



- (51) **International Patent Classification:**
G06Q 30/02 (2012.01) *G06F 21/30* (2013.01)
H04L 9/32 (2006.01)
- (21) **International Application Number:**
PCT/US2015/031209
- (22) **International Filing Date:**
15 May 2015 (15.05.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/993,910 15 May 2014 (15.05.2014) US
- (71) **Applicant:** CORNELL UNIVERSITY [US/US]; Center for Technology Licensing ("CTL") at Cornell University, 395 Pine Tree Road, Ithaca, New York 14850 (US).
- (72) **Inventors:** PASS, Rafael; 849 Carroll St., Apt. 4, Brooklyn, New York 11215 (US). WATERS (HOHENBERGER), Susan; 3505 Clearview Drive, Austin, Texas 78703 (US). MYERS, Steven; 462 Ridgeview Lane, Columbus, Indiana 47201 (US). SHELAT, Abhi; 517 Lexington Ave, Charlottesville, Virginia 22902 (US).
- (74) **Agents:** VALAUSKAS, Charles C. et al.; Valauskas Corder LLC, 150 S. Wacker Drive, Suite 620, Chicago, Illinois 60606 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- of inventorship (Rule 4.17(iv))

Published:

- with international search report (Art. 21(3))

(54) **Title:** LARGE-SCALE ANONYMOUS SURVEY SYSTEM AND METHODS

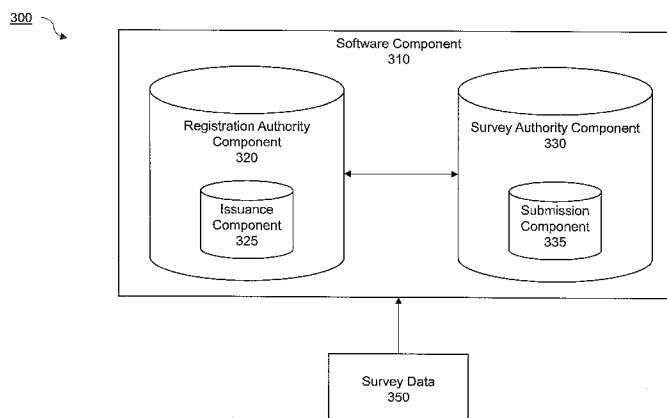


FIG. 3

(57) **Abstract:** A secure ad-hoc survey scheme enables a survey authority to independently (without any interaction) select an ad-hoc group of registered users based only on their identities (e.g., their email addresses), and create a survey where only selected users can anonymously submit exactly one response.



LARGE-SCALE ANONYMOUS SURVEY SYSTEM AND METHODS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application No. 61/993,910 filed May 15, 2014, incorporated by reference.

5

FIELD OF THE INVENTION

The invention relates to a system and methods that maintains anonymity between multiple network participants during data collection. More specifically, the invention is directed to a system and methods involving a cryptographic protocol that enables ad-hoc surveys with secure implementation.

10

BACKGROUND OF THE INVENTION

Companies, universities, healthcare providers, and government agencies often attempt to collect data from targeted groups of users by running surveys. Such surveys aim to satisfy two basic but conflicting properties: survey results need to be authentic – that is, only a specific set of users should be allowed to submit data, and each user should be allowed to submit only once – yet must be anonymous – that is, no link should exist between users and their survey data, so users feel safer about submitting honest feedback. The intrinsic conflict between anonymity and authenticity may result in users self-censoring or purposely biasing data they submit.

15

20

The most straightforward way to implement authenticity is for the survey implementer to request usernames during submission, but this obviously breaks user anonymity. The most straightforward way to implement anonymity is to avoid collecting usernames during submission, but this might allow attacks in which malicious users submit hundreds of responses to skew the results.

25

Another way to implement authenticity along with anonymity is to involve a third party. For example, a trusted third party collects usernames during submission, and then deletes the names when providing results to the survey initiator. However, placing such trust in a survey collector might be too dangerous. Even if the survey collector intends to keep the links between users and their surveys private, its system might be stolen or broken into, and the information leaked.

30

For instance, in 2009, a computer at a major university was stolen, containing sensitive personal information, such as name and social security number, for over 45,000 current and former university members. Additionally, even if users have full confidence in the trusted third party, and in particular, its
5 ability to keep its data secure, developing an anonymous survey system using such a trusted party still requires some care.

As another example, in the implementation of course reviews, side channel information indicating which users have already filled out the survey may leak information about the order in which students participated. Later, the order of
10 the students' comments in the aggregated responses may be correlated to break anonymity.

Furthermore, in many situations, jurisdictional boundaries or legal requirements make it unfeasible to rely on solutions with external trusted third parties: it may be illegal to store sensitive patient information on a third-party
15 system; similarly, many countries do not permit sensitive data to be stored on servers run by foreign corporations due to the potential for this data to be seized.

Finally, if a trusted third party removes all identifying information accompanying a submission to provide anonymity or accepts submissions from anonymized networks, then the trusted party loses the ability to verify whether a
20 participant submits multiple responses.

For these reasons, cryptographic solutions to the problem of anonymous surveys are sought that offer security guarantees where anonymity and authenticity hold without needing to trust a third party.

A simple example is a course evaluation for a university class. A typical
25 implementation of such a survey requires a trusted third party – such as the university, or some external party – to ensure that feedback is collected anonymously from the participants and that only authorized participants, *i.e.*, the students enrolled in a particular class, can submit feedback for that class. In such trusted-party implementations, students are required to authenticate themselves
30 with their university IDs and thus leave a link between their evaluation and their identity; they trust the survey collector to keep such links private.

Cryptographic voting schemes described in prior work may offer a partial solution to this problem. In such schemes, each survey consists of two steps: (1) users authenticate themselves to a server and anonymously check out a single-

use “token”; the token itself carries no link to the user’s identity, (2) a user can then use her token to participate in the specified survey. Such schemes provide good anonymity assuming that users actually separate steps (1) and (2) with a reasonably long time lag – otherwise there is a clear time link between the user and its data. But if users are required to separate the two steps by, say, a day, the ease-of-use of the survey is significantly hampered and become much less convenient than “non-anonymous” surveys or anonymous surveys employing a trusted third party. In addition, the extra steps required to authenticate for each survey may be onerous. Furthermore, voting schemes do not allow for the authenticated users to be selected ad-hoc for multiple elections. Consequently, such techniques have gained little traction.

In addition to voting schemes, other primitives previously considered include group signatures, ring signatures, and anonymous credentials. Generally, group signatures and ring signatures allow members of a set of users to sign messages in a way that makes it indistinguishable who in the set signed the message – in the case of group signatures the set is fixed, whereas in the case of ring signatures the set can be selected “ad-hoc”.

In a ring signature scheme, a user may sign multiple messages with impunity which corresponds to the ability to complete the survey multiple times skewing results.

An anonymous credential system allows users to obtain credentials from authorities and to anonymously demonstrate possession of these credentials. In essence such systems provide methods for providing, a “zero-knowledge proof of knowledge of a signature on a set of attributes.” Moreover, since anonymous credentials typically are not analyzed under concurrent executions, new techniques must be developed for security analysis.

Therefore, there is a need for a system and methods that anonymously collects data from multiple network participants while maintaining authenticity of the data. The present invention satisfies this need by providing a cryptographic protocol that enables ad-hoc surveys with secure implementation to an authenticated group of individuals of a network.

SUMMARY OF THE INVENTION

Cryptography is directed to secure communication techniques in the presence of third parties, known as adversaries. More generally, cryptography includes constructing and analyzing protocols that block adversaries to ensure data confidentiality, data integrity, authentication, and non-repudiation.

According to the invention, security properties of ad-hoc surveys are precisely defined such as anonymity in that there is no link between users and the surveys they submit, and authenticity in that only authorized users can complete the survey, and they can complete it only once.

More particularly, the invention is directed to an ad-hoc survey scheme protocol. The term “ad-hoc” represents that anyone can select a group of individuals and create a survey in which those and only those individuals can complete the survey at most once; additionally the survey initiator can initiate this survey knowing only the identities, such as email address, of the users in the ad-hoc group – no further interaction between the survey initiator and the users is required. Before a user can complete a survey, the user must register their identity with the system. The registration is performed only once and can be used for any number of subsequent surveys.

As such, the invention provides essentially the same ease-of-use as traditional (non-anonymous) electronic surveys, which may user participation and make the feedback submitted more valuable.

The invention can be implemented with easily handling large numbers of users with moderate resources. The computational costs on the users are quite low as well, with a typical desktop being able to compute the worst-case scenario in under a few seconds, using a single core of the machine. Thus, the invention is scalable to manage that vast majority of practical surveying needs at costs that are easily affordable.

In one embodiment of the invention, there are three parties in an ad-hoc survey system: a single registration authority (RA) that issues master user tokens, one or more survey authorities (SA) that can create surveys, and users that provide survey data. A user must first register with the RA and retrieve a secret “master user token” or simply referred to as “master token”. The terms “master user token” and “master token” are used interchangeably herein. This is a single token that can be used for all future surveys the user participates in.

Anyone can act as an SA by choosing a unique survey ID and publishing a list of identities that are permitted to participate in that survey. The list of identities that can participate in a particular survey can grow dynamically, and the SA can create a survey without any interaction with others. Finally, a user who is on the
 5 list of valid identities for a survey can non-interactively submit a response to the survey by simply routing one message to the SA using an anonymous tool such as the Tor Network, or anonymous proxy relay.

The invention ensures that, even if the RA and SA are arbitrarily corrupted and in collusion, they cannot learn anything about how particular users answered
 10 submission or discover correlations between groups of users.

Once all submissions are collected, the SA might publish a list of all survey responses, depending on external privacy requirements. If survey responses are made public, they can further be audited. Survey responders can inspect the output to check that their submissions were counted. Moreover, anyone can
 15 check that each submission was from a unique authorized user – for example, users can check for “ballot stuffing” and verify the list of authorized users.

According to a high-level overview of the invention, a user with identity id registers with the registration authority by sending a commitment to a random seed s_{id} of a pseudo-random function (PRF) F . If the user has not previously
 20 been registered, the registration authority signs the user’s name along with the commitment. The signature σ is returned to the user and is its “master token”.

To create a survey with identity user identities along with a survey id – referred to as v_{id} or simply “vid” –, the survey authority generates a signature key pair (vk_{SA}, sk_{SA}) and publishes the signature verification key vk_{SA} and a list of
 25 signed pairs $\{(vid, id)\}_{id \in I}$ where I is the set of users authorized for the survey.

To complete a survey for survey vid, a user id generates a single-use token $tok = Fs_{id}(vid)$ (by evaluating the PRF on the seed s_{id} with input vid) and presents a NIZK that it “knows a signature by the RA on its identity id and a commitment to a seed s_{id} ” (neither id or s_{id} is revealed), that it “knows a
 30 signature by the SA on the pair (vid, id) (again id is not revealed), and that the single-use token is computed as $Fs_{id}(vid)$. The user’s actual survey data as well as tok and vid are included into the “tag” of the NIZK to ensure “non-malleability” of submitted responses.

In contrast to dynamic group signatures, the ad-hoc survey scheme protocol according to the invention does not require that every group member or potential group member has their own personal public key, established and certified, e.g., by a PKI, independently of any group authority.

- 5 To enable an efficient implementation of the invention, direct game-based definitions of security analogous with other cryptographic game-based definitions, e.g., blind signatures, may be provided that directly analyze the security of the ad-hoc survey scheme protocol under concurrent executions.

Specifically, in a game-based definition, there are two parties: a challenger
10 who represents all honest parties and an adversary who represents all corrupted parties. Challengers and adversaries interact with one another according to the rules of the game; for instance, adversaries might be able to ask to register corrupted users and see the survey outputs generated by honest users of their choice. At some point, a challenger gives an adversary a challenge – for
15 instance, an honestly generated survey response. At the end of the game, the adversary provides a response to this challenge; the adversary might guess which honest user generated the challenge. If this challenge response is correct, the adversary wins the game.

The definition of security states that for any realistic, time-bounded
20 adversary, the probability of winning the game is very close to the probability of winning based on a random guess. Thus, a proof under this definition rules out all realistic attackers, provided the game accurately captures all actions that the adversary can make in the real world.

Malicious users should not be able to submit responses unless they are
25 authorized by the SA to participate in the survey. This property should hold when users arbitrarily create fake identities, fake surveys, and new surveys, which may be related in some form to the survey under attack. Moreover, this property ensures that potentially malicious users can complete such surveys only once. If they successfully submit multiple times, their submissions use the same token
30 and can be easily identified, then joined or discarded, depending on the survey policy. According to this embodiment, the security game starts when a challenger establishes the parameters for one RA and many SAs. An adversary can then generate new survey IDs for any SA, ask for any survey submission output by any honest user for chosen surveys, and register corrupted users. The

challenge involves a new, honestly generated survey ID, but the adversary chooses both the list of participants and the SA. The adversary responds with a set of survey submissions, which the challenger checks against four conditions, determining whether: (1) an adversary produced more submissions than allowed,
5 (2) all submissions are valid, (3) all submissions have different token numbers, and (4) all token numbers are new and therefore created by the adversary. Satisfying all the conditions results in the adversary winning.

One advantage of the invention is that it provides security not only for a single survey, but also if an attacker participates in many surveys, be they in the
10 past, concurrent, or in the future. Specifically, the ad-hoc survey scheme protocol proves secure even if the adversary participates in an arbitrary number of concurrent surveys.

Another advantage of the invention is that it admits practical and efficient solutions for very large surveys and supports millions of “write-in” (i.e., collection
15 of arbitrary strings of data) surveys in minutes. This is in stark contrast to mix-net or zero knowledge-based voting systems, which currently can handle only thousands of votes in several hours.

Another advantage of the invention is that it provides a provably-secure cryptographic multi-party protocol that scales to handle millions of users. The
20 invention efficiently enables secure implementation of million-person anonymous surveys using a single workstation.

The present invention is applicable to many online survey scenarios and possibly enables new ones. Examples of how the surveys according to the invention might be used are described below – university course evaluation,
25 online product review, and whistleblowing; however, these examples are merely exemplary as the invention might be used with a wide variety of contemplated applications including, for example, software distribution, financial transactions, and in cases where it is important to detect forgery or tampering.

University Course Evaluation

30 Most universities let students evaluate each course that they complete. These surveys typically include write-in sections in which open-ended answers are encouraged. In the past, many universities conducted these surveys on papers handed out and then collected during one of the final class sessions. However, many universities are moving to online surveys to increase participation

and ease data collection. A link to an online course evaluation survey is typically emailed to all students, who must trust the website collecting their responses to keep them anonymous. As discussed above, this is a dangerous assumption, even if the website makes a good faith effort to do so. To increase student
5 confidence in the system, the ad-hoc survey scheme protocol according to the invention may be used.

When students are asked to register through a registration process to set up their university account information (while proving their identity using a variety of known methods including traditional, nonelectronic methods, they generate an
10 unlinkable master user token that is tied to their school email address. This step can be done at a later stage if desired, or after a student has lost his or her credential and needs a new one, but it needs to be done only once.

When administrators want to set up a course survey, they generate a survey key based on a unique survey ID, such as "Survey for CS350 for Spring
15 2014 by Professor Brown at ABC University," and a list of course participants' email addresses.

After the survey is complete, the students' client – either a computer or smartphone – combines the survey key and the master user token to generate an unlinkable one-time token. This token satisfies two properties: it carries no link to
20 students' identity supporting anonymity, and for a given survey key, students can obtain at most one such token ensuring that each student completes the survey only once. Survey results are tabulated and possibly announced. If results are made public, students can verify that their responses were included.

Once registration is complete, setup and execution can be performed
25 repeatedly. Participants do not need to check out a new single-use token for each survey; rather, their client uses the master user token to create a unique single-use token for each survey without any interaction that could de-anonymize them.

Online Product Review

Many online retailers display a set of customer reviews next to each
30 product. These reviews are often influential to prospective customers. To avoid returns and customer dissatisfaction, these retailers have a vested interest in the reviewers' credibility. To bolster this credibility, many retailers indicate which reviewers they can verify purchased this product on their site. This process is currently non-anonymous; the retailer knows exactly which customer posted

which review. It is likely that a significant fraction of customers would be more likely to post a review if they could do so anonymously.

The ad-hoc survey scheme protocol can give customers this anonymity while still allowing the retailer to verify their purchases and ensure at most one review per purchase. When customers create an online account with a retailer and providing an email address and credit card to confirm identity, they are given the option to enroll in anonymous reviewing. If they choose to do so, they can then interact with the retailer to generate an unlinkable master user token that is tied to their online account identifier, such as their username or email address.

10 This step can also be done at a later stage, but needs to be done only once.

Whenever customers enrolled in anonymous reviewing complete a transaction, the retailer adds their online account identifier to an internal list of certified purchasers of a given product. This list, together with a product identifier, forms the survey ID. If customers want to post a review for a product or service they have purchased, their client combines the survey ID and their master user token to generate an unlinkable one-time token that they can use to complete the review. This token carries no link to user identity but can be used only once. Once the retailer receives the review with the token, which could be routed anonymously, the retailer can verify it and post it as a “verified purchase review.”

15

20 Again, once the registration step – that is, enrollment in anonymous reviewing and obtaining a master token – is complete, users can perform an unlimited number of purchases and reviews.

In this example, the retailer helps to create the master user tokens. Alternatively, customers could obtain master user tokens by interacting with their bank or credit card company. Retailers, restaurants, service providers, and so forth could then generate lists of authorized reviewers based on the bank account or credit card number used for the purchases. The review execution would remain the same. This model could work well for websites that review other parties’ services, because the sites could guarantee that they were posting reviews of actual customers, while customers remain anonymous.

25

30

Whistleblowing

Frequently, whistleblowers want to provide information to an organization’s ombudsman about alleged misconduct. Due to fears of reprisal, many whistleblowers prefer to remain anonymous. However, upon receiving a

complaint for investigation, an ombudsman should first ascertain that the source of the complaint is legitimate – i.e., from a verified employee – and not just sent by a random discontent.

5 In many cases, whistleblowers might be able to prove that they are in the organization by providing information only an employee would know, but doing so could break anonymity. An ad-hoc survey can give whistleblowing employees anonymity while letting an ombudsman verify that a complaint comes from within the organization.

10 When employees first join an organization, they register an account and issued a master user token tied to their system account. Concurrently, the ombudsman adds them to a whistleblowing survey that consists of all organization employees and provides employees – in conjunction with the master user token – a signature showing that their employee ID is certified for participation in the survey. The ombudsman publishes a signed list of all
15 participants to show that all employees can contribute.

Should employees uncover illegal or unethical activities, they can write a memo to the ombudsman via the whistleblowing survey. They certify the memo with their master user token and signed employee ID on the whistleblowing participant list. Upon receipt via anonymous channel, the ombudsman can verify
20 that the submission comes from a valid survey participant, and thus a legitimate employee.

The invention and its attributes and advantages may be further understood and appreciated with reference to the detailed description below of one contemplated embodiment, taken in conjunction with the accompanying
25 drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiments of the invention will be described in conjunction with the appended drawings provided to illustrate and not to limit the
30 invention, where like designations denote like elements, and in which:

FIG. 1 illustrates an exemplary network system that may be used to implement the methods according to the invention.

FIG. 2 illustrates an exemplary computer system that may be used to implement the methods according to the invention.

FIG. 3 illustrates a block diagram of the components of a cryptographic protocol that enables ad-hoc surveys with secure implementation according to the invention.

FIG. 4 illustrates a flow chart of the steps of the registration phase that enables ad-hoc surveys with secure implementation according to the invention.

FIG. 5 illustrates a flow chart of the steps of the survey creation phase that enables ad-hoc surveys with secure implementation according to the invention.

FIG. 6 illustrates a flow chart of the steps of the survey submission phase that enables ad-hoc surveys with secure implementation according to the invention.

FIG. 7 illustrates one embodiment of an ad-hoc survey scheme according to the invention.

FIG. 8 illustrates one embodiment of a cryptographic protocol of the registration phase according to the invention.

FIG. 9 illustrates one embodiment of a cryptographic protocol of the survey creation phase according to the invention.

FIG. 10 illustrates one embodiment of a cryptographic protocol of the survey submission phase according to the invention.

20 DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

FIG. 1 illustrates an exemplary communications network system 100 that may be used to implement the methods according to the invention. One or more network systems 100 may be used to implement the methods according to the invention, for example as computer code processed by a processor such as one similar to that described in reference to FIG. 2.

Specifically, the communications network system 100 includes at least one client computer 110A (also referred to as "client"). The client computer 110A may be any device through the use of which a distributed computing environment may be accessed to perform the methods disclosed herein, for example, a traditional computer, portable computer, handheld device, mobile phone, personal digital assistant, smart hand-held computing device, cellular telephone, or a laptop or netbook computer, hand held console or MP3 player, tablet, or similar hand held computer device, such as an iPad®, iPad Touch® or iPhone®. More specifically,

the client computer 110A may include one or more components as described in reference to the computer system of FIG. 2.

The one or more client computers 110A establish communication with the Internet 120 (including untrusted web browsers) to one or more servers 130 (also referred to as "server"). A server computer 130 permits access to a collection of computing resources and components that can be invoked to instantiate a machine, process, or other resource for a limited or defined duration. For example, one group of resource servers can host and serve an operating system or components thereof to deliver and instantiate a virtual machine. Another group of resource servers can accept requests to host computing cycles or processor time, to supply a defined level of processing power for a machine or virtual machine.

One embodiment of the client computer 110A or server computer 130 may be shown by the exemplary computer system 200 of FIG. 2. One or more computer systems 200 may be used to implement the methods according to the invention, for example as computer code.

Computer system 200 includes an input/output display interface 202 connected to communication infrastructure 204 – such as a bus – that forwards data including graphics, text, and information, from the communication infrastructure 204 to other components of the computer system 200. The input/output display interface 202 may be, for example, a display device, a keyboard, touch screen, joystick, trackball, mouse, monitor, speaker, printer, Google Glass® unit, web camera, any other computer peripheral device, or any combination thereof, capable of entering and/or viewing data.

Computer system 200 includes one or more processors 206, which may be a special purpose or a general-purpose digital signal processor configured to process certain information. Computer system 200 also includes non-transitory computer-readable storage medium such as a main memory 208, for example random access memory ("RAM"), read-only memory ("ROM"), mass storage device, or any combination thereof. Computer system 200 may also include a secondary memory 210 such as a hard disk unit 212, a removable storage unit 214, or any combination thereof. Computer system 200 may also include a communication interface 216, for example, a modem, a network interface (such as an Ethernet card or Ethernet cable), a communication port, a PCMCIA slot

and card, wired or wireless systems (such as Wi-Fi, Bluetooth, Infrared), local area networks, wide area networks, intranets, etc.

It is contemplated that the main memory 208, secondary memory 210, communication interface 216, or a combination thereof, function as a non-transitory computer-readable storage medium to store and/or access computer software including computer instructions. Certain embodiments of a computer readable storage medium do not include any transitory signals or waves. For example, computer programs or other instructions may be loaded into the computer system 200 such as through a removable storage device, for example, a floppy disk, ZIP disks, magnetic tape, portable flash drive, optical disk such as a CD or DVD or Blu-ray, Micro-Electro-Mechanical Systems ("MEMS"), nanotechnological apparatus. Specifically, computer software including computer instructions may be transferred from the removable storage unit 214 or hard disc unit 212 to the secondary memory 210 or through the communication infrastructure 204 to the main memory 208 of the computer system 200.

Communication interface 216 allows software, instructions and data to be transferred between the computer system 200 and external devices or external networks. Software, instructions, and/or data transferred by the communication interface 216 are typically in the form of signals that may be electronic, electromagnetic, optical or other signals capable of being sent and received by the communication interface 216. Signals may be sent and received using wire or cable, fiber optics, a phone line, a cellular phone link, a Radio Frequency ("RF") link, wireless link, or other communication channels.

Computer programs, when executed, enable the computer system 200, particularly the processor 206, to implement the methods of the invention according to computer software including instructions.

The computer system 200 described herein may perform any one of, or any combination of, the steps of any of the methods presented herein. It is also contemplated that the methods according to the invention may be performed automatically, or may be invoked by some form of manual intervention.

The computer system 200 of FIG. 2 is provided only for purposes of illustration, such that the invention is not limited to this specific embodiment. It is appreciated that a person skilled in the relevant art knows how to program and

implement the invention using any computer system such as a cloud computer system.

The invention is also directed to computer products, otherwise referred to as computer program products. Computer products store software on any computer useable medium, known now or in the future. Such software, when
5 executed, may implement the methods according to certain embodiments of the invention.

The exemplary network system 100 of FIG. 1 and the exemplary computer system 200 of FIG. 2 are provided only for purposes of illustration and do not limit
10 the invention to these specific embodiments. It is appreciated that a person skilled in the relevant art knows how to program and implement the invention using any computer system or network architecture.

FIG. 3 illustrates a block diagram of the components of a cryptographic protocol 300 that enables ad-hoc surveys with secure implementation according
15 to the invention. More specifically, survey responses may be obtained from one or more users through a communications network such that the users are authenticated and the responses remain anonymous.

The ad-hoc survey scheme protocol 300 includes a software component 310 comprising a single registration authority component 320 and one or more
20 survey authority components 330, which are operable for use by users securely and without access by another or others.

It is assumed that the registration authority component 320 has the ability to set up a secure session (private and authenticated) with the user associated with a particular user identity. Each user additionally has the ability to setup an
25 anonymous connection to the survey authority component 330 when returning their survey.

According to a high-level overview of the invention, a registration issuance component 325 issues a master token to each registered user. More specifically, a user with identity id registers with the registration authority component 320 by
30 sending a commitment to a random seed s_{id} of a pseudo-random function (PRF) F and providing a non-interactive zero-knowledge (NIZK) that the commitment is well-formed. If the user has not previously been registered, the registration authority component 320 signs the user's name along with the commitment. The

signature returned to the user is its “master token”. The security property required here is weaker than that of a blind signature. To create a survey, survey authority component 330 publishes a list of signed user identities along with a survey id, v_{id} . To complete a survey for survey id v_{id} , a user id generates a single-use token $FS_{id}(v_{id})$ (by evaluating the PRF on the seed s_{id} with input v_{id}) and presents a NIZK that it “knows a signature by the RA on its identity id and a commitment to a seed s_{id} ” and that it “knows a signature by the SA on its id ” and that the single-use token is computed as $FS_{id}(v_{id})$. The user’s actual survey data will be part of and thereby authenticated by this NIZK. The NIZK in the survey completion step ensures that only authorized users can complete the survey, and that they can compute at most one single-use token, and thus complete it at most once. If, however, a user wants to replace her survey response before the deadline and this is allowed by the system, then she can create a new NIZK with new data for the same $FS_{id}(v_{id})$ value. The old survey result with this value is then deleted.

15 Anonymity, on the other hand, follows from the fact that neither the registration authority component 320 nor the survey authority component 330 ever get to see the seed s_{id} (they only see commitments to it), the zero-knowledge property of the NIZKs, and the pseudo-randomness property of the PRF.

According to a more specific embodiment of the invention, an ad-hoc survey scheme protocol is a tuple of algorithms: GenRA , GenSA , $\text{RegUser}^{\text{RA}}$, $\text{RegUser}^{\text{U}}$, GenSurvey , Authorized , SubmitSurvey , Check . The registration authority component 320 generates a public key-pair $\text{pk}_{\text{RA}}, \text{sk}_{\text{RA}} \leftarrow \text{GenRA}(1^n)$; pk_{RA} is made public and sk_{RA} is secretly stored by the registration authority component 320. Each survey authority component 330 generates a public key-pair $\text{pk}_{\text{SA}}, \text{sk}_{\text{SA}} \leftarrow \text{GenSA}(1^n)$; pk_{SA} is made public and sk_{SA} is secretly stored by the survey authority component 330. It should be noted that security properties hold even if new survey authority components are added on-the-fly. When the use of a Common Reference String (CRS) is required; a CRS is generated and made publicly available. For simplicity of notation, CRS has been omitted in the discussion below and it is simply assumed that all these procedures get the CRS as an input.

The registration authority component 320 permits users to register with the system such as by providing profile information such as name, contact

information, etc. The user sets up a secure session with the registration authority component 320. The registration authority component 320 checks that user identity id previously has not been registered. If it has, the registration authority component 320 closes the session. Otherwise, the registration authority component 320 and the user invoke the interactive protocol ($\text{RegUser}^{\text{RA}}$, $\text{RegUser}^{\text{U}}$) on the common input $1^n, id$. If the protocol ends successfully, the registration authority component 320 stores that user identity id has been registered, and the user secretly stores the output as cred_{id} .

The survey authority component 330 creates surveys. According to one embodiment of the invention, a unique survey identification (SurveyID) is obtained that is associated with a list of identities, i.e., email addresses, that can participate in the survey.

More particularly, when a survey authority component 330 sets up a survey with identifier SurveyID, it generates a survey public key based on the identities of the participants (and its own secret key). More precisely, the survey authority component 330 on input a survey identifier SurveyID and a list L of user identities (they may be previously registered or not) computes and makes public $\text{pk}_{\text{SurveyID}} \leftarrow \text{GenSurvey}(1^n, \text{SurveyID}, L, \text{sk}_{\text{SA}})$.

Users submit survey data 350 non-interactively (i.e, there is no back-and-forth communication between the client computer and server computer). The survey data comprises or consists of only one response to the survey. The response can be, for example, a message consisting of one or more answers to survey questions. Only the user identities of which appear on the participation list can submit a response to the survey such as using an anonymous tool like Tor Network. Users may submit their response using any device such as cellular telephone, or a laptop or netbook computer, hand held console or MP3 player, tablet, or similar hand held computer device, such as an iPad®, iPad Touch® or iPhone®.

Given a registered survey with identifier SurveyID and its associated public-key $\text{pk}_{\text{SurveyID}}$, each “authorized” user id_i can combine its master credential cred_{id} with the survey identifier SurveyID and public-key $\text{pk}_{\text{SurveyID}}$ to generate an unlikable “one-time token” that it can then use to make a submission in the survey. The “one-time token” satisfies two properties: (1) it carries no link to the

user's identity (anonymity) and (2) for a given "survey key", the user can obtain at most one such token (and thus can only submit one response).

More precisely, user id with master credential $cred_{id}$ submits the message m as the completed survey by privately executing the algorithm $Sub = (tok, m, tokauth) \leftarrow \text{SubmitSurvey}(1^n, \text{SurveyID}, pk_{\text{SurveyID}}, m, cred_{id})$ and then submitting Sub to the survey authority component 330 through an anonymous channel; tok is the "one-time token", and $tokauth$ is an authenticator required to bind the message m to the one-time token, and to ensure uniqueness of the one-time token. The survey authority component 330 checks whether the submission is correctly computed by executing $\text{Check}(pk_{SA}, pk_{RA}, \text{SurveyID}, pk_{\text{SurveyID}}, Sub)$; if it outputs accept it stores the submission. If a submission with the same tok has been previously stored (i.e., if a Sub of the form $(tok, m', tokauth')$ has already been stored, the old record is removed, i.e., the new Sub is not stored.

Once all the submissions have been collected, the SA may (depending on external privacy requirements) publish a list of all stored submissions $Sub = (tok, m, tokauth)$.

The invention also includes audit procedures. First, users can check that their submission was "counted" by simply inspecting that their submission is output. Second, a user may use $\text{Check}(pk_{SA}, pk_{RA}, \text{SurveyID}, pk_{\text{SurveyID}}, Sub)$ to check whether Sub is a valid submission (i.e., user can check that there is no "ballot/survey-stuffing"). Finally, to ensure that a survey is not targeted to a particular user (for de-anonymization purposes), the user may use function $\text{Authorized}(pk_{SA}, \text{SurveyID}, pk_{\text{SurveyID}}, id')$ to check whether user id' is also authorized for survey SurveyID with public key pk_{SurveyID} .

A crucial aspect of an ad-hoc survey is the privacy property: even if the RA and SA are arbitrarily corrupted (and in collusion) they cannot learn anything about how particular users answered submissions (or even learn correlations between groups of users). The key security property of our ad-hoc survey is that only authorized users can complete a survey, and furthermore they can complete it at most once. According to one embodiment for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous, the method comprises a registration phase, a

survey creation phase, and a survey submission phase. FIG. 4, FIG. 5, and FIG. 6 illustrate block diagrams of the steps of a cryptographic protocol that enables ad-hoc surveys with secure implementation according to the invention. The following considers the invention and its anonymity/authenticity properties.

5 As shown in FIG. 4, a user registers using a client computer at step 402. The registration phase is conducted between a client and a server and occurs only once for each client. For example a user sets-up his or her account information such as a profile that requires proof of identity (including using traditional, non-electronic, methods). The registration is accepted if it is a new
10 registration and has not been previously set-up.

At step 404, the server prepares a master server secret and the client prepares a master token secret. At step 405, the client prepares a message derived from the master token secret and an identification element of the user, such as an email address. The client sends the message and the identification
15 element, which are received by the server. At step 406, the server combines the message and the master server secret to obtain a pre-master token. The server sends the pre-master token to the client and the client derives a client master token from the pre-master token at step 407. The client master token is associated to an identity such as the user's school email identity or email
20 address. Again, the registration phase can also be done at a later stage if the user desires (or if the user loses his or her credential), but it only needs to be done once.

The survey creation phase includes receiving by the server a survey created through a series of inputs, the survey including a survey key that
25 comprises one or more selected identification elements for participation in the survey. More specifically as shown in FIG. 5, a user creates a survey at step 412. Identification elements for participation in a survey are selected at step 414. At step 416, the identification elements are used to generate a survey key. For example, when an administrator wishes to set-up a survey, the administrator
30 generates a survey key based only on the actual identities – email addresses – of the participants.

The survey submission phase is conducted between the client and the server. As shown in FIG. 6, a user attempts through a client computer to access the survey and the survey key by one or more users at step 422. If a match exists

the client prepares a plurality of responses to the survey at step 424. At step 426, the client combines the survey key and the client master token. At step 428, a client survey token is generated. More specifically, upon filling out a survey with its associated survey key, the user's client (either computer or smart phone) combines the survey key and the master token to generate an unlikable one-time token that can be used to complete the survey, i.e., survey token. The one-time survey token satisfies two properties: (1) it carries no link to the user's identity (anonymity), and (2) for a given survey key, the user can obtain at most one such token ensuring that a user can only complete the survey once. The response may be submitted using an anonymous network such as the Tor Network or anonymous proxy relay.

At step 430, the client submits to the server computer a server response, which is exactly one survey response. The survey response includes the plurality of responses to the survey and the client survey token.

As shown in step 432, the survey token is compared to a list of previously submitted survey tokens to determine whether or not the survey token has been previously used. If the survey token has been previously used the response is declined at step 436. If the survey token does not appear on the list of previously submitted survey tokens, the response is accepted at step 434.

In an alternate embodiment, the invention supports the optional ability for the user to change his or her response before the voting deadline in a manner that replaces the previous submission, but in no other way leaks any information about the user's identity.

Again, once a user registration is completed, surveys can be created and accessed any number of times. The participants do not need to obtain new single-use tokens for each survey; rather their client uses the master user token to create a unique single-use token for this survey without any interaction, which may de-anonymize the user.

In order to construct a system according to the invention, secure ad-hoc surveys are implemented from generic primitives, such as commitment schemes, signature schemes, pseudorandom functions (PRFs), and generic non-interactive zero-knowledge (NIZK) arguments for all assertions that can be efficiently verified. A commitment scheme lets a sender commit to a message without revealing that message to a receiver. A signature scheme allows public

authentication of a message. A PRF is a seeded deterministic function that maps any input to a random looking output, assuming one has no knowledge of the seed. Finally, an NIZK argument provides a proof of an assertion – for example, “I know a signature by the RA on message m ” – without revealing anything
5 beyond the truth of this statement, such as signature bits. The ad-hoc survey scheme’s security is proved based on the assumption that all generic primitives employed are secure. The ad-hoc survey scheme remains secure even when an adversary initiates many concurrently executing sessions in the system.

The generic scheme is instantiated with a specific commitment scheme,
10 signature scheme, PRF, and NIZK arguments to obtain efficient, secure ad-hoc survey scheme. The generic protocol does not rely on the underlying primitives in a black-box way; rather, the NIZK argument is used to prove complex statements that require code of the actual commitments, signatures, and PRFs used.

FIG. 7 illustrates one embodiment of an ad-hoc survey scheme according
15 to the invention.

FIG. 8 illustrates one embodiment of a cryptographic protocol of the registration phase according to the invention.

FIG. 9 illustrates one embodiment of a cryptographic protocol of the survey creation phase according to the invention.

20 FIG. 10 illustrates one embodiment of a cryptographic protocol of the survey submission phase according to the invention.

An unoptimized implementation demonstrates efficiency for nearly all practical surveys. In particular, a particular implementation of the invention utilizes only one core of the CPU, but user registration and survey verification one
25 can easily be load-balanced over multiple cores and machines by having all cores run the same processes. Similarly, when generating new surveys, the participant list can be split among several different cores at the SA, and each would sign the names of the individuals on its portion of the list.

It is contemplated that one or two workstations or servers are sufficient to
30 manage millions of surveys using the more efficient BN curves, and a small number of high-performance machines could easily handle surveys of larger or similar sizes using the BLS curves.

While the disclosure is susceptible to various modifications and alternative forms, specific exemplary embodiments of the invention have been shown by

way of example in the drawings and have been described in detail. It should be understood, however, that there is no intent to limit the disclosure to the particular embodiments disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the scope of the
5 disclosure as defined by the appended claims.

CLAIMS

1. A system for obtaining survey responses from one or more users through a communications network such that the users are authenticated and the responses remain anonymous, the system comprising:
- 5 a registration issuance component that permits the one or more users to obtain a registration with the system;
- a registration authority that issues a master token to each of the one or more users who obtain the registration;
- a survey authority established by obtaining a unique survey ID and
- 10 permitted to publish a list of identities that can participate in the survey as the one or more users; and
- a submission component by which the one or more users the identities of which appear on the participation list can submit a response to the survey using an anonymous tool.
- 15
2. The system of claim 1, wherein the submission component is configurable to permit a complete response to a survey in a single message.
3. The system of claim 1, wherein said registration issuance
- 20 component, said registration authority, said survey authority, and said submission component are operable for use by the one or more users securely and without access by another or others.
4. The system of claim 1, wherein the master token is receivable and
- 25 storable on a mobile device and the submission component is configurable to permit the one or more users to submit the response from the mobile device.
5. A method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such
- 30 that the users are authenticated and the responses remain anonymous, the method comprising:
- conducting a registration phase between a client and a server, wherein the registration phase occurs only once for each client, the registration phase further comprising the steps of:

- preparing by the server a master server secret;
- preparing by the client a master token secret;
- preparing by the client a message derived from the master token secret and an identification element of the user;
- 5 sending by the client to the server the message and the identification element;
- receiving by the server the message along with the identification element of the user;
- combining by the server the message and the master server secret
- 10 to obtain a pre-master token;
- sending by the server the pre-master token to the client;
- receiving by the client the pre-master token;
- deriving by the client a client master token from the pre-master token;
- 15 conducting a survey creation phase between the client and the server, the survey creation phase further comprising the steps of:
 - receiving by the server a survey created through a series of inputs, the survey including a survey key that comprises one or more selected identification elements for participation in the survey;
- 20 conducting a survey submission phase between the client and the server, survey submission phase further comprising the steps of:
 - attempting through the client access to the survey and the survey key by one or more users;
 - preparing by the client a plurality of responses to the survey;
 - 25 combining by the client the survey key and the client master token to generate a client survey token;
 - submitting to the server a survey response, the survey response including the plurality of responses to the survey and the client survey token;
 - comparing by the server the survey token to a list of previously
 - 30 submitted survey tokens; and
 - accepting by the server the survey response.

6. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 5, wherein the step of accepting by the server the survey response
5 occurs when the survey token does not appear on the list of previously submitted survey tokens.

7. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such
10 that the users are authenticated and the responses remain anonymous according to claim 5, wherein the step of accepting by the server the survey response further comprises the step of replacing any previously recorded response that shares the same survey token.

15 8. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 5, wherein the identification element is an email address.

20 9. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 5, wherein the submitting step is performed through an anonymous
network.

25 10. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 9, wherein the anonymous network is Tor Network.

30 11. The method for obtaining survey responses from one or more users through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according

to claim 5, wherein the preparing step further comprises the step of using an untrusted web browser.

12. The method for obtaining survey responses from one or more users
5 through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 5, wherein the client computer is a portable handheld device.

13. The method for obtaining survey responses from one or more users
10 through use of a computer-based system and a communications network such that the users are authenticated and the responses remain anonymous according to claim 5, wherein the submitting step is performed simultaneously by a plurality of client computers.

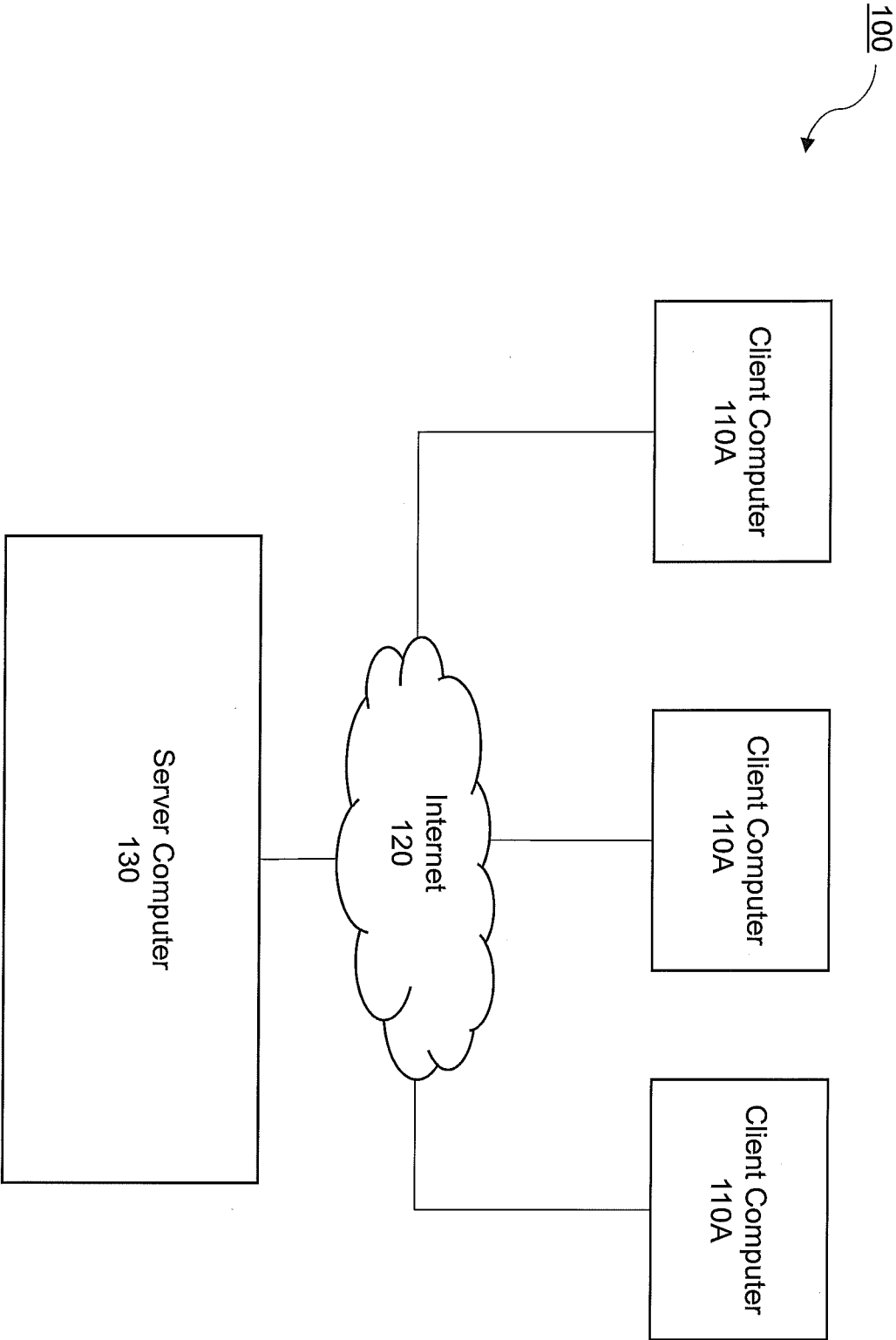


FIG. 1

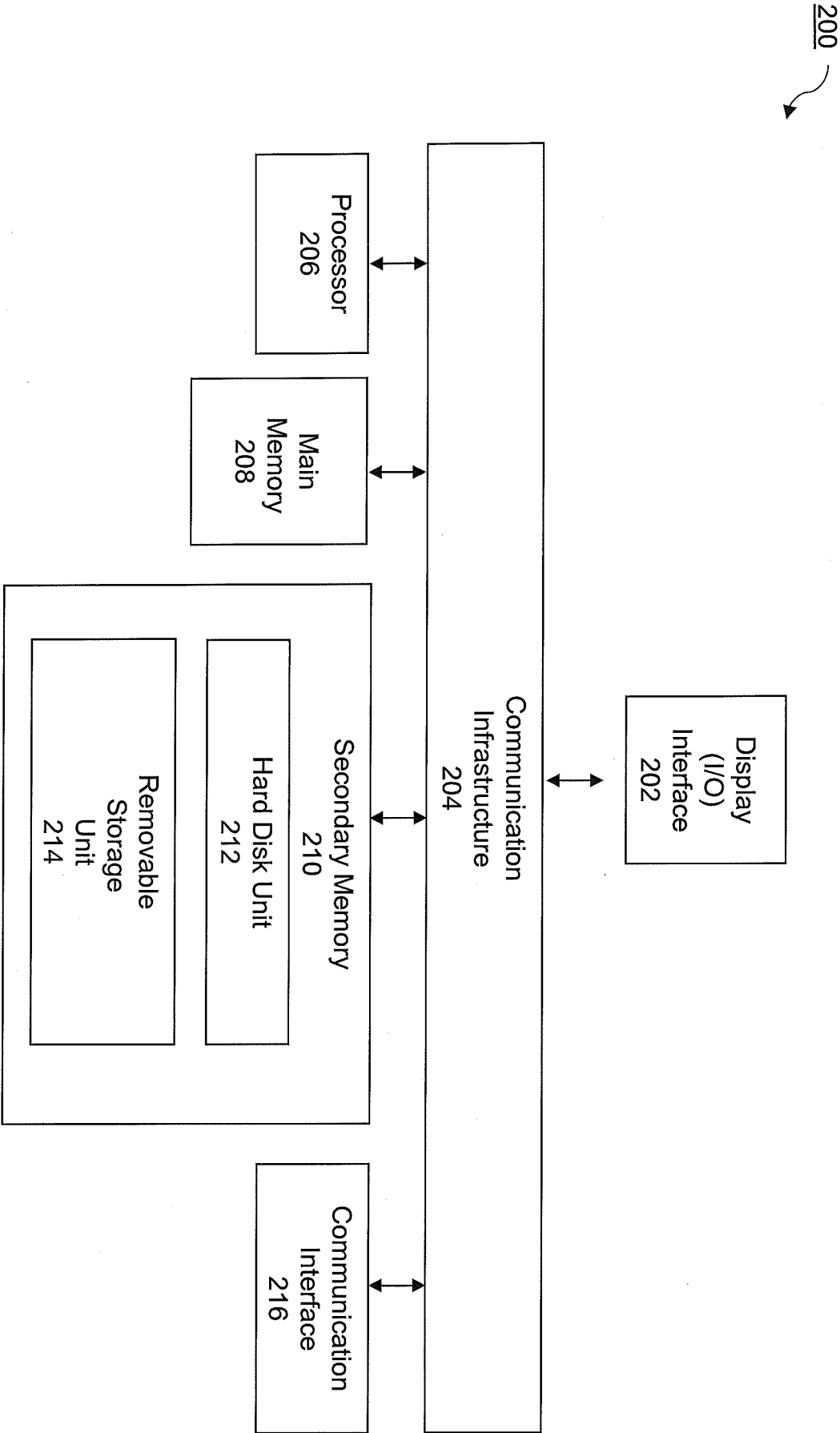


FIG. 2

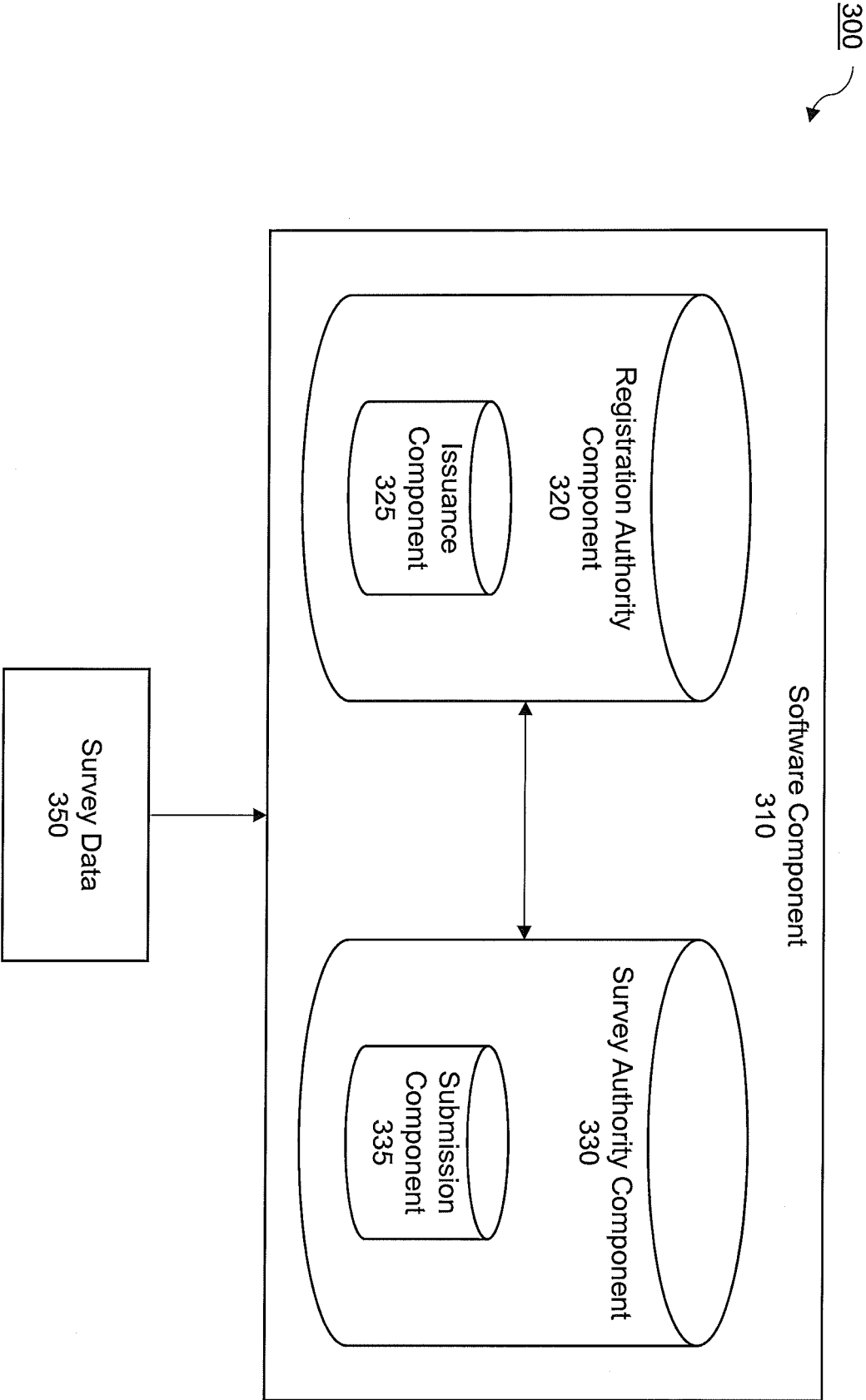


FIG. 3

4/10

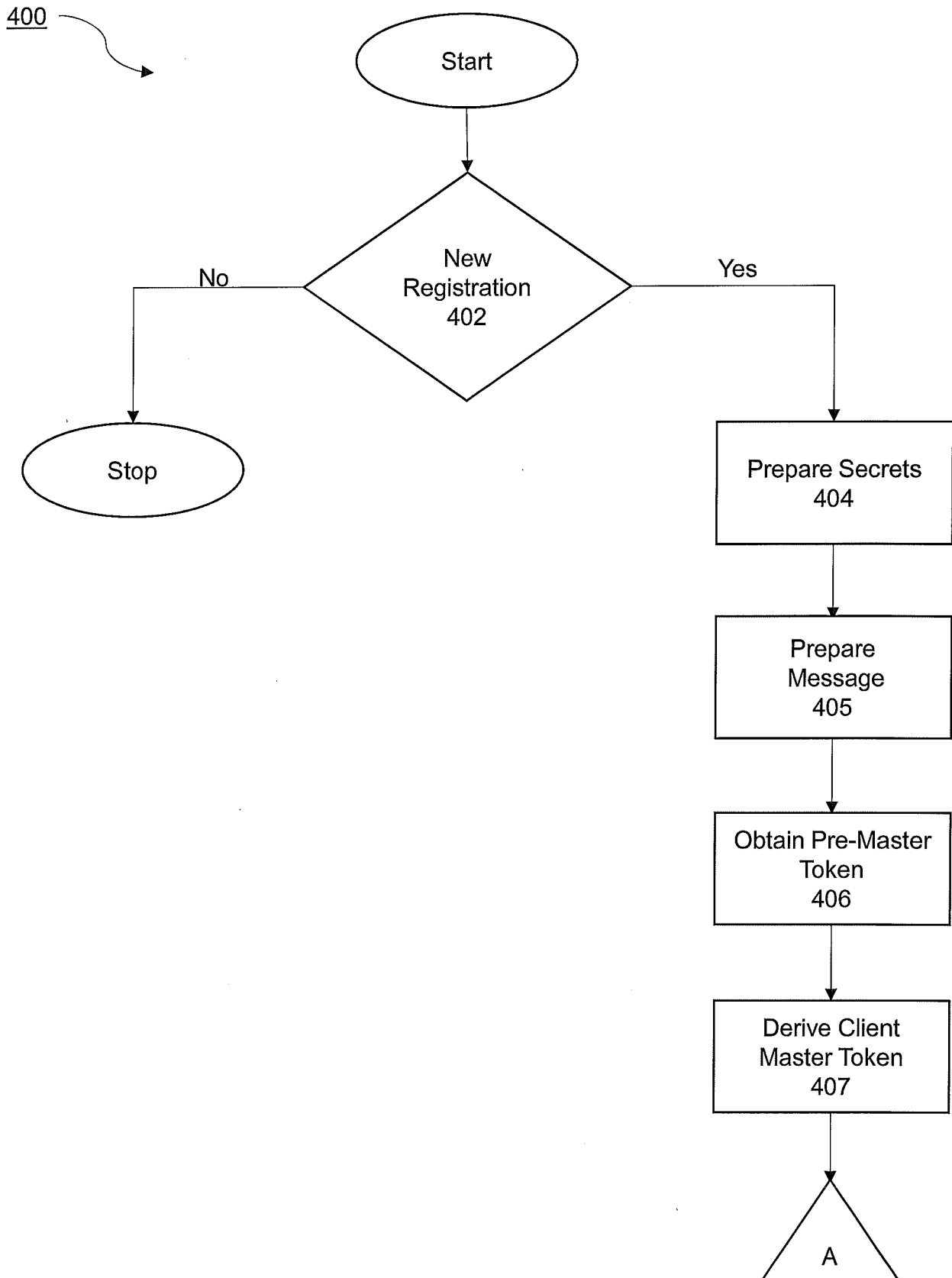


FIG. 4

5/10

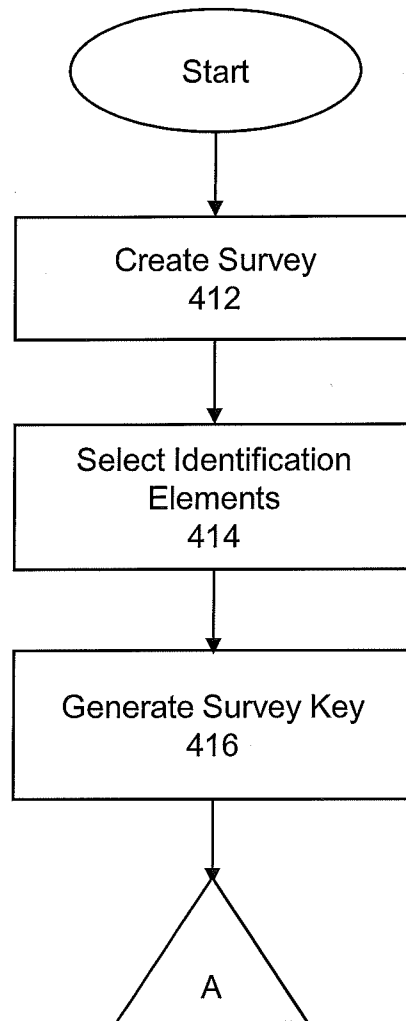
500

FIG. 5

6/10

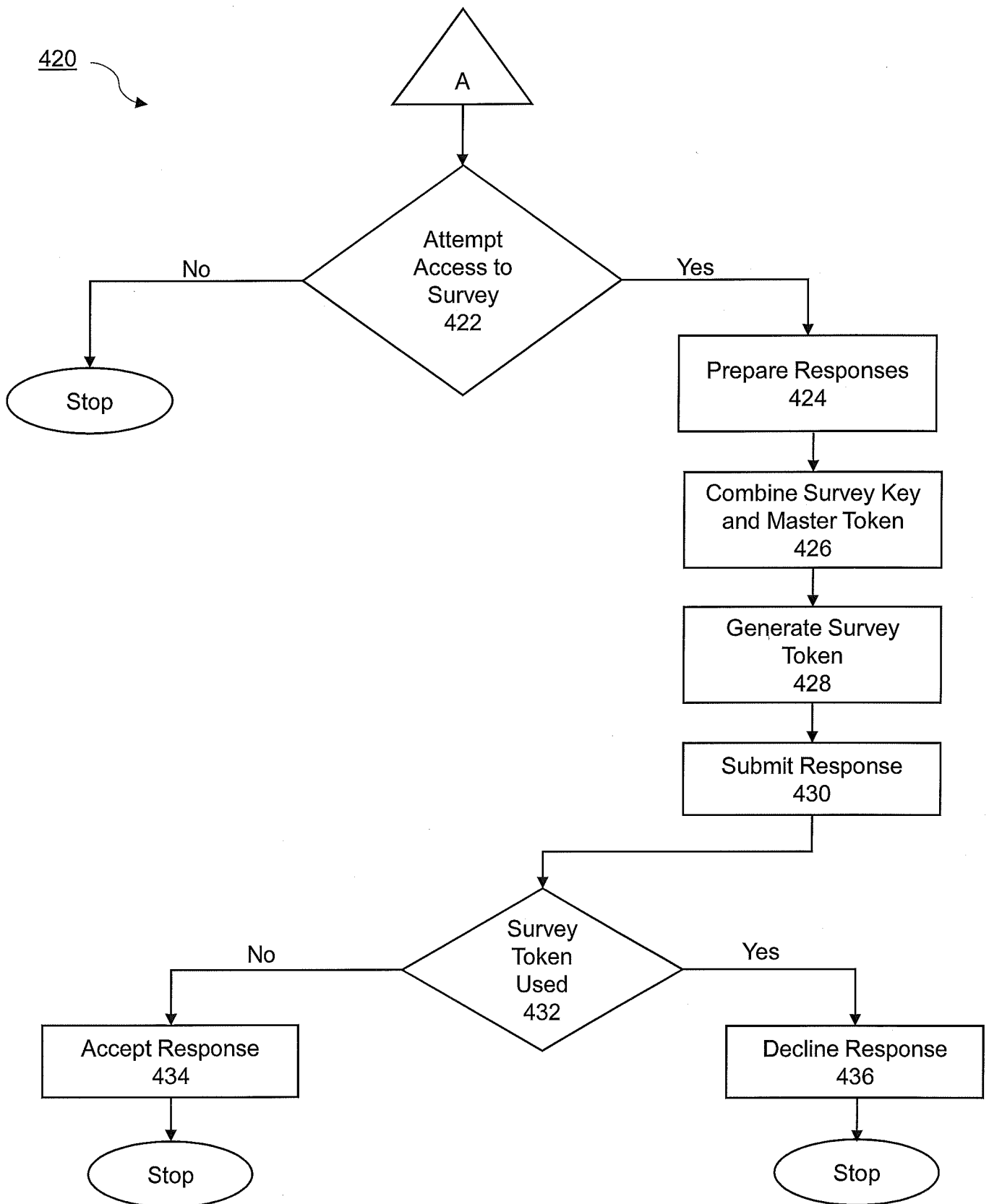


FIG. 6

7/10

Ad-hoc Survey Construction

Let,

- $(\text{Gen}, \text{Sign}, \text{Ver})$ be a signature scheme.
- $(\text{Gen}', \text{Ver}', \text{Sign}', \text{Blind}', \text{Unblind}')$ be a partially blind signature scheme.
- $\{f_s\}_{s \in \{0,1\}^*}$ be a family of PRFs.
- Let L be the NP language defined as follows: $(\text{tok}, \text{vid}, \text{vk}_{\text{RA}}, \text{vk}_{\text{SA}}) \in L$ iff there exist strings $s, id, \sigma_s, \sigma_{\text{vid}, id}$ such that $\text{Ver}'(\text{vk}_{\text{RA}}, (id, s), \sigma_s) = 1$ and $\text{Ver}(\text{vk}_{\text{SA}}, (\text{vid}, id), \sigma_{\text{vid}, id}) = 1$ and $\text{tok} = f_s(\text{vid})$
- Let $(P, V, \mathcal{O})$ be an oSE NIZK protocols for L .
- $\text{GenRA}(1^n) = \text{Gen}'(1^n)$;
- $(\text{RegUser}^{\text{RA}}(\text{sk}_{\text{RA}}), \text{RegUser}^{\text{U}})(1^n, id_i)$ proceeds as follows:
 - A user with identity id uniformly generates and stores $s \leftarrow \{0,1\}^n, r \leftarrow \{0,1\}^{\text{poly}(n)}$ and computes $y = (id, \text{Blind}_r(\text{vk}_{\text{RA}}, s))$ and sends it to the RA.
 - The RA returns $x = \text{Sign}'(\text{sk}_{\text{RA}}, y)$.
 - The user computes $\sigma_s = \text{Unblind}'_r(\text{vk}_{\text{RA}}, x)$, checks if $\text{Ver}'(\text{vk}_{\text{RA}}, (id, s), \sigma_s) = 1$ and if so outputs $\text{cred} = (s, \sigma_s)$ and otherwise $\perp$.
- $\text{GenSurvey}(1^n, \text{vid}, L)$ proceeds as follows.
 - $\text{vk}_{\text{SA}}, \text{sk}_{\text{SA}} \leftarrow \text{Gen}(1^n)$ For each $id \in L$, compute $\sigma_{id}^{\text{vid}} = \text{Sign}(\text{sk}_{\text{SA}}, (\text{vid}, id))$ and output vk_{SA} and the list of tuples $(id, \sigma_{id}^{\text{vid}})_{id \in L}$.
 - $\text{Authorized}(\text{vid}, \text{vk}_{\text{vid}}, id)$ parses vk_{vid} as $(\text{vk}_{\text{SA}}, \tilde{L})$ and outputs YES iff $\tilde{L}$ contains a record of the form $(id, \sigma_{id}^{\text{vid}})$ such that $\text{Ver}(\text{vk}_{\text{SA}}, (\text{vid}, id), \sigma_{id}^{\text{vid}}) = 1$
 - $\text{SubmitSurvey}(1^n, \text{vid}, \text{vk}_{\text{vid}}, m, id, \text{cred})$ proceeds as:
 - * Parse $\text{cred} = (s, \sigma_s)$.
 - * Parses $\text{vk}_{\text{vid}} = (\text{vk}_{\text{SA}}, \tilde{L})$
 - * Compute token-number $\text{tok} = f_s(\text{vid})$.
 - * Recover a tuple of the form $(id, \sigma_{id}^{\text{vid}})$ from $\tilde{L}$. If no such tuple exists, or if $\text{Ver}(\text{vk}_{\text{SA}}, (\text{vid}, id), \sigma_{id}^{\text{vid}}) \neq 1$ abort.
 - * Compute a on SE NIZK π using P that $(\text{tok}, \text{vid}, \text{vk}_{\text{RA}}, \text{vk}_{\text{SA}}) \in L$ with tag $\text{tok}||\text{vid}||m$ using $s, \text{vid}, \sigma_s, \sigma_{id}^{\text{vid}}$ as witness.
 - * Send the tuple $\text{Sub} = (\text{tok}, m, \pi)$ to the SA.
 - $\text{Check}(\text{vk}_{\text{RA}}, \text{vid}, \text{tok}, m, \pi)$ outputs accept if V accepts π as a proof of the statement $(\text{tok}, \text{vid}, \text{vk}_{\text{RA}}) \in L$ with tag $\text{tok}||\text{vid}||m$.

FIG. 7

8/10

Concrete scheme

GenRA and GenSA The RA picks random group elements $u, v, h \in G_1$ and a secret element $x \in \mathbb{Z}_q$. The RA's public key $vk_{RA} = (u, v, h, e(g, g_2)^x)$ and $sk_{RA} = x$. (RA will be signing m_1 as the id with u and m_2 as the user's secret seed with v .)

The SA picks random group elements $u_v, v_v, h_v \in G_1$ and a secret element $y \in \mathbb{Z}_q$. The SA's public key $SA_{vk} = (u_v, v_v, h_v, e(g, g_2)^y)$ and $SA_{sk} = y$. (m_1 will be the vid and m_2 will be the user id of a participant authorized to submit in the survey.)

The RegUser protocol A user registers by invoking the following protocol with the RA:

Common: $RA_{vk} = (u, v, h, e(g, g_2)^x)$

RA Secret Key: x

User identity: id

User and RA establish a mutually authenticated secure communication channel.

$U \rightarrow RA$ The user chooses a random PRF seed $s_{id} \in \mathbb{Z}_q$ and a random $d \in \mathbb{Z}_q$, computes $\alpha = v^{s_{id}} g^d$, and sends (id, α) to RA.

The user also gives a (NI)zero-knowledge proof of knowledge for $(s_{id}, d) \in L_1$ using the Σ -protocol for L_1 described above:

$$PoK \left\{ (s_{id}, d) : \alpha = v^{s_{id}} g^d \right\}$$

$U \rightarrow RA$ User picks a random b_1, b_2 and sends $\gamma = v^{b_1} g^{b_2}$ to RA.

$U \rightarrow RA$ User generates a random challenge $c \in \mathbb{Z}_q$ by using the random-oracle H and the tag 0^n as $c = H(g, RA_{vk}, id, \alpha, \gamma, 0^n)$

$U \rightarrow RA$ User computes $z_1 = b_1 + cs_{id}$, $z_2 = b_2 + cd$ and sends (z_1, z_2) to RA.

RA verifies $v^{z_1} g^{z_2} \stackrel{?}{=} \alpha^c \gamma$.

$U \leftarrow RA$ RA checks that the identity id has not been registered before. RA chooses $r \in \mathbb{Z}_q$ randomly, computes the signature tuple $\sigma_1 \leftarrow g^x (u^{id} \alpha h)^r$, $\sigma_2 \leftarrow g_2^r$ and sends R the signature $\sigma_{id} = (\sigma_1, \sigma_2)$.

U User verifies the signature by checking that

$$e(\sigma_1, g_2) = e(g, g_2)^x \cdot e(u^{id} v^{s_{id}} g^d h, \sigma_2).$$

If this verifies, the user removes the commitment randomness by computing $\sigma'_1 = \sigma_1 / \sigma_2^d$ and stores the secret credential $(id, s_{id}, \sigma_{id} = (\sigma_1, \sigma_2))$.

FIG. 8

9/10

Survey Registration To create a survey:

SA Input: $SA_{vk} = (u_v, v_v, h_v, e(g, g_2)^y), SA_{sk} = y, vid \in \mathbb{Z}_q$

List of identities: L

SA For each $id \in L$, the SA computes the following:

Pick a random $r \in \mathbb{Z}_q$ and compute

$$\sigma^{vid_{id}} = (g^y (u_v^{vid} v_v^{id} h)^r, g_2^r)$$

Publish the list $L_{vid} = (vid, \{id_i, \sigma^{vid_{id}}\}_{i \in L})$

Authorized: Anyone can verify that a user with identity id is authorized to submit in survey vid by finding the corresponding signature $\sigma^{vid_{id}} = (\sigma_1, \sigma_2)$ in L_{vid} and then checking that

$$e(\sigma_1, g_2) \stackrel{?}{=} e(g, g_2)^y \cdot e(u_v^{vid} v_v^{id} h, \sigma_2).$$

FIG. 9

10/10

Submission To submit a survey:

Common Input: List L_{vid} , the public keys $SA_{vk} = (u_v, v_v, h_v, e(g, g_2)^v)$, and $RA_{vk} = (u, v, h, e(g, g_2)^x)$

User Secrets: id , submission m , credential (σ_{id}, s_{id})

The user aborts if the user has already participated in an survey with vid or $vid = s_{id}$.

The user and SA establish a secure connection in which SA is authenticated, but the user is anonymous.

U The user identifies the tuple $(vid, id_i, \sigma^{(i)})$ in L_{vid} in which $id_i = id$. The user computes $F_{s_{id}}(vid) = C \leftarrow e(g, g_2)^{1/(s_{id}+vid)}$.

$U \rightarrow SA$ User sends (vid, C, m, s_2, s_4) and an NIZKPOK of the statement (id, s_{id}, s_1, s_3) in L with tag $1||vid||m$ to the SA:

$$PoK \left\{ \begin{array}{l} (id, s_{id}, s_1, s_3) : \\ e(g, g_2)^x e(h, s_2) = e(s_1, g_2) e(u^{id} v^{s_{id}}, s_2)^{-1} \wedge \\ e(g, g_2)^y e(u_v^{vid} h_v, s_4) = e(s_3, g_2) e(v_v^{id}, s_4)^{-1} \wedge \\ e(g, g_2) \cdot C^{-vid} = C^{s_{id}} \end{array} \right\}$$

SA : If the proof verifies, record the submission (C, m) replacing any prior occurrence of $(C, \cdot)$.

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US15/31209

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 30/02; H04L 9/32; G06F 21/30 (2015.01)

CPC - G06Q 30/0203 H04L 9/3273; G06F 21/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8): G06Q 30/02; H04L 9/00, 9/32; G06F 17/30, 21/30 (2015.01)

CPC: G06Q 30/0203; H04L 9/3202, 9/3273; G06F 17/30, 21/31, 21/445; H04L 29/06816

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, INPADOC Data)

Keywords: survey, opinion poll, voting, anonymous, participant, respondent, user, client, authenticate, token, secret, message, identifier, nonce, key fob, private key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y ----- A	US 2008/0294559 A1 (WIELD, G. et al.) 27 November 2008; figures 1, 2; paragraphs [0034], [0036], [0040], [0046], [0071], [0079].	1, 3-4 ----- 2 ----- 5-13
Y ----- A	US 2014/0101262 A1 (ORACLE INTERNATIONAL CORPORATION) 10 April 2014; paragraph [0114].	2 ----- 5-13
A	US 2011/0307703 A1 (OGG, C. et al.) 15 December 2011; entire document.	1-13

☐

Further documents are listed in the continuation of Box C.

☐

See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

04 August 2015 (04.08.2015)

Date of mailing of the international search report

18 AUG 2015

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Shane Thomas

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774