3.兰州交通大学光电技术与智能控制教育部重点实验室，730070，兰州；4.香港城市大学深圳研究院，
518057，广东深圳)

摘要：针对移动终端息票定向投放服务中的隐私安全问题，提出一种支持加密搜索的定向息票安全投放框架。该框架根据息票定向投放过程中不同阶段的安全需求，通过使用多密钥可搜索加密技术实现移动终端用户只需要提交单个加密请求，就能在息票平台中对来自不同商家的加密息票进行安全高效的搜索，降低了系统的通信开销；同时结合局部敏感哈希技术和口令认证密钥交换协议，保证只有行为数据满足商家息票投放策略的移动用户才能获得息票，保护了移动终端用户的行为数据隐私和商家的息票投放策略。理论分析证明了该框架的安全性。实验结果表明，移动用户使用该框架获取10个商家的息票时所需计算时间为57.8 ms，带宽为2.9 KiB，能耗为8.7 J。所提框架在息票定向投放服务的安全性和性能方面取得了很好的平衡，适合在移动终端上使用，对设计安全、实用的定向投放应用具有一定的理论和实际意义。

关键词：隐私安全；息票投放；定向投放；加密搜索；行为数据
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2017)02-0013-07

A Framework of Secure Delivery Service for Targeted Coupons with Encrypted Search

JIANG Jinghua[1,2], GUI Xiaolin[1], ZHENG Yifeng[2,4], ZHANG Xuejun[1,3],
YUAN Xingliang[2,4], WANG Cong[2,4]
(1. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;
2. Department of Computer Science, City University of Hong Kong, Hong Kong 999077, China;
3. Key Laboratory of Opto-Technology and Intelligent Control Ministry of Education, Lanzhou 730070, China;
4. City University of Hong Kong Shenzhen Research Institute, Shenzhen, Guangdong 518057, China)

Abstract: A framework of secure delivery service of targeted coupons with encrypted search is proposed to solve privacy issues of users and vendors in delivery service of mobile targeted coupons. The proposed framework adopts a newly developed cryptographic primitive, called multi-key searchable encryption, which ensures that a user only needs to submit a single encrypted request to the coupon site so as to conduct secure and effective search over encrypted coupons from different vendors. Meanwhile, the framework ensures that eligible users can obtain targeted coupons without leaking their behavioral data while non-eligible users learn nothing beyond their non-eligibility status by combining locality-sensitive hashing with password

收稿日期：2016-09-12。 作者简介：蒋精华(1988—)，男，博士生；桂小林(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金资助项目(61472316，61572412)；陕西省科技计划资助项目(2016ZDJC-05)；中央高校基本科研业务费专项资金资助项目(XKJC2014008)；兰州交通大学光电技术与智能控制教育部重点实验室开放课题资助项目(KFKT2016-7)。
网络出版时间：2016-12-05 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20161205.1204.004.html

authenticated key exchange. Theoretical analysis proves the security of the proposed framework. Extensive experiments show that when a mobile user obtains coupons from 10 different vendors, the computation cost of the proposed framework is 57.8 ms, bandwidth cost 2.9 KiB, and energy cost 8.7 J. The proposed framework provides a well-balanced tradeoff between security and efficiency, and has certain theoretical and practical significance for the design of secure and practical targeted delivery systems.

Keywords: privacy security; coupon delivery; targeted delivery; encrypted search; behavioral data

随着网络和移动设备的普及,息票已成为一种新型商业促销工具,越来越受到商家和消费者的重视和欢迎[1]。商家可以通过息票吸引更多消费者,从而获得更多利润,也可以通过投放息票与已有的用户建立长期关系,而消费者则可以通过息票节省他们的开支。调查报告显示,90%的年轻人购物时会使用息票来节省开支[2]。

近年来,越来越多的商家通过集中的平台统一管理投放息票给用户,例如 Groupon、RetailMeNot 等。在息票投放过程中,定向投放日渐成为一种趋势。商家将息票及投放策略发布到息票平台,息票平台收集用户的行为数据,例如地理位置、浏览过的网页等,将息票投放给行为数据满足投放策略的用户。在该模式下,用户可以收到自己感兴趣的息票,减少经济开支;而商家的息票可以精准地投放给用户得以充分利用。然而,定向投放需要息票平台收集用户的行为数据[3],这给用户隐私造成了严重威胁[4-5]。如何在实现定向息票投放的同时保护用户隐私是一个亟待解决的重要问题。

针对定向投放服务中的用户隐私保护问题,研究者已经提出了一些解决方案[6-7],但是大多数集中于实现隐私保护的定向广告投放,这些技术方案无法直接适用于定向息票投放,因为定向息票投放服务除了要保护用户隐私,还有其他的安全需求。例如,息票必须投放给行为数据满足投放策略的用户,而不满足投放策略的用户不能获取关于投放策略的任何信息。为了在定向息票投放服务中同时保护用户隐私和商家的息票,Partridg 等和 Rane 等分别利用局部敏感哈希(locality-sensitive hashing,LSH)技术和模糊承诺(fuzzy commitment,FC)技术提出安全的定向息票投放框架[8-9],在他们的框架中,商家使用投放策略加密息票,然后将加密的息票投放给用户。如果用户的行为数据和息票的投放策略足够相似,即满足投放策略,则用户能正确解密息票,否则不能正确解密息票。虽然该框架可以支持安全的定向息票投放服务,但其针对的是商家直接投放息票给用户的场景,不适用现有的通过第三方息票平台统一管理投放息票的场景。

针对这一问题,本文提出一种支持商家通过第三方息票平台进行安全高效的定向息票管理投放的框架。该框架支持加密搜索,用户只需提交单个加密请求就可以搜索息票平台中来自不同商家的加密息票,息票平台进行加密搜索并返回匹配的加密息票给用户。在加密搜索的基础上,为了保护用户的行为数据隐私并实现商家息票的安全定向投放,该框架有效地结合 LSH 技术和口令认证密钥交换(password authenticated key exchange,PAKE)协议,保证用户的行为数据信息不会被息票平台和商家获取,同时只有行为数据满足投放策略的用户才能解密从息票平台搜索到的加密息票,而不满足投放策略的用户则无法获取关于投放策略的任何信息。安全分析表明,该框架能够有效地保护用户隐私和商家的息票及投放策略。实验结果表明,该框架给移动终端用户带来较小的计算、通信、能量开销,能支持高效的隐私保护移动终端定向息票投放服务。

1 问题定义

1.1 定向息票投放系统框架

现有的定向息票投放系统框架主要包含用户、商家和息票平台 3 个实体,如图 1 所示。用户为了节省经济开支希望通过息票平台搜索并获得感兴趣的息票,同时不想泄露自己的搜索关键词和行为数据给息票平台和商家。商家拥有息票并制定相应的投放策略,希望息票能精准地投放给行为数据满足投放策略的用户。息票平台从不同商家收集息票和相应的投放策略,并收集用户的相关信息,将息票投放给相关用户。

1.2 威胁模型

在定向息票投放系统框架中,本文所考虑的安全威胁因素主要有:息票平台可能试图获取用户的搜索关键词及行为数据,也可能试图获取商家的息

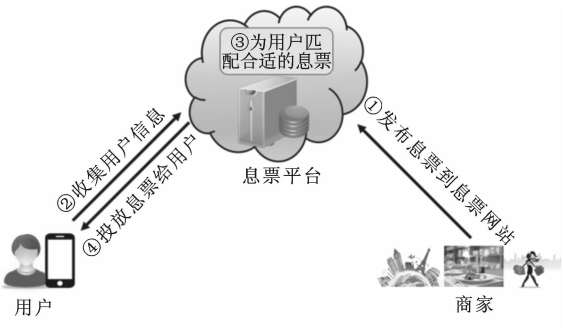

图 1　定向息票投放系统框架

票及投放策略；商家可能试图获取用户的行为数据；行为数据不满足息票投放策略的用户可能试图获取息票或关于投放策略的信息。和已有的工作[8-9]一样，本文不考虑用户兑换息票时的行为数据保护，因为用户兑换息票时商家不可避免地知道用户的行为数据满足息票投放策略这一信息，商家需要用户的兑换情况来改善其息票的投放策略。

2　支持加密搜索的定向息票安全投放框架

2.1　设计思路

为了使用户安全地搜索感兴趣的息票，该系统框架引入加密搜索。商家将加密的息票以及支持加密搜索的元数据（加密的息票关键词及对用户的授权信息）发布到息票平台，用户提交加密的关键词给息票平台，然后息票平台进行加密搜索并返回匹配的加密息票。已有的可搜索对称加密（searchable symmetric encryption，SSE）技术[10]可以实现加密搜索，但是针对不同商家加密的息票，需要用户提交多个加密请求，给资源受限的移动终端设备造成较大的通信开销。针对该问题，本文采用多密钥可搜索加密（multi-key searchable encryption，MKSE）技术[11]，用户只需要提交单个加密请求，息票平台便可搜索来自不同商家的加密息票。

在实现用户安全高效地搜索不同商家的加密息票的基础上，该系统框架进一步支持精准的定向息票投放。具体而言，只有行为数据满足投放策略的用户才能解密息票。和已有的工作[8]一致，本文使用 n 维向量表示用户的行为数据和息票的投放策略，当息票的投放策略和用户的行为数据相似时，即 2 个向量之间的距离小于给定阈值，则认为用户满足息票的投放策略。为了实现高效的相似性匹配计算，本文采用 LSH 技术处理用户行为数据向量和息票投放策略向量，使得相近的向量能高概率地被映射到相同值，这样用户行为数据和息票投放策略在距离上的相似性计算即可转化为相等性的比较。基于该思想，为了保护用户的行为数据隐私和商家的息票及投放策略，一个直接的方案是让商家使用 LSH 技术处理投放策略，然后使用其结果加密息票，用户使用 LSH 技术处理自己的行为数据，然后使用其结果解密从息票平台搜索到的加密息票，当用户行为数据满足投放策略时，即 LSH 技术处理的结果相等，用户方能解密息票。因为用户的行为数据没有离开本地设备，所以该方法可以有效保护用户隐私，因为只有行为数据满足投放策略的用户才能解密息票，所以该方法可以有效保护商家的息票，在该方法中，如果息票投放策略明文空间较小，则用户能通过离线穷举所有可能的投放策略去解密息票。

针对此问题，该系统框架引入 PAKE 协议，该密码协议允许双方协商一个会话密钥，当且仅当双方有相同的短口令时，双方才能得到一个相同的会话密钥。在该系统框架中，商家随机选择密钥对息票进行加密。用户从息票平台搜索到加密的息票后，通过与商家运行 PAKE 协议获得解密密钥。具体地，在 PAKE 协议中，用户以 LSH 技术处理的行为数据的哈希值作为其短口令，而商家以 LSH 技术处理的投放策略的哈希值作为其短口令。运行完 PAKE 协议后，用户和商家会在不知道对方输入内容的情况下分别得到一个会话密钥。商家使用其会话密钥加密息票的密钥，然后通过息票平台把密文发给用户，用户使用其会话密钥解密该息票密钥的密文，进而对息票进行解密。在该过程中，如果 LSH 技术处理的用户行为数据的哈希值与 LSH 技术处理的商家投放策略的哈希值相同（即用户行为数据满足商家投放策略），则用户可以正确解密息票。由于息票密钥的获取需要用户与商家在线运行 PAKE 协议，所以用户无法通过离线穷举的方式解密息票。

2.2　框架具体实现

基于上述的设计思路，本节将具体描述该系统框架的设计实现。息票的安全投放过程分为 3 个阶段：准备阶段、搜索阶段和解密阶段。

2.2.1　准备阶段　在准备阶段，商家加密息票并准备支持加密搜索的元数据，然后将其发布到息票平台，具体细节如下。

假设商家有一个息票 m，其对应的关键词为 w。商家随机选择密钥 k 加密息票为

$$c_m = E_k(m \| \sigma) \tag{1}$$

式中：$\sigma=\mathrm{Sig}(m)$是商家对息票的签名，用于验证息票的有效性。

商家为了保护息票的关键词 w 并支持用户加密搜索，使用其密钥 k_v 加密关键词 w 为

$$c_w = H_2(r, e(H_1(w), g_2)^{k_v}) \tag{2}$$

式中：$e: G_1 \times G_2 \rightarrow G_T$ 是乘法循环群 G_1、G_2、G_T 上的双线性映射，$e(g_1, g_2) \neq 1$，g_1 和 g_2 分别是 G_1 和 G_2 的生成元，$H_1: \{0,1\}^* \rightarrow G_1$ 和 $H_2: G_T \times G_T \rightarrow \{0,1\}^*$ 是哈希函数，r 是一个随机数。

如果商家授权密钥为 k_u 的用户对其加密息票进行搜索，则商家需要计算授权信息为

$$\Delta_{uv} = g_2^{k_v/k_u} \tag{3}$$

出于安全考虑，用户发送 g_2^{1/k_u} 给商家用于计算授权信息 Δ_{uv}，而不是直接发送密钥 k_u 给商家。

商家将加密的息票 c_m、加密的关键词 c_w、随机数 r、授权信息 Δ_{uv} 以及授权关系发布到息票平台。

2.2.2 *搜索阶段* 在搜索阶段，用户加密搜索关键词并提交给息票平台，息票平台根据授权关系搜索对应商家的加密息票，将匹配结果返回给用户，具体细节如下。

用户使用其密钥 k_u 加密关键词 w' 为

$$c_{w'} = H_1(w')^{k_u} \tag{4}$$

将其发送给息票平台。

息票平台收到用户发送的加密关键词后，先检查各个商家与该用户的授权关系。如果商家授权了该用户，即息票平台存储了相应的授权信息 $\Delta_{uv} = g_2^{k_v/k_u}$。此时，息票平台将用户的加密关键词 $c_{w'}$ 转化为能搜索对应商家加密息票的密文形式，即

$$c'_{w'} = e(c_{w'}, \Delta_{uv}) = e(H_1(w')^{k_u}, g_2^{k_v/k_u}) = e(H_1(w'), g_2)^{k_v} \tag{5}$$

针对加密息票 c_m，息票平台先取出 c_m 的加密关键词 c_w，并使用其对应的随机数 r 计算下式

$$c^*_{w'} = H_2(r, c'_{w'}) \tag{6}$$

通过比较息票的关键词 $c^*_{w'}$ 与 c_w 是否相等，来判断该商家的息票是否与用户的请求匹配，如果相等，则匹配(即 $w'=w$)，息票平台返回加密的息票 c_m，然后比较下一个息票，直到搜索完与用户有授权关系的所有商家的加密息票。

2.2.3 *解密阶段* 在解密阶段，用户收到加密息票后，通过息票平台与息票所属的商家运行 PAKE 协议，从而实现当用户的行为数据与商家的息票投放策略足够相似时，才可获取加密息票的密钥 k，否则用户不能获取息票和投放策略的信息，具体细节如下。

商家使用 LSH 技术处理投放策略向量 $\boldsymbol{a}$ 得 $\mathrm{LSH}(\boldsymbol{a})$，然后进行哈希操作得到 $h_v = H_3(\mathrm{LSH}(\boldsymbol{a}))$。用户也对自己的行为数据向量 $\boldsymbol{b}$ 进行相同的处理，得到 $h_u = H_3(\mathrm{LSH}(\boldsymbol{b}))$。

在开始描述具体协议之前，先介绍用户和商家共享的公开信息：素数 p 和有限域 Z_p、p 的一个有限循环群 G、G 的生成元 g、用户对应的元素 m_u ($m_u \in G$)、商家对应的元素 m_v ($m_v \in G$)。用户和商家通过息票平台运行 PAKE 协议具体如下。

用户生成随机数 x ($x \in Z_p$)并计算下式

$$X = g^x m_u^{h_u} \tag{7}$$

用户经由息票平台将 X 发给息票所属的商家。

商家生成随机数 y ($y \in Z_p$)，商家使用式(7)的结果分别计算下式

$$Y = g^y m_v^{h_v} \tag{8}$$

$$k_v = (X/m_u^{h_v})^y \tag{9}$$

商家使用式(8)和式(9)的结果计算会话密钥为

$$s_v = H(I_u, I_v, X, Y, h_v, k_v) \tag{10}$$

式中：I_u 和 I_v 分别为用户和商家的 ID。商家使用式(10)中的会话密钥 s_v 加密息票密钥 k 为

$$c_k = E_{s_v}(k) \tag{11}$$

商家经由息票平台将 Y 和 c_k 发送给用户。

当用户收到 Y 和 c_k 后，使用 Y 计算下式

$$k_u = (Y/m_v^{h_u})^x \tag{12}$$

用户使用式(7)、式(8)和式(12)计算会话密钥为

$$s_u = H(I_u, I_v, X, Y, h_u, k_u) \tag{13}$$

用户使用式(13)的会话密钥 s_u 解密式(11)加密的息票密钥为

$$k' = D_{s_u}(c_k) \tag{14}$$

在该协议中，商家的短口令为 h_v，用户的短口令为 h_u。根据式(7)～式(10)、式(12)、式(13)可知，如果 $h_u = h_v$，即用户的行为数据满足息票投放策略，则商家的会话密钥 s_v 和用户的会话密钥 s_u 相等，反之不相等。运行完 PAKE 协议后，商家用 s_v 加密息票的密钥 k 得到密文 c_k 如式(11)所示，然后通过息票平台转发给用户。如果用户的行为数据满足息票投放策略，则 $s_u = s_v$，根据式(11)和式(14)可知，此时用户可以正确解密 c_k 得到息票密钥，即 $k = k'$，从而正确解密息票；否则用户不能正确解密息票，此时用户除了知道其不满足要求外，无法获取关于投放策略的任何信息。同时，PAKE 协议的安全性使得商家也无法知道用户是否满足投放策略，即在息票定向投放过程中，商家无法知道关于用户行为数据的任何信息。用户正确解密息票后，可以对

息票进行兑换。此时，商家可以通过验证签名 σ 来检查息票的有效性。

在以上的 PAKE 协议中，即使用户搜索到来自多个商家的加密息票，也只需提交单个 PAKE 协议请求给息票平台，然后息票平台将其请求转发给对应的商家，即可完成和不同商家间的 PAKE 协议[12]。这样可以进一步减少用户的开销，即有效降低了用户移动设备的能量和带宽开销。

LSH 技术存在错误否定问题，即少量满足投放策略的用户不能正确解密息票；LSH 技术也存在错误肯定问题，即少量不满足投放策略的用户可以正确解密息票。错误否定不会给商家带来损失，所以少量的错误否定对商家来说是可以接受的。虽然错误肯定的存在会使少量不满足投放策略的用户获得息票，但是可以通过调节 LSH 技术的相关参数，极大地降低错误肯定发生的概率[8]，从而不破坏商家的利益。

3　安全性分析

本系统框架的安全性是由所使用的密码学技术 MKSE 和 PAKE 协议保证的，能够实现对用户数据隐私的保护以及对商家息票的保护。

3.1　用户数据隐私保护

在该系统框架的搜索阶段，我们使用了 MKSE 这一密码学技术来支持加密搜索。MKSE 协议的安全性是基于 bilinear Diffie-Hellman variant(BDHV)和 external Diffie-Hellman variant(XDHV)这 2 个密码学假设在随机预言模型下进行严格证明的[11]。MKSE 协议的安全性保证了用户的搜索关键词不会泄露给息票平台。一方面，用户发送给息票平台的关键词是由用户的密钥加密的，因此息票平台无法从收到的关键词密文获知用户的关键词明文；另一方面，为了搜索不同商家的加密息票，息票平台根据商家对用户的授权信息，将用户的加密关键词转换到对应商家密钥加密的密文，在这一过程中，因为授权信息是在用户与商家相互验证的情况下生成，息票平台无法对用户的加密关键词进行随意转换，所以息票平台仍无法获取用户的关键词，因此该框架可以有效保护用户的关键词。

在该系统框架的息票解密阶段，使用了 PAKE 这一密码学技术。PAKE 协议的安全性是基于 computational Diffie-Hellman(CDH)密码学假设在随机预言模型下进行严格证明的[13]。用户通过息票平台与商家运行 PAKE 协议，PAKE 协议的安全性保证了用户的行为数据信息不会泄露给息票平台和商家，因此该系统框架可以有效保护用户的行为数据。

3.2　商家息票保护

在本系统框架的准备和搜索阶段，MKSE 协议的安全性保证了商家的息票关键词不会泄露给息票平台和未授权的用户。商家使用其私钥加密息票关键词发布到息票平台，只有被授权用户的加密请求才能转换到该商家密钥的密文下进行搜索，因此未授权用户及息票平台无法获取商家息票的关键词。

在解密阶段，商家与用户运行 PAKE 协议，PAKE 协议的安全性保证了商家的投放策略不会泄露给息票平台和用户，同时保证只有满足投放策略的用户(即 PAKE 协议中的 $h_u=h_v$)才能解密 c_k，进而解密息票。不满足投放策略的用户除了知道自己不满足要求外，无法获取息票及投放策略信息，因此该系统框架可以有效保护商家的息票、关键词及投放策略。

由于息票密钥的获取需要用户与商家在线运行 PAKE 协议，所以用户无法通过离线穷举的方式解密息票，但用户可能试图通过线上猜测解密息票。本文框架可以采用一些方法缓解此威胁，如商家限制针对每个息票运行 PAKE 协议的次数，这样可以有效阻止单个用户或多个用户联合对单个息票进行不断的猜测攻击。

4　实验及结果分析

本文实现了一个定向息票安全投放服务的基本原型系统以评估本文框架的性能。该系统原型基于 Java 语言实现，客户端运行于 SamSung Galaxy S4 手机上，息票平台和商家端运行于一个双核 2.7 GHz 处理器和 8.0 GiB(Gi 为二进制的“兆”)内存的 PC 机上。实验主要从计算复杂度及时间、存储开销、通信开销和用户端能量开销 4 个方面评估该框架的性能。实验结果是执行 100 次的平均值。

4.1　计算复杂度及时间

本文提出的框架主要分为准备阶段、搜索阶段、解密阶段 3 个阶段。分别分析这 3 个阶段的计算复杂度及运行时间，各个阶段的计算复杂度见表 1。其中，商家的授权用户数为 n_{v-u}，每个用户对应的授权商家数为 n_{u-v}，每个商家的息票数为 n_{v-c}，每个息票的关键词数为 n_w，用户需要解密的息票所属的商家数为 n_{c-v}。

接下来测量该框架准备阶段、搜索阶段和解密

表 1 各阶段的计算复杂度

阶段	复杂度		
	商家	用户	息票平台
准备阶段	$O(n_{v-c}n_w+n_{v-u})$		
搜索阶段		$O(1)$	$O(n_{u-v}n_{v-c}n_w)$
解密阶段	$O(1)$	$O(n_{c-v})$	

阶段的具体计算时间。准备阶段的任务主要包括商家加密息票、加密关键词以及生成授权信息 Δ。实验中未测量息票的加解密时间，因为采用的是标准的 AES 加密算法，加解密时间取决于息票的大小，例如息票可能是息票码、文本、图片的形式。在加密关键词及生成授权信息方面，实验测得加密一个关键词需 31 ms，生成一个授权信息需 36 ms。图 2 给出了当商家授权用户数变化时，商家在准备阶段为一个息票准备元数据的时间开销(为简单起见，假设该息票有 10 个关键词，即 $n_w=10$)。由图 2 可以看出，商家的时间开销随着授权用户数的增加而线性增加，具体地，当授权用户数 n_{v-u} 为 100 时，商家准备一个息票的时间开销约为 3.9 s。

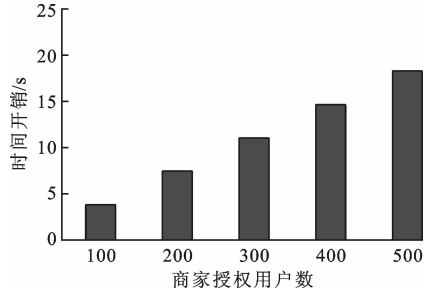

图 2 商家准备一个加密息票的时间开销($n_w=10$)

搜索阶段的计算开销主要有用户加密关键词的时间和息票平台使用授权信息将用户密钥加密的关键词转换成商家密钥加密的关键词的时间。实验中，在手机上测得用户加密一个关键词的时间为 9.9 s，注意用户加密关键词为一次性开销，即用户加密一次关键词，以后的搜索都可使用该加密的关键词。此外，测得息票平台转换一次关键词的时间为 20 ms。

在解密阶段主要测量用户通过息票平台与商家运行 PAKE 协议的时间。实验测得用户产生一个 PAKE 请求需 2.8 ms，而计算一个会话密钥的时间为 5.5 ms，所以在解密阶段用户的计算开销为 $(2.8+5.5n_{c-v})$ ms，用户运行 PAKE 协议的计算开销随需要解密的息票所属的商家数增加而线性增加。具体地，当需要解密的息票所属的商家数 $n_{c-v}=10$ 时，用户端的计算时间为 57.8 ms。此外，实验测得在 PAKE 协议中商家的计算时间为 2 ms。

4.2 存储开销

息票平台除了存储加密的息票外，还需存储息票的元数据，即加密的关键词和用户授权信息。实验中用 HMAC-SHA1 实现哈希函数 H_2，输出结果为 20 B，随机数 r 为 4 B，授权信息大小为 40 B，假设一个商家的息票数为 n_{v-c}，单个息票的关键词平均数为 n_w，该息票对应商家的授权用户数为 n_{v-u}，所以息票的元数据存储开销为 $(24n_{v-c}n_w+40n_{v-u})$ B，可以看出，对于一个商家，其元数据存储开销随息票数、息票关键词数和商家授权用户数的增加而增加，具体地，当 $n_{v-c}=1$，$n_w=10$，$n_{v-u}=100$ 时，元数据的存储开销约为 4.1 KiB。

4.3 通信开销

本实验中主要计算用户端的通信开销。用户端的通信开销来自搜索阶段和解密阶段。在搜索阶段，用户需提交加密的关键词给息票平台，加密关键词的大小为 40 B。在解密阶段，用户提交 PAKE 协议请求 X 给息票平台，然后通过息票平台收集对应商家的响应，即用于计算会话密钥的中间结果 Y 和加密的息票密钥 c_k，X 和 Y 的大小为 256 B，c_k 的大小为 16 B，假设用户运行 PAKE 协议的商家数为 n_{c-v}，则用户的通信开销为 $(40+256+(256+16)n_{c-v})$ B。图 3 给出了当息票对应的商家数变化时，用户端的通信开销，可以看出，用户端的通信开销随用户需要解密的息票对应的商家数 n_{c-v} 的增加而线性增加，当 $n_{c-v}=10$ 时，客户端通信开销约为 2.9 KiB。

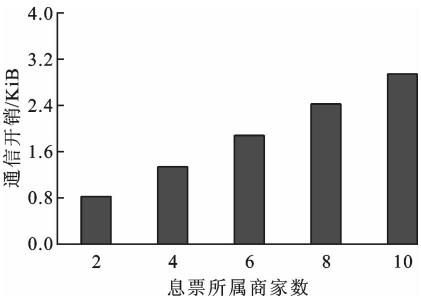

图 3 用户在解密阶段的通信开销

4.4 用户端能量开销

考虑到用户移动设备的资源受限，尤其是电池能量，所以本实验也测量了框架中用户端的能量开销。使用现有的 Power Tutor 2 Pro 工具分析用户端在计算方面的能耗，主要包括加密关键词和运行 PAKE 协议的开销，其中，运行 PAKE 协议的能耗

和用户所需要解密的息票对应的商家数相关。因此，用户的计算能耗随用户运行 PAKE 协议的商家数增加而增加。当商家数 $n_{c-v}=10$ 时，实验测得用户端的计算能耗为 8.7 J。为了直观体现该能耗对于移动设备来说是较小并可接受的，测量了播放 10 min 音频的能耗，结果为 10 J，因此本文所提出的框架对移动设备是适用的。

5　结　论

本文提出了一种适用于移动设备的定向息票安全投放框架。该框架支持用户安全高效地搜索感兴趣的加密息票，并且支持精准的定向息票投放。安全分析表明，该框架既能有效保护用户的隐私，又能保护商家的息票及投放策略。在 Android 平台上的实验结果表明，该框架具有较低的性能开销，适用于移动设备用户。在后续工作中，将考虑如何防止恶意用户通过伪造行为数据获取息票，进一步增强该框架的安全性。

参考文献：

[1] 柳欣，徐秋亮. 实用的强不可分割多重息票方案 [J]. 计算机研究与发展，2012，49(12)：2575-2590.
LIU Xin，XU Qiuliang. Practical multi-coupon schemes with strong unsplittability [J]. Journal of Computer Research and Development，2012，49(12)：2575-2590.

[2] ALISON G. Millennials use coupons more than their parents [EB/OL]. (2014-03-07) [2016-08-05]. http://www.businessinsider.com/millennials-use-coupons-more-than-parents-2014-3.

[3] 周傲英，周敏奇，宫学庆. 计算广告：以数据为核心的 Web 综合应用 [J]. 计算机学报，2011，34(10)：1805-1819.
ZHOU Aoying，ZHOU Minqi，GONG Xueqing. Computational advertising：a data-centric comprehensive web application [J]. Chinese Journal of Computers，2011，34(10)：1805-1819.

[4] 张学军，桂小林，伍忠东. 位置服务隐私保护研究综述 [J]. 软件学报，2015，26(9)：2373-2395.
ZHANG Xuejun，GUI Xiaolin，WU Zhongdong. Privacy preservation for location-based service：a survey [J]. Journal of Software，2015，26(9)：2373-2395.

[5] 张学军，桂小林，冯志超，等. 位置服务中的查询隐私度量框架研究 [J]. 西安交通大学学报，2014，48(2)：8-13.
ZHANG Xuejun，GUI Xiaolin，FENG Zhichao，et al. A quantifying framework of query privacy in location-based service [J]. Journal of Xi'an Jiaotong University，2014，48(2)：8-13.

[6] GUHA S，CHENG B，FRANCIS P. Privad：practical privacy in online advertising [C]// Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation. Berkeley，CA，USA：USENIX Association，2011：169-182.

[7] BACKES M，KATE A，MAFFEI M，et al. Obliviad：provably secure and practical online behavioral advertising [C]// Proceedings of the 33rd IEEE Symposium on Security and Privacy. Piscataway，NJ，USA：IEEE，2012：257-271.

[8] PARTRIDGE K，PATHAK M A，UZUN E，et al. Picoda：privacy-preserving smart coupon delivery architecture [C]// Proceedings of the 5th Workshop on Hot Topics in Privacy Enhancing Technologies. Berlin，Germany：Springer-Verlag，2012：94-108.

[9] RANE S，UZUN E. A fuzzy commitment approach to privacy preserving behavioral targeting [C]// Proceedings of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments. New York，USA：ACM，2014：31-35.

[10] CURTMOLA R，GARAY J，KAMARA S，et al. Searchable symmetric encryption：improved definitions and efficient constructions [C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. New York，USA：ACM，2006：79-88.

[11] POPA R A，ZELDOVICH N. Multi-key searchable encryption [EB/OL]. (2013-08-17)[2016-09-05]. http://eprint.iacr.org/2013/508.pdf.

[12] LIU J，ASOKAN N，PINKAS B. Secure deduplication of encrypted data without additional independent servers [C]// Proceedings of the 22nd ACM Conference on Computer and Communications Security. New York，USA：ACM，2015：874-885.

[13] ABDALLA M，POINTCHEVAL D. Simple password-based encrypted key exchange protocols [C]// Proceedings of the the Cryptographers' Track at the RSA Conference. Berlin，Germany：Springer-Verlag，2005：191-208.

（编辑　武红江）