基于非交互零知识证明的匿名电子调查系统

柳璐，李宇溪，周福才
（东北大学软件学院，辽宁 沈阳 110819）

摘　要：针对电子调查存在的不少安全问题，如信息欺骗、隐私安全等，构建了一个基于非交互零知识证明（NIZK，non-interactive zero knowledge proofs）的匿名电子调查系统，系统具有自组织、非交互、防重放、更安全等特点。系统采用 NIZK 协议和 Boneh-Boyen 签名方案对用户的身份进行非交互式的验证，保证了系统的真实性；系统还采用 Pedersen 承诺方案和伪随机函数对用户的身份和相关信息进行隐藏，保证了系统的匿名性。安全性分析表明，系统具有抵抗恶意用户并发攻击和匿名性等安全特性。最后，对系统的功能进行了仿真并验证，结果表明，系统能够正确完成各项功能，并有效地保证系统的匿名性与真实性。

关键词：匿名电子调查；NIZK；真实性；匿名性
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2016.00121

Anonymous survey system based on NIZK

LIU Lu, LI Yu-xi, ZHOU Fu-cai
(Software College, Northeastern University, Shenyang 110819, China)

Abstract：Aiming at the security problem that the existing in electronic surveys, such as information fraud, privacy security etc. An anonymous electronic survey scheme based on non-interactive zero knowledge proofs (NIZK) was constructed, which had the characteristics of self-organization, non-interactive, anti-replay, and high efficiency. The system uses the NIZK protocol and the Boneh-Boyen signature scheme to verify the user's identity in non-interactive manner, which guarantees the authenticity of the scheme. The system also uses the Pedersen commitment scheme and the pseudo random function to hide the user’s identity and the related information, which guarantees the anonymity. Security analysis show that the system has security features such as malicious users attack resistance and anonymity. Finally, the function of the system was also verified and the result show that the system can accomplish all the functions correctly and guarantee the anonymity and authenticity of the system effectively.

Key words：anonymous electronic survey, NIZK, authenticity, anonymity

---

收稿日期：2016-09-03；**修回日期：**2016-10-17。**通信作者：**周福才，fczhou@mail. neu, edu. cn
基金项目：国家科技重大专项基金资助项目（No.2013ZX03002006）；辽宁省科技攻关基金资助项目（No.2013217004）；辽宁省博士启动基金资助项目（No.20141012）；中央高校基本科研业务费专项资金资助项目(No.130317002)；沈阳市科技基金资助项目（No.14231108）；国家自然科学基金资助项目（No.61472184, No.61321491, No.61272546）
Foundation Items: The National Science and Technology Major Project (No.2013ZX03002006), The Science and Technology Project of Liaoning Province (No.2013217004), The Doctor Startup Fund of Liaoning Province (No.20141012), The Fundamental Research Funds for the Central Universities (No. N130317002), The Shenyang Science and Technology Projects (No.14231108), The National Natural Science Foundation of China (No.61472184, No.61321491, No.61272546)

1 引言

电子调查是指以网络为媒介，通过在线发布调查问卷的形式来收集相关调查数据的一种调查手段[1]。电子调查伴随着网络信息技术的发展，逐渐被广大的网民群众所接受。人们通过参与网络电子调查，无需面对面即能方便地表述个人的观点和建议。与传统的调查方式相比，电子调查具有调查成本低、实时性强、不受时间和空间的限制、互动性强、调查结果更易于收集和统计等优点[2,3]。2012 年，美国调研机构 IBISWorld 的新榜单列出了最适合创业者的行业，其中，电子调查软件赫然在列，这表明在电子调查领域还有很大的发展空间。电子调查正逐渐被我国广泛使用[4]，中国政府网（www.gov.cn）也专门开辟了一个电子调查的板块用于进行民意调查。现在国内已有很多调查公司或者研究机构开发了一些专用的调查系统，如“问卷星”“第一调查网”“51 调查网”等。

目前，电子调查已经在电子商务、新闻媒体、电子政务、网络教学等领域有着广泛的应用。但网络的急速发展也给电子调查带来一些新的挑战。作为开放性的网络环境，人们在参与电子调查时可以填写自己的意见，但这些不一定真实，可能存在恶意用户随意填写结果。如果恶意结果很多，会造成调查结果的错误统计。除此之外，一些调查可能会涉及人们的个人隐私问题，如果泄露可能会给用户带来困扰，这也使一些人不愿意参与或者不愿填写真实情况。这些都制约了电子调查的发展。

与此同时，满足调查系统对真实性和匿名性的要求，有些系统引入了第三方机构。但第三方机构也无法做到绝对安全，它们有可能或主动或被动地将数据泄露，如数据库遭到破坏等。因此，如何不引入第三方调查机构，而是由调查者自己开展调查，便成为了最近研究者的研究热点。一些在电子投票方案和匿名证书系统中使用的技术，如盲签名、比特承诺等，可以为解决这类问题提供一些参考[5,6]。这些方法虽然都较好地保证了电子调查的安全性（匿名性），但是这些方法严重破坏了电子调查的易用性，而且也加重了系统的负担。2014 年，Hohenberger 等[7]将非交互式零知识证明技术应用在电子调查中，很好地解决了安全性和效率等问题，得到了广大学者们的关注。

本文在研究电子投票系统和电子调查系统的基础上，将其与 NIZK 协议[8]、Boneh-Boyen 签名方案、Pedersen 承诺方案和伪随机函数[9]等方法相结合，以保证系统的真实性和匿名性，从而实现一个基于非交互式零知识证明的匿名调查系统。本文给出了系统的实体构成、形式化定义以及安全性定义。与此同时，给出了算法的具体描述以及安全性证明：系统具有抵抗恶意用户并发攻击和匿名性等安全特性。最后对系统进行仿真，结果表明该系统能够实现一次调查的全过程（发起调查、参与调查、提交调查结果、发布与统计结果等），同时能满足电子调查对真实性和匿名性的要求。

2 相关工作

2.1 Boneh-Boyen 签名方案

Boneh-Boyen 签名方案是一个基于配对的短签名，该签名方案是根据 Boneh 和 Boyen[10]这 2 个人在 2004 年提出的一个新的 IBE（identity based encryption）方案转化过来的。Boneh-Boyen 签名方案的具体执行过程如下。

1) $Gen(1^n)$：生成签名所需要的公私钥。随机选取一个整数 $\alpha \in Z_q$ 作为签名者的私钥 sk。选取一个阶为素数 q 的群 G 和群的生成元 u,v,g,h。计算 $U=e(g,g)^{\alpha}$，则验证的公钥为 $vk=(u,v,g,h,U)$。

2) $Sign(sk,m_0,m_1)$：签名者欲对消息 m_0、m_1 进行签名，则签名者随机选取一个整数 $r \in Z_q$，计算 $\sigma_1 \leftarrow g^{\alpha}(u^{m_0}v^{m_1}h)^r$ 和 $\sigma_2 \leftarrow g^r$，则签名者将 (σ_1,σ_2) 作为签名值输出。

3) $Verify(vk,m_0,m_1,\sigma_1,\sigma_2)$：验证者验证签名是否有效。验证者需要验证等式 $e(\sigma_1,g)=Ue(u^{m_0}v^{m_1}h,\sigma_2)^r$ 是否成立。如果等式成立，则接受该签名；否则拒绝接受签名。

可以看出，Boneh-Boyen 签名方案的一个特点是可以同时对 2 个消息进行签名，这使该签名方案的签名效率更高。

2.2 Pedersen 承诺方案

目前，最常用的承诺方案是 Pedersen 承诺方案，该方案是一种计算绑定、完美隐藏的承诺方案，而且承诺值是均匀分布的[11,12]。Pedersen 承诺方案的完美隐藏性不依赖于任何困难性假设，但它的计算绑定性依赖于求离散对数的困难性，即离散对数假设。Pedersen 承诺方案可分为 3 个阶段。

1) 初始化：假设 g,h 是群 G（阶为 q）的 2 个生成元。$\log_g h$ 是未知的，即离散对数的计算是不可行的。

2) 承诺阶段：承诺者想要承诺一个整数 $m \in Z_q$，首先选择一个随机数 $r \in Z_q$，然后计算承诺值 $c = C(m,r) = g^m h^r$，最后将承诺者 c 发送给接收者。

3) 打开阶段：承诺者可以选择一个适当的时机将承诺打开。打开时，承诺者将承诺的消息 m 和选取的随机数 r 发给接收者，接收者计算 $c' = g^m h^r$ 并与他之前接收到的承诺值 c 进行比较，看是否相等。如果相等，则正确打开承诺；否则，就拒绝承诺。

2.3 非交互零知识证明

概括地讲，一个非交互式零知识证明系统由一个公共参考串生成算法 K（由可信第三方来运行）、一个证明者 P 和一个概率多项式时间的验证者 V 构成[13,14]。给定安全参数 n，公共参考串算法生成一个多项式长度的公共参考串 σ。证明者 P 将公共输入 x、相应的证据 ω 以及公共参考串 σ 作为输入，生成一个证明 π。验证者 V 验证三元组 (x,σ,π) 并输出接受或者拒绝。

3 基于 NIZK 的匿名调查系统

3.1 实体构成

目前的电子调查系统一般都需要多方参与，分别为调查发起者、被调查者、注册机构、统计机构。统计机构又被认为是第三方信任机构。通常认为统计机构不会泄露相关用户的身份和调查信息，是可信的。事实上，引入第三方信任机构会带来较大的风险，并且使整个电子调查系统变得更加复杂。为保证电子调查系统对真实性和匿名性的要求，基于 NIZK 的电子调查系统由 3 种实体构成。

1) 注册机构（RA，registration agency）是一个记录注册信息的机构，主要负责生成系统公共参数和返回给用户的签名公私钥对。注册机构只有唯一的一个，且并不参与调查的其他过程。

2) 调查机构（SA，survey agency）作为调查的发起者和结果的接收者，担负着调查机构和统计机构的双重任务。

3) 用户（user）作为最重要的一方，旨在和注册机构和调查机构进行交互, 以完成包括注册、参与调查及验证等过程。

用户和调查机构实际上都属于用户实体。本文基于它们在一次调查中的不同职能将用户分为两类。一个用户既可以作为调查机构来发起调查，也可以是其他调查的参与者。系统的架构如图 1 所示。

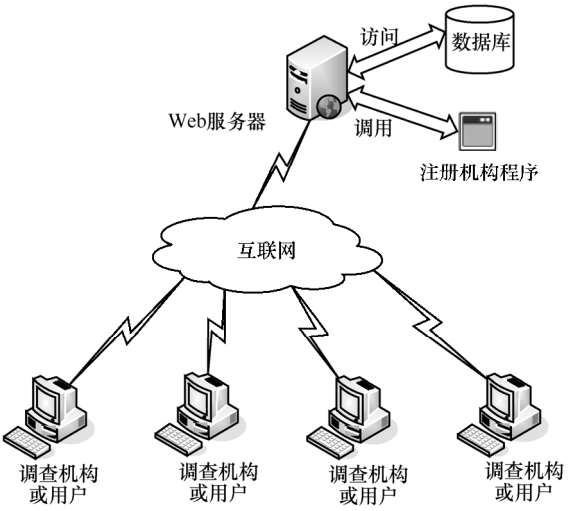

图 1　系统架构

用户在最初与 Web 服务器（作为注册机构）交互，完成注册。成功后获得自己的主密钥。

用户成为调查机构发起调查时，需生成调查密钥对，并将公钥提交给 Web 服务器。此时，Web 服务器接管了调查具体过程的实现。调查机构直接发布相关调查信息到 Web 服务器。

用户选择某次调查后，可根据调查信息在本地调用程序生成一次令牌及验证参数，将其与填写的调查结果一起发送给 Web 服务器。Web 服务器验证成功则保存数据，否则丢弃。

3.2 形式化定义

基于 NIZK 的电子调查系统由以下算法或协议组成，每个算法或协议的具体描述如下。

1) $(RA_{pk}, RA_{sk}) \leftarrow GenRA(1^n)$：注册机构初始化算法。该算法由注册机构执行，用于生成注册机构的公私钥对。

2) $(SA_{pk}, SA_{sk}) \leftarrow GenSA(1^n, RA_{pk})$：调查机构初始化算法。该算法由调查机构执行，用于生成调查机构的公私钥对。

3) $RA_{out}(O_{id}), User_{out}(cred_{id}) \leftarrow Reg(RA_{in}(1^n,)$ $RA_{pk}, RA_{sk}) User_{in}(id, a, r, c, z_1, z_2)$：注册协议。该协议是由注册机构和用户之间运行协议，以供新用户生成自己的主密钥。

4) $L_{sid} \leftarrow GenSurvey(1^n, sid, L, SA_{pk}, SA_{sk})$：创建调查算法。该算法由调查机构执行，用于生成某次调查的调查公钥。

5) $Sub = (tok, m, tokauth) \leftarrow Submit(1^n, sid, L_{sid},\ m,$ $cred_{id})$：生成结果算法。该算法由用户执行，用于生成用户的调查结果。

6) $Out \leftarrow Authorized(id, sid, SA_{pk}, L_{sid})$：资格审核算法。该算法用于检查某用户是否是某次调查的合法用户。

7) $Out \leftarrow Check(id, L_{sid}, SA_{pk}, SA_{sk}, Sub)$：结果验证协议。该协议是由调查机构 *SA* 和用户 *User* 之间运行的两方交互协议，用于检查用户提交的调查结果是否有效。

3.3 安全性定义

一个安全的电子调查系统应该满足 2 个安全特性：真实性和匿名性。

3.3.1 匿名性

匿名性（anonymity）是指，假设注册机构 RA 和调查机构 SA 都是恶意的，那么即使它们知道某些调查信息，仍无法区分出这 2 个调查结果对应于哪个合法的被调查者。

定义 1 匿名性：给定一个匿名调查系统 Γ，令 *A* 为一个自适应敌手，*C* 为一个挑战者。考虑下面的实验 $EXEC^b(1^n, A)$。

敌手 *A* 任意生成一对注册机构 RA 的签名公私钥 (RA_{pk}, RA_{sk})，任意选取 2 个不同的合法用户 id_0 和 id_1，并获得其主密钥，则敌手 *A* 可以向 *Submit* 预言机发起 $Submit(1^n, \cdots, cred_{id})$ 询问。然后敌手 *A* 选取一个调查机构的公钥 SA_{pk} 并创建一个调查，其中，调查标识符为 *sid*，调查公钥为 L_{sid}，并且 id_0 和 id_1 都是该调查的合法用户，m_0 和 m_1 是这 2 个用户在此次调查中填写的调查内容。

对于 $l, j \in \{0,1\}$，如果算法 $Authorized(id_l, sid, pk_{SA}, L_{sid})$ 输出标识符 *Fail* 或者敌手 *A* 已经向预言机查询过 $Submit(1^n, sid, \cdot, m_j, cred_{id_l})$ 的话，则实验输出标识符 *Fail*。

当 l=0 和 l=1 时，挑战者 *C* 分别计算 $Sub_l = Submit(1^n, sid, pk_{sid}, m_l, cred_{id_{l\oplus b}})$，并将得到的结果 Sub_0 和 Sub_1 发送给敌手 *A*。最后敌手 *A* 根据以上内容输出一个字符 *b*。

定义敌手 *A* 获胜的优势为

$$Adv_A(n) = |\Pr[EXEC^0(1^n, A) = b] - \Pr[EXEC^1(1^n, A) = b]|$$

如果对于所有 PPT 敌手 *A* 都只能有最多可忽略的优势在上述实验中获胜，则称该电子调查系统是匿名的。

3.3.2 抵抗恶意用户攻击性

抵抗恶意用户攻击性是指，即使敌手能够注册多个用户，并且能够选择查看调查中任意用户的调查结果，也只有合法的用户才能完成调查，并且他们提交的调查结果只能有一个被计入到总的调查结果中。

定义 2 抵抗恶意用户攻击性，给定一个匿名电子调查系统 Γ，令 *A* 是一个自适应的敌手，*C* 是一个挑战者，考虑下面的实验。

挑战者 *C* 运行 $GenRA(1^n)$ 算法得到注册机构的公钥 RA_{pk} 与私钥 RA_{sk}。挑战者 *C* 运行 $p(n)$ 次 $GenSA(1^n)$ 算法得到 $p(n)$ 个调查机构的公钥 SA_{pk} 与私钥 SA_{sk}。在接下来的实验中，敌手 *A* 可以访问 $GenSurvey(1^n, \cdots, RA^i_{sk})$ 预言机和 $Submit'(1^n, \cdots, RA_{pk}, RA_{sk})$ 预言机。

敌手 *A* 并发地使用自适应选择、唯一的用户（身份标识符为 $id \in \{0,1\}^n$）来与用户注册协议 Reg 进行交互。令 L' 表示敌手 *A* 在这个并发的交互过程中所选取用户身份的集合。

敌手 *A* 在 1~ $p(n)$ 中随机选取一个整数 *i*，接着敌手 *A* 为第 *i* 个调查选取调查标识符 *sid*，并选取该调查的被调查者集合 *L*。挑战者 *C* 运行 $GenSurvey(1^n, sid, L, SA^i_{sk})$ 算法生成该调查的调查公钥 L_{sid} 并将其发送给敌手 *A*。敌手 *A* 根据上面得到的内容生成调查结果集合 *S*。

当下述 4 个条件有一个满足时，实验输出提示符 *Success*。

1) $|S|>|L\cap L'|$。

2) 对于所有的 $Sub\in S$，协议 $Check(sid,L_{sid},RA_{pk},SA_{pk},Sub)$ 都输出提示符 *Accept*。

3) 对于 $(tok,m,tokauth)\in S$ 和 $(tok',m',tokauth')\in S$，$tok\neq tok'$。

4) 对于所有的 $(tok,m,tokauth)\in S$，当敌手 A 向 Submit′ 预言机提出关于调查标识符为 *sid* 的询问时，$(tok,m,tokauth')$ 不会作为 Submit′ 预言机的一个输出。

定义敌手 A 的获胜情况为在实验中输出提示符 *Success*，如果对于所有 PPT 敌手在上述实验中获胜的概率至多为 $\mu(n)$，其中，$\mu(\cdot)$ 是一个可忽略函数，且 $n\in N$，则称该匿名电子调查系统是抵抗恶意用户并发攻击的。

3.4　算法描述

基于 NIZK 的匿名调查系统 Γ 由 3.2 节描述的 7 个算法或协议组成，具体如下。

1) GenRA 算法

设 G 是阶为素数 p 的双线性群，且存在双线性映射 $e:G\times G\to G_T$。

①注册机构随机挑选一个 G 的生成元 $g\in G$ 和一个随机数 $x\in Z_q$，使 x 作为私钥。同时，随机选取 $u,v,h\in G$。

②用双性配对计算 $U=e(g,g)^x$。将 (g,u,v,h,U) 作为公钥。

2) GenSA 算法

①调查机构选取随机数 $y\in Z_q$，使 y 作为私钥。同时，随机选取 $u_v,v_v,h_v\in G$。

②调查机构根据 RA 公钥选取的生成元 $g\in G$、私钥 y 和 u_v,v_v,h_v 计算 $U_v=e(g,g)^y$。将 (g,u_v,v_v,h_v,U_v) 作为公钥。

3) Reg 协议

①身份标识符为 *id* 的用户随机选取 $S_{id},d\in Z_q$，并计算承诺值 $a=v^{S_{id}}g^d$。将 (id,a) 发送给 RA。

②生成其他验证参数：随机选取 $b_1,b_2\in Z_q$，计算 $r=v^{b_1}g^{b_2}$。

③挑战值 c 由随机预言机 H 生成，即 $c=H(g,RA_{pk},id,a,r,0^n)$；根据 c 计算出 $z_1=b_1+c\cdot S_{id}$，$z_2=b_2+cd$。将 NIZK 验证参数 r,c,z_1,z_2 一起发送给 RA。

④注册机构接到承诺参数 a 和 NIZK 验证参数 r,c,z_1,z_2 后，进行验证：$v^{z_1}g^{z_2}=a^cr$。如果不等，则注册机构输出标识符 *Out=Fail*。如果证明成功，则注册机构输出标识符 *Out=Success*，并使用其私钥用签名方案中的签名算法 *Sign* 来对用户的承诺值和身份标识符进行签名 $O_1\leftarrow g^x(u^{id}ah)^r$，$O_2\leftarrow g^r$，将签名值记为 $O_{id}=(O_1,O_2)$。然后注册机构将签名值 O_{id} 发给用户。

⑤用户得到签名值后，先进行签名的验证算法 *Verify*，即计算

$$e(O_1,g)=Ue(u^{id}v^{S_{id}}g^dh,O_2)$$

⑥验证成功则用签名生成主密钥

$$cred=\left(id,S_{id},O_1'=\frac{O_1}{O_2^{\,d}},O_2\right)$$

4) GenSurvey 算法

①对于调查名单 L 中的每一个用户 *id*（即 $id\in L$），调查机构使用其签名私钥对用户身份符 *id* 和调查表示符 *sid* 一起签名，将签名值记为 $SO_{id}=(g^y(u_v^{sid}v_v^{id}h_v)^{r'},g^{r'})$。

②算法输出调查公钥 L_{sid}，即二元组 $L_{sid}=(sid,\{id_i,SO_{id_i}\}_{i\in L})$ 的集合。

5) Submit 算法

①用户根据 *id* 寻找到 L_{sid} 中的 SA 签名对 $SO_{id}=(SO_1,SO_2)$。

②计算对应于该调查的一次令牌，即 $tok=e(g,g)^{\frac{1}{S_{id}+sid}}$。

③填写调查结果 m。

④生成 NIZK 证据 π：首先，将主密钥随机化，通过随机选取两个整数 $d_1,d_2\in Z_q$，并计算 $s_1=O_1(u^{id}v^{s_{id}}h)^{d_1}$，$s_2=O_2g^{d_1}$，$s_3=SO_1(u_v^{sid}v_v^{id}h_v)^{d_2}$，$s_4=SO_2\cdot g^{d_2}$ 然后，用户生成其他验证参数

$$E_1\leftarrow e(J_1,g)e(u^{b_1}v^{b_2},s_2)^{-1}$$

$$E_2\leftarrow e(J_2,g)e(v_v^{b_1},s_4)^{-1}$$

$$E_3\leftarrow tok^{b_2}$$

其中，J_1,J_2 为群 G 的群元素，b_1,b_2 为整数域 Z_q 上的 2 个随机数，均由用户随机选取。接着，还需生成验证参数 c。

$$c'=H(sid,SA_{pk},id,E_1,E_2,E_3,1^n)$$

用户根据 c' 计算出

$$z_1 \leftarrow b_1 + c \cdot id, z_2 \leftarrow b_2 + cs_{id}$$

$$z_3 \leftarrow s_1^c J_1, z_4 \leftarrow s_3^c J_2$$

将 π=$s_2, s_4, E_1, E_2, E_3, c', z_1, z_2, z_3, z_4$ 发送给调查机构。

⑤算法输出调查结果 $Sub = (tok, m, \pi)$。

6) Authorized 算法

①在调查公钥 L_{sid} 中选择某条记录 (id, SO_{id})。

②验证

$$e(SO_1, g) = U_v e(u_v^{sid} v_v^{id} h_v, SO_2)$$

若 3 次验证均通过，则算法输出 Out=Yes，否则算法输出 Out=No。

7) Check 协议

调查机构在接收到调查结果 *Sub* 后，验证以下式子。

$$E_1 e(g,g)^{xc} e(h, s_2)^c = e(z_3, g) e(u^{z_1} v^{z_2}, s_2)^{-1}$$

$$E_2 e(g,g)^{yc} e(u_v^{sid} h_v, s_4)^c = e(z_4, g) e(u^{z_1}, s_4)^{-1}$$

$$E_3 e(g,g)^c tok^{-c(sid)} = tok^{z_2}$$

如果 3 个式子均成立，则表明验证通过，则调查机构将输出 Out=Yes，并将结果 m 和一次令牌值 *tok* 记录到数据库。若不通过，则调查机构不承认此调查结果，不予记录。

3.5 安全性证明

3.5.1 匿名性

根据定义 1, 实验 $EXEC^b(1^n, A)$ 的最后将输出 2 个调查结果 Sub_0 和 Sub_1，形式都为 $Sub_i = (tok_i, m_i, \pi_i)$ ($i \in \{0,1\}$), 其中，tok_i 为一次令牌，m_i 为调查内容，π_i 为非交互式零知识证明。但它们的意义不同：对实验 $EXEC^0(1^n, A)$ 来说，输出的 2 个调查结果 Sub_0 和 Sub_1 分别是由 $cred_{id_0}$ 和 m_0 与 $cred_{id_1}$ 和 m_1 所产生的，而对实验 $EXEC^1(1^n, A)$ 来说，则分别是由 $cred_{id_0}$ 和 m_1 与 $cred_{id_1}$ 和 m_0 所产生的。

非交互式零知识证明的一个重要特性：证据不可区分性，敌手无法区分哪个用户填了哪个内容，即无法区分 m_0 是由 $cred_{id_0}$ 还是 $cred_{id_1}$ 产生。因此也就无法区分出实验 $EXEC^0(1^n, A)$ 和 $EXEC^1(1^n, A)$。

3.5.2 抵抗恶意用户攻击性

根据定义 2，只有当安全性定义中的 4 个条件同时成立时，实验才输出 *success*。如果实验最终输出 *success* 的概率为可忽略的, 则称匿名调查系统具有抵抗恶意用户攻击性。

条件 1) 和条件 4) 是实验的前提条件和基本要求，是实验所必须要满足的，否则就违反了逻辑的合理性。根据上面的分析，敌手 *A* 在其生成的所有调查结果 $(tok, m, tokauth)$ 中至少有一个调查结果是敌手在不知道用户主密钥的情况下生成的。

条件 2) 表述的意思为敌手生成的所有调查结果都能通过调查结构的验证。因此，如果该条件成立，则意味着敌手伪造的调查结果是有效的。

条件 3) 表述的意思为敌手生成的所有调查结果都有不同的一次令牌值。如果该条件成立，则意味着敌手伪造的调查结果中的一次令牌和其他调查结果中的一次令牌是不同的。但本文假设承诺方案和签名方案都是安全的，即承诺方案具有隐藏性和绑定性，签名方案具有不可伪造性、不可否认性等安全特性。而在具体实现的系统中，本文使用的是 Pedersen 承诺方案和 Boneh-Boyen 签名方案。Pedersen 承诺方案具有完美隐藏性，即承诺者生成的任何承诺值的分布都是相同的，而 Boneh-Boyen 签名方案具有普通签名方案所具有的一切安全特性。因此敌手不能伪造出一个合法的调查结果且生成的调查结果的一次令牌不会都是新的而且互不相同，即条件 2)和条件 3)对敌手来说是无法满足的。

综上，实验最终不能以不可忽略的概率输出 success，因此系统具有抵抗恶意用户攻击性。

4 仿真实现

4.1 开发环境

本节对设计的系统进行了仿真实现。系统仿真原型基于 Linux 平台，操作系统为 Ubuntu-12.04-server-i386 系统。散列函数的实现采用了 openssl-1.0.2a 开发包。双线性配对的运算主要使用的是斯坦福大学 Ben Lyn 开发的 PBC 库。PBC 库主要用于配对密码系统上的数学运算，而且该库是免费的。PBC 库中提供了很多库函数，如椭圆曲线生成函数、椭圆曲线算法和配对运算等，使用者可以直接使用它们而不需要考虑实现的细节。

4.2 系统验证

系统实现的主要功能包括用户注册、创建调查、参与调查、资格审核以及公布结果等。

1) 用户注册部分。首先用户选取私钥，并在本地计算生成关于私钥的承诺值和 NIZK 证明，如图 2 所示。然后用户将承诺值和 NIZK 证明等内容发送给 Web 服务器（注册机构），Web 服务器进行验证。如果验证通过，Web 服务器返回“ 注册成功 ”的提示，并为用户提供签名值的下载链接，如图 3 所示。用户下载 Web 服务器（注册机构）生成签名值，计算并生成自己的主密钥，如图 4 所示。

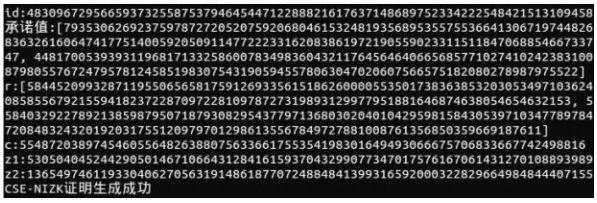

图 2　生成 NIZK 证明

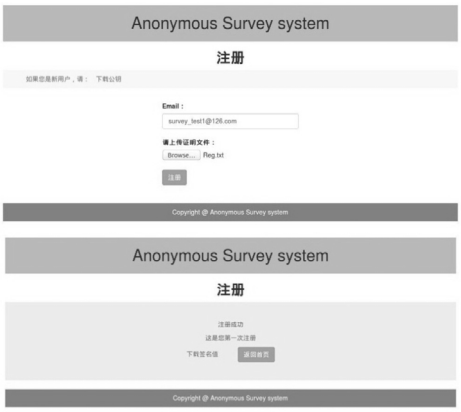

图 3　用户注册

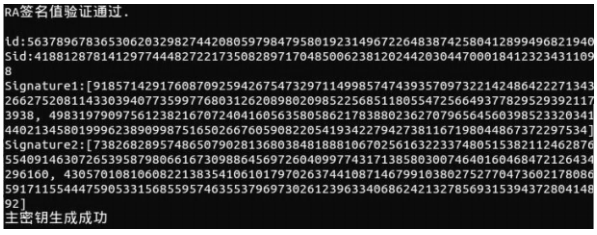

图 4　生成主密钥

2) 创建调查部分。首先调查机构输入调查名称，并提交被调查者的名单。然后调查机构填写调查问卷内容，调查问卷的选项包括单选、多选和问答等多种形式，如图 5 所示。调查问卷编辑完成后，调查机构即可发布调查。被调查者名单中的每一位用户都能收到一封系统邮件，提醒其参与该调查。

3) 参与调查部分。用户选择要参与的调查名称，系统会显示出调查问卷以及用户有无资格参与调查。如果用户有资格参与调查，则用户先填写调查问卷并保存问卷的结果，然后计算生成一次令牌和 NIZK 证明。最后用户将调查内容、一次令牌和 NIZK 证明一起发送给调查机构，如图 6 所示。

图 5　生成调查问卷

图 6　填写调查问卷

4) 资格审核部分。用户输入某次调查的调查名和被审核用户的身份标识 *id*（邮箱号），Web 服务器检查该被审核用户是否有资格参与该次调查，如图 7 所示。

图 7　资格审核

5) 公布结果部分。调查机构将调查结果公布后，用户输入调查名即可查看某次调查的调查结果，如图 8 所示。

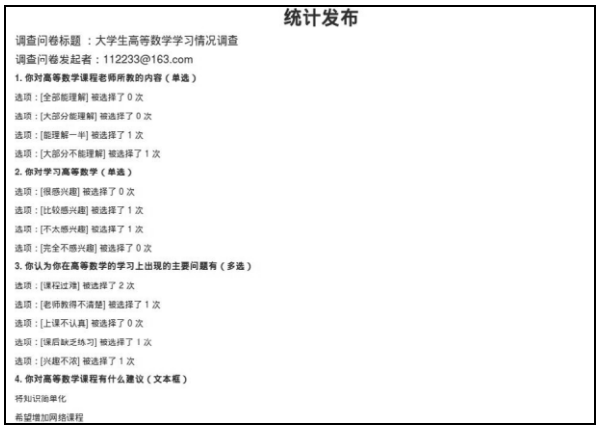

图 8 查看调查结果

5 结束语

本文深入研究了电子调查系统机制，介绍了非交互零知识证明的相关知识。在研究电子投票系统和电子调查系统的基础上，将其与 NIZK 协议、Boneh-Boyen 签名方案、Pedersen 承诺方案和伪随机函数等方法相结合，实现一个基于非交互式零知识证明的匿名调查系统。

系统有三方实体构成：注册机构、调查机构和用户。调查机构作为调查发起者与参与调查的用户地位平等, 即一个用户既可以作为调查机构, 也可以作为参与调查者。本文给出了系统的形式化定义以及安全性定义以及算法具体描述和安全性证明：系统具有抵抗恶意用户并发攻击和匿名性等安全特性。最后对系统进行仿真，结果表明该系统能够实现一次调查的全过程（发起调查、参与调查、提交调查结果、发布与统计结果等），同时能满足电子调查对真实性和匿名性的要求。

参考文献：

[1] 孙立娟. 现代电子调查技术研究[J]. 浙江统计, 2005 (6): 34-35.
SUN L J. Study of modem electronic survey technique[J]. Zhejiang Statistics, 2005(6): 34-35.

[2] [EB/OL].http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201502/P020150203548852631921.pdf.

[3] United Nations. United nations E-Government survey 2010[EB/OL]. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010.

[4] 晓晖. 搜狐、零点携手演绎“ 新新合作 ”——中国调查业步入网络时代[J]. 计算机与网络, 1998(8): 7.
XIAO H. Soho, Zero demonstrate “new cooperation” ——China investigation step into network times[J]. Computer & Network, 1998(8): 7

[5] NEFF C A. A verifiable secret shuffle and its application to E-Voting[C]//The 8th ACM Conference on Computer and Communications Security. 2001: 116-125.

[6] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]//Advances in Cryptology – CRYPTO 2004. 2004: 56-72.

[7] HOHENBERGER S, MYERS S, PASS R, et al. ANONIZE: a large-scale anonymous survey system[C]//Security and Privacy, 2014 IEEE Symposium on. 2014: 375-389.

[8] BLUM M, FELDMAN P, MICALI S. Non-interactive zero-knowledge and its applications[C]//The 20th Annual ACM Symposium on Theory of Computing. 1988: 1084-1118.

[9] DODIS Y, YAMPOLSKIY R. A verifiable random function with short Proofs and keys[J]. Lecture Notes in Computer Science, 2004: 416-431.

[10] BONEH D, BOYEN X. Efficient selective-ID secure identity-based encryption without random oracles[J]. Lecture Notes in Computer Science, 2004: 223-238.

[11] BRASSARD G, CHAUM D, CRE’PEAU C. Minimum disclosure proofs of knowledge[J]. Journal of Computer & System Sciences, 1988, 37(2): 156-189.

[12] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Advances in Cryptology. 1994: 129-140.

[13] GOLDREICH O, MICALI S. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems[J]. Journal of the ACM, 1991, 38(3): 691-29.

[14] BARAK B, PRABHAKARAN M, SAHAI A. Concurrent non-malleable zero knowledge[J]. Foundations of Computer Science Annual Symposium on, 2006(4):345-354.

作者简介：

柳璐（1992-），女，辽宁沈阳人，东北大学硕士生，主要研究方向为密码学与信息安全。

李宇溪（1990-），女，辽宁朝阳人，东北大学博士生，主要研究方向为密码学与信息安全。

周福才（1964-），男，吉林长春人，东北大学软件学院教授、博士生导师, 主要研究方向为网络与信息安全。