1-1-2014

# New insight to preserve online survey accuracy and privacy in big data era

Joseph K. Liu
*Institute for Infocomm Research*

Man Ho Au
*University of Wollongong*, aau@uow.edu.au

Xinyi Huang
*Fujian Normal University*, xh068@uow.edu.au

Willy Susilo
*University of Wollongong*, wsusilo@uow.edu.au

Jianying Zhou
*Institute for Infocomm Research Singapore*, jyzhou@i2r.a-star.edu.sg

*See next page for additional authors*

# New insight to preserve online survey accuracy and privacy in big data era


## Abstract

An online survey system provides a convenient way for people to conduct surveys. It removes the necessity of human resources to hold paper surveys or telephone interviews and hence reduces the cost significantly. Nevertheless, accuracy and privacy remain as the major obstacles that need additional attention. To conduct an accurate survey, privacy maybe lost, and vice versa. In this paper, we provide new insight to preserve these two seeming contradictory issues in online survey systems especially suitable in big data era. We propose a secure system, which is shown to be efficient and practical by simulation data. Our analysis further shows that the proposed solution is desirable not only in online survey systems but also in several potential applications, including E-Voting, Smart-Grid and Vehicular Ad Hoc Networks. 2014 Springer International Publishing Switzerland.



## Keywords

privacy, insight, preserve, online, era, data, big, survey, accuracy


## Disciplines

Engineering | Science and Technology Studies


## Publication Details

Liu, J. K., Au, M., Huang, X., Susilo, W., Zhou, J. & Yu, Y. (2014). New insight to preserve online survey accuracy and privacy in big data era. Lecture Notes in Computer Science, 8713 (PART 2), 182-199.



## Authors

Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo, Jianying Zhou, and Yong Yu

# New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era

Joseph K. Liu[1], Man Ho Au[2], Xinyi Huang[3], Willy Susilo[4], Jianying Zhou[1], and Yong Yu[5]

[1] Institute for Infocomm Research, Singapore
{ksliu, jyzhou}@i2r.a-star.edu.sg
[2] Department of Computing, The Hong Kong Polytechnic University, Hong Kong
allen.au@gmail.com
[3] Fujian Normal University, China
xyhuang81@gmail.com
[4] University of Wollongong, Australia
wsusilo@uow.edu.au
[5] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
yyucd2012@gmail.com

**Abstract.** An online survey system provides a convenient way for people to conduct surveys. It removes the necessity of human resources to hold paper surveys or telephone interviews and hence reduces the cost significantly. Nevertheless, accuracy and privacy remain as the major obstacles that need additional attention. To conduct an accurate survey, privacy maybe lost, and vice versa. In this paper, we provide new insight to preserve these two seeming contradictory issues in online survey systems especially suitable in big data era. We propose a secure system, which is shown to be efficient and practical by simulation data. Our analysis further shows that the proposed solution is desirable not only in online survey systems but also in several potential applications, including E-Voting, Smart-Grid and Vehicular Ad Hoc Networks.

## 1 Introduction

Privacy has always been considered as a significant issue in our daily life. As an age-old concern, it is not unique in the digital world but the advances in digital technologies have brought an array of new privacy challenges. The granularity (or depth) of information captured in the digital world and the rapid information dissemination facilitated by the Internet are factors that contribute most to those new privacy concerns.

**Online Survey System.** One of the situations that privacy plays an important factor is an online survey system. An online survey system (e.g., Kwik Survey [15], My3q [23] or Survey Monkey [30]) is an Internet surveying technique in which the interviewee follows a script provided in a website. The questionnaires are created in a program for creating web interviews. The program allows for the

questionnaire to contain pictures, audio and video clips, or links to different web pages. The website is able to customize the flow of the questionnaire based on the answers provided, as well as information already known about the participant. It is considered to be a cheaper way of conducting surveys since it does not require any human resources to conduct surveys or telephone interview. With the increasing use of the Internet, online questionnaires have become a popular way of collecting information. The design of an online questionnaire often has an effect on the quality of data gathered. There are many factors in designing an online questionnaire, and issues including guidelines, available question formats, administration, ***accuracy*** and ***privacy*** should be carefully addressed. Here we focus on the last two factors.

A survey form may collect the interviewee's personal particulars, such as sex, age, salary range and interest. Such information may be very useful for the interviewer to conduct a survey with accurate information. However, the interviewer has no way to verify the authenticity of this information. For example, a 15 years old boy may say that "she" is a 50 years old woman earning one million US dollars per annual. This may not be possible if a face-to-face survey or telephone interviewing survey is carried out, or at least to some certain extent. Nevertheless, in a virtual world such as Internet, anonymity without authentication means the source is highly questionable. Furthermore, this 15 years old boy may fill in the online survey multiple times. Next time he may pretend he is a retired 80 years old man. There is no way to verify whether these 2 different surveys are from the same source or not.

Digital signature provides an easy and convenient way to authenticate the message sender in the Internet. By digitally signing a message (the survey), the verifier (the interviewer) can be convinced that the sender is a person with true particulars provided. Using the above example, assume Bob is that 15 years old boy. If he signs the survey, the interviewer may check his certificate (or identity if ID-based signature [29] is used) to find out his personal information from the certificate authority (or private key generator for ID-based signature). He cannot pretend to be another person. If he conducts the survey more than once, it will be easily detected since the signature contains the information of the signer.

It seems that digital signature can easily solve the problem of *accuracy*. However, on the other side, signing the survey means the loss of privacy. In reality, many users are not willing to reveal their real identities to interviewers due to privacy concerns. If it is a compulsory requirement for conducting the survey, they will decline the survey invitation. It maybe the main reason that many existing online survey systems do not compulsorily require interviewees to input their real identifying information (or no need to verify their information, e.g., no email validation is required).

**Contributions.** In this paper, we provide a new insight to preserve accuracy and privacy in online survey systems. We propose a new system which provides the following desirable features:

1. **Authentication**: It allows only those authenticated or qualified users to take part into the survey.

2. **Anonymity**: No one knows the identity of the user who has submitted the survey.
3. **Detection of double submission**: No one can submit more than once in a single survey event without being detected.
4. **Unlinkability**: Given two surveys from two different events, no one can tell whether they are from the same user.
5. **Constant Complexity**: The complexity of our system is independent to the total number of users in the system. Thus it is particularly suitable for any system with large user database in the **big data analytic era**.

We provide a concrete instantiation of our system. Further, we show our system to be efficient and practical by some simulation data analysis.

We believe our proposed system can fully resolve the contradiction between accuracy and privacy in online survey system. We also suggest other practical applications that can employ our system with only slightly modification required.

**Organization.** The rest of this paper is organized as follows. Some related works will be given in Section 2. Section 3 reviews the preliminaries required in this paper. In Section 4 we give an overview of our scheme, which is followed by detail description in Section 5. We present other applications that can deploy our primitive in Section 6 and conclude our paper in Section 7.

## 2 Related Works

There are many ways to resolve the contradiction between user privacy and data accuracy. Several solutions have been proposed and notable examples include ring signatures [27, 6] and group signatures [8, 2]. In ring signatures, one can spontaneously form a group of possible signers and sign on behalf of the group anonymously. One can also use group signatures to sign on behalf of a group of possible signers, but group signatures require an initial group setup procedure performed by the group manager who can revoke the anonymity of any group signer.

Attribute-Based Signatures [28, 16, 22, 26] (or, ABS for short) is another primitive proposed to provide signer anonymity. As a versatile primitive, ABS allows an entity to sign a message with fine-grained control over identifying information. A valid ABS signature attests to the fact that "A single user, whose attributes satisfy the predicate, has endorsed the message". Ring signatures and group signatures are then comparable to special cases of ABS, in which the only allowed predicates are disjunctions over the universe of attributes (identities). In ABS, each entity possesses a set of attributes and a key-authority generates the associated private keys, with which one can sign a message with a predicate satisfied by his/her attributes. The signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, ABS does not provide any information on the particular set of attributes used to satisfy the predicate. For example, an "(Engineer, Department A)" or an "(Engineer, Department B)" can independently

generate an ABS to assure the recipient that the signature was produced by an "Engineer" without disclosing the department information. Furthermore, users of ABS cannot collude to pool their attributes together (which separates ABS from mesh signatures): It is never possible for an "(Engineer, Department A)" and an "(Auditor, Department B)" to collude and generate an ABS satisfying the predicate "(Auditor, Department A)".

Yet all these solutions cannot resolve the contradiction. They are not practical enough to be used in an online survey system. For example, in a ring signature, it requires the signer to know all other members within the group. It is obvious impossible for an interviewee to know all other interviewee in a survey. For group signature, the properties of the group have to be fixed at the beginning. That is, assume we need to conduct a survey for female engineers aged between 20-25. Such a group has been formed (thus a group manager needs to distribute user secret keys for every user). Later on, another survey for British engineers ages between 20-25 will be conducted. Although there are some overlaps between these two groups of people, the secret key (obtained from the first group) cannot be reused, even for the same person since the properties of the group are fixed. In other words, for every single survey, it is required for the group manager to generate a new set of secret keys to every user. It is again impractical.

ABS seems to be the nearest solution. It provides user privacy. At the same time, it also authenticates the signers for some attributes at a flexible way. For example, assume Alice is a "female" "engineer" working in "Department A". Now there is a survey for all engineers in Department A. Those eligible interviewee including Alice can use their attribute "(Engineer, Department A)" to sign the survey. Later on, another survey for all female staff in department will be conducted. Alice can reuse her secret key but on a different attribute set "(Female, Department A)" to sign the survey. Different from ring signature, she does not need to know who else users will participate the survey. Also different from group signature, she does not need to obtain a different secret key for a different survey.

There is just one problem that ABS cannot resolve. Since ABS is anonymous, by no mean the verifier knows whether Alice has conducted twice or more in a survey, as depicted in Fig 1. In the Internet world, the situation is even worse. There are many programming scripts that can automatically submit online form. By using these scripts, one can submit a thousand of online forms in a very short period of time. The result will then be heavily biased. No existing designs of ABS can detect this kind of behavior.

It is fair to say no existing solutions can perfectly resolve the contradiction in an online survey system.

## 3 Preliminaries

### 3.1 Mathematical Definitions

**Bilinear Maps**. Let $\mathbb{G}_1, \mathbb{G}_2, G_T$ be cyclic (multiplicative) groups of order $p$, where $p$ is a prime. Let $g$ be a generator of $\mathbb{G}_1$, and $h$ be a generator of $\mathbb{G}_2$.

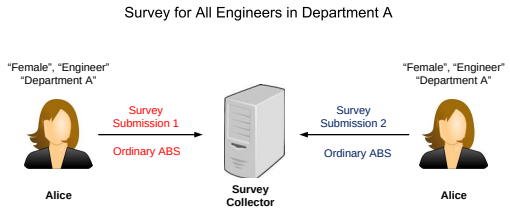


**Fig. 1.** Undetectable Double Submission Using Ordinary ABS

Then $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map if $\hat{e}(g, h)$ is a generator of $G_T$, and $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$ for all $a, b \in \mathbb{Z}_p$.

**Mathematical Hard Problem**. The security of our construction depends on the hardness of the following problem:

**Definition 1 (Decisional Diffie-Hellam Problem (DDH).).** *On input $g$, $g^a$, $g^b, Z \in \mathbb{G}$, decide whether $Z = g^{ab}$ or just a random element in $\mathbb{G}$. The DDH assumption states that the DDH problem is hard for any polynomial-time bounded algorithm.*

### 3.2 Monotone Span Programs

Let $\Upsilon : \{0,1\}^n \to \{0,1\}$ be a monotone boolean function. A monotone span program for $\Upsilon$ over a field $\mathbb{F}$ is an $\ell \times t$ matrix $\mathbf{M}$ with entries in $\mathbb{F}$, along with a labeling function $a : [\ell] \to [n]$ that associates each row of $\mathbf{M}$ with an input variable of $\Upsilon$, that for every $(x_1, ..., x_n) \in \{0,1\}^n$, satisfies the following:

$$\Upsilon(x_1, ..., x_n) = 1 \Longleftrightarrow \exists \boldsymbol{v} \in \mathbb{F}^{1\times\ell} \text{ such that}$$
$$\boldsymbol{v}\mathbf{M} = [1, 0, 0, ..., 0], \text{ and } (\forall i : x_{a(i)} = 0 \Rightarrow v_i = 0).$$

In other words, $\Upsilon(x_1, ..., x_n) = 1$ if and only if the rows of $\mathbf{M}$ indexed by $\{i | x_{a(i)} = 1\}$ span the vector $[1, 0, 0, ..., 0]$. We call $\ell$ the length and $t$ the width of the span program, and $\ell + t$ the size of the span program.

Readers may refer to [22] for the details.

## 4 Overview

### 4.1 Basic Idea

There are three entities in our system:

– Attribute Authority (AA): It is responsible for setting up the public parameters and issuing user secret keys for various attributes. In practice, it can be a government authority, computer service centre of an university or human resources department of a company.

- User: Any entity who has a user secret key is an user. A user can have different attributes.
- Survey Centre (SC): It is an organization to organize a survey. It is responsible to define the required policy of the survey, to collect the survey from users and to verify the result.

Basically our system is an ABS scheme. Each user generates an ABS using his own attributes required by the current survey. However, due to the unlinkability property of an ABS scheme, it is not suitable to be used directly, since a user may submit the survey more than once. We modify an ABS scheme from [22] by adding linkability to it. That is, any verifier is able to detect whether two signatures are generated by the same user within a single survey. Yet any user that generates two signatures in two different surveys cannot be linked. The survey centre can discard any double-submitted survey to maintain the accuracy of the result.

### 4.2 Assumptions

We assume each user communicates with SC through an anonymous channel [25, 14] or uses some IP-hiding technology. We also assume that the user keeps his secret key in a safe place. This can be achieved by some external means, such as keeping the secret key in a device to be always in possession or set it to be password-protected. When considering some attacks such as IP hijacking, distributed denial-of-service attack, man-in-the-middle attack etc., it is out of the scope of this paper.

### 4.3 Threat Model

In this sytem, we consider the following attacks:

1. (Unforgeability Attack:) The attacker acts as an unauthorized user (who does not possess the required attributes) who tries to submit a survey to the SC for being accepted.
2. (Anonymity Attack:) The attacker acts as the AA colluded with the SC who tries to find out the identity of the user of a particular submission.
3. (Linkability Attack:) The attacker acts as an authorized user who tries to submit more than one survey to the SC for being accepted in a single survey event.
4. (Unlinkability (for different users) Attack:) The attacker acts as an authorized user who tries to submit some surveys to link with other surveys submitted by honest users. The attack may have intention to do so in order to remove other undesirable results submitted by other users.

### 4.4 Notations

Notations used in our system are summarized in Table 1.

**Table 1.** Frequently Used Notations

| | |
|---|---|
| $TPK$ | system parameters |
| $APK$ | public key of the AA |
| $ASK$ | master secret key of the AA |
| $\mathbb{A}$ | universe of attributes |
| $\mathcal{A}$ | an attribute set of a user |
| $USK$ | user secret key |
| $m$ | data or the content of a survey |
| $event$ | the description of a particular survey event |
| $\Upsilon$ | policy of the survey |
| $\sigma$ | signature of the survey |

# 5 Details of Our Online Survey System

## 5.1 The Construction

Our system consists of different phases. The detailed step-by-step construction of each phase is given in the framed box.

**Setup.** The AA defines all system parameters and generates the public key and a master secret key.

*Details*: The AA first generates the system parameters as follows:

1. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear map (defined in Section 3.1) such that $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$ for some prime $p$. Let $g, G$ be generators of $\mathbb{G}_1$ and $\mathfrak{g}, \mathfrak{h}, h, h_0, \ldots, h_{t_{max}}, H$ be generators of $\mathbb{G}_2$. The value $t_{max}$ is the maximum width of the monotone span programs as defined in Section 3.2. Let $\mathbb{A} = \mathbb{Z}_p^*$ be the universe of attributes.
2. Assume the DDH problem (defined in Section 3.1) is hard in $\mathbb{G}_1$ and $\mathbb{G}_2$. Let $\mathcal{G} : \{0,1\}^* \rightarrow \mathbb{G}_1$, $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be hash functions that will be modeled as random oracles. The system parameters $TPK$ is ($\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, $\hat{e}$, $p$, $g$, $G$, $\mathfrak{g}$, $\mathfrak{h}$, $h$, $h_0$, …, $h_{t_{max}}$, $H$, $\mathcal{H}$, $\mathcal{G}$).

Then it generates the public and master secret keys as follows:

1. Choose $a_0, a, b, c \in_R \mathbb{Z}_p$ and compute: $C = g^c$, $A_0 = h_0^{a_0}$, $A_j = h_j^a$, $B_j = h_j^b$ for $j = 1, \ldots, t_{max}$.
2. Choose $s, v, w, z \in_R \mathbb{Z}_p$ and compute: $U = G^s$, $V = H^v$, $W = H^w$, $Z = H^z$.
3. Set the public key $APK$ as ($C$, $A_0$, $\{A_j, B_j\}_{j=1}^{t_{max}}$, $U$, $V$, $W$, $Z$) and the master secret key $ASK$ as $(a, a_0, b, s, v, w, z)$. Publish both $APK$ and $TPK$ while keep $ASK$ secret.

**User Key Generation.** The AA issues user secret key to each user, according to different attributes each user possesses. This is an interactive protocol between each user and the AA.

*Details*:

1. The user with an attribute set $\mathcal{A} \in \mathbb{A}$ randomly selects $L, r_L \in \mathbb{Z}_p$ and computes $C_L = \mathfrak{g}^L \mathfrak{h}^{r_L} \in \mathbb{G}_2$ and sends $C_L$ to the AA.
2. The AA randomly chooses $K_{base} \in_R \mathbb{G}_1$, $r \in_R \mathbb{Z}_p$ and uses the master secret key $ASK$ to compute: $K_0 = K_{base}^{\frac{1}{a_0}}$, $K_u = K_{base}^{\frac{1}{a+bu}}$ $\forall u \in \mathcal{A}$, $R = G^r$, $S = G^{z-rv} K_{base}^{-w}$, $T = (HC_L{}^{-s})^{\frac{1}{r}}$.
3. The AA returns $K_{base}$, $K_0$, $\{K_u\}_{u\in\mathcal{A}}$, $R$, $S$, $T$ to the user.
4. The user parses his user secret key $SK_{\mathcal{A}}$ as ($K_{base}$, $K_0$, $\{K_u\}_{u\in\mathcal{A}}$, $R$, $S$, $T$, $L$, $r_L$).

**Survey Submission.** The SC defines a survey event and a policy such that only those users that fulfill the policy with their attributes can participate this survey. The user submits the survey data together with the corresponding signature signed with his user secret key through an anonymous channel to the SC.

*Details*: Let $m$ be the data and *event* be the description of this survey. For a given policy $\Upsilon$ such that if a user with an attribute set $\mathcal{A}$ fulfills this policy, we have $\Upsilon(\mathcal{A}) = 1$. First convert the policy to its corresponding monotone span program $\mathcal{M} \in \mathbb{Z}_p^{\ell\times t}$ (defined in Section 3.2), with row labeling function $u : [\ell] \to \mathbb{A}$ and the vector $\boldsymbol{v}$ that corresponds to the satisfying assignment of $\mathcal{A}$. The user executes the following steps with his user secret key $SK_{\mathcal{A}}$:

1. Compute $\mu = \mathcal{H}(m||\Upsilon)$ and $\tau = \mathcal{G}(event)^L$.
2. Pick $r_0 \in_R \mathbb{Z}_p^*$, $r_1, \ldots, r_\ell \in_R \mathbb{Z}_p$ and compute $Y = K_{base}^{r_0}$, $W = K_0^{r_0}$, $S_i = (K_{u(i)}^{v[i]})^{r_0} (Cg^{\mu})^{r_i} (\forall i \in [\ell])$, $P_j = \prod_{i=1}^{\ell} (A_j B_j^{u(i)})^{\mathcal{M}_{ij}\cdot r_i} (\forall j \in [t])$.
3. Compute $\Pi_\tau$ as a non-interactive zero-knowledge proof-of-knowledge of the values ($R$, $S$, $T$, $K_{base}$, $r_0$, $L$, $r_L$) satisfying the following relation:

$$\begin{aligned} \hat{e}(R,V)\hat{e}(S,H)\hat{e}(K_{base},W) = \hat{e}(G,Z) \quad &\wedge \\ \hat{e}(R,T)\hat{e}(U,\mathfrak{g}^L\mathfrak{h}^{r_L}) = \hat{e}(G,H) \quad &\wedge \\ Y = K_{base}^{r_0} \quad &\wedge \\ \tau = \mathcal{G}(event)^L. \end{aligned}$$

   The details of $\Pi_\tau$ are shown in Appendix A.
4. Submit the survey data $m$ with its signature $\sigma = \left(Y, W, \{S_i\}_{i\in[\ell]}, \{P_j\}_{j\in[t]}, \tau, \Pi_\tau\right)$ to the SC.

**Validity Checking.** Upon received the survey, the SC checks its validity. The checking consists of two parts. In the first part, it verifies the signature to see

whether it is generated by a qualified user. In the second part, it checks whether this user has submitted another survey before. Note that the user is not allowed to submit more than one survey, no matter the content is the same or not.

*Details*: Upon received the data $m$ and the signature $\sigma$, the SC executes the followings:

1. Signature Verification:
   (a) Convert the policy $\Upsilon$ such that $\Upsilon(\mathcal{A}) = 1$ to its corresponding monotone span program $\mathcal{M} \in \mathbb{Z}_p^{\ell \times t}$, with row labeling function $u : [\ell] \to \mathbb{A}$.
   (b) Compute $\mu = \mathcal{H}(m||\Upsilon)$ and check if $\hat{e}(W, A_0) \stackrel{?}{=} \hat{e}(Y, h_0)$ and

$$\prod_{i=1}^{\ell} \hat{e}(S_i, (A_j B_j^{u(i)})^{\mathcal{M}_{i,j}}) \stackrel{?}{=} \begin{cases} \hat{e}(Y, h_1)\hat{e}(Cg^{\mu}, P_1), & \text{for } j = 1. \\ \hat{e}(Cg^{\mu}, P_j), & \text{for } j > 1. \end{cases}$$

   (c) Checks if $\Pi_\tau$ is a valid proof. The verification of $\Pi_\tau$ is also shown in Appendix A.

   If all equalities hold and the proof is correct, it outputs ACCEPT and proceeds to the second part. Otherwise it outputs REJECT.
2. Double Submission Checking: The SC extracts $\tau$ from $\sigma$ and checks its database whether any other signatures for this survey *event* also contain the the same $\tau$. If yes, that means the user has double submissions. It then outputs REJECT. Otherewise, it outputs ACCEPT and stores the data and signature into its database.

### 5.2 Security Analysis

To explain the security of our online survey system, we first present our design philosophy in details. As discussed in Section 2, the primitive attribute-based signature (ABS) is the closest solution to our problem. Thus, it is natural to construct our system from an existing ABS. An ABS is a tuple of five algorithms, namely, TSetup, ASetup, AttrGen, Sign, Ver, which are briefly reviewed below for completeness. Interested readers may refer to [22] for their formal definitions.

- TSetup is responsible for system parameters creation.
- ASetup is the process of creating the master key of the attribute authority.
- AttrGen is invoked to certify the attribute of a user.
- Sign is responsible for signature generations.
- Ver is responsible for signature verifications.

It is straightforward to observe the correspondence of an ABS and an online survey system. Specifically, the Setup procedure of our system consists of TSetup and ASetup. User Key generation procedure corresponds to AttrGen. For survey submission, the user submits the survey response together with an ABS-signature generated from Sign. Finally, the validity checking is realized by verifying the ABS-signature on the survey response, that is, an invocation of the algorithm Ver.

The security properties of any ABS, namely, unforgeability and perfect privacy would protect the resulting online survey system from unforgeability attack, anonymity attack and linkability attack. Unfortunately, such a system will be vulnerable under unlinkability attack. The reason is obvious, since an authorized user can submit the survey response together with a freshly generated attribute-based signature repeatedly without being detected. This lead to our approach, which is to restrict the number of times a signing key can be used for each survey *event*.

Our idea is to require that for each signature, the signer is required to attach with a piece of information called tag, which is a pseudo-random function on input of *event* and a secret that is known only to the user. If the user is in possession of one single secret, for each event, he/she can only create one tag without being detected. At the same time, since the secret is known only to the user, no one will be able to trace this user given tag.

The final issue is to bind the user secret to his/her signing key. With this binding, one authorized user will only be able to use the specific signing key. We introduce the technique of "certified signing key". Specifically, for each attribute-based signing key issued to an authorized user, the attribute authority also generates a standard signature on the signing key together with the commitment of the user secret. This standard signature is used to certify that this specific signing key is generated directly from the attribute authority and binds the signing key to this specific user secret. At the same time, the user secret is not revealed to the attribute authority due to the hiding property of the commitment scheme.

Finally, whenever the user uses his/her signing key, a zero-knowledge proof will be attached. The zero-knowledge proof serves as an evidence that the attribute-based signature is created from a "certified" signing key and that the tag is generated correct from *event* and the committed user secret.

**Notes on Our Practical System.** Our online survey system is built following the above framework using the ABS from [22]. The standard signature scheme used to certify the signing key together with the committed user secret is the signature scheme from [1]. The user secret is just a random element from $L \in \mathbb{Z}_p$ for some prime $p$ and that the commitment scheme is the well-known Pedersen commitment. The pseudo-random function on the user secret and *event* was defined as: $\mathcal{F} : L, event \mapsto \mathcal{G}(event)^L$.

It can be seen easily that the user secret key ($K_{base}$, $K_0$, $\{K_u\}_{u \in \mathcal{A}}$, $R$, $S$, $T$, $L$, $r_L$) in our system can be classified into three groups.

1. ABS signing key. $(K_{base}, K_0, \{K_u\}_{u \in \mathcal{A}})$ is exactly a signing key from the ABS scheme due to [22]
2. User secret: $(L)$. The Pedersen commitment of the user secret is $C_L = \mathfrak{g}^L \mathfrak{h}^{r_L}$ and thus $r_L$ is the randomness used in the commitment.
3. Certification of the signing key. $(R, S, T, L)$ is the standard signature (of the scheme [1]) on the tuple $(K_{base}, C_L)$.

Note that we have simplified the process of "certified signing key" by signing $K_{base}$ and $C_L$ since each signing key is uniquely determined by the value $K_{base}$.

The role of the zero-knowledge proof $\Pi_\tau$ in the survey submission can be explained easily after this classification. It states that the generator of the ABS signature is in possession of a user secret $L$ and that the tag $\tau$ is created correctly from $\tau$. In addition, the generator of the signature is creating this signature from a "certified signing key" (i.e., he/she is in possession of a standard signature $(R, S, T, L)$ on the tuple $(K_{base}, C_L)$ and that $K_{base}$ is used in this ABS signature creation and $C_L$ is a commitment of $L$).

Now we are ready to give a security argument based on the threat model defined in Section 4.3.

1. **Security against Unforgeability Attack.** Each survey response has to be accompanied with a properly created attribute-based signature and in our system, only authorized users are issued the signing keys. Thus, if the ABS scheme from [22] is unforgeable, our system is secure against unforgeability attack.
2. **Security against Anonymity Attack.** The only information related to the survey participant is the ABS signature, the zero-knowledge proof $\Pi_\tau$ and the tag $\tau$. Due to the perfect privacy of the ABS scheme from [22], the ABS part leaks no information about the actual participant. The zero-knowledge proof $\Pi_\tau$ (details are given in Figure **??**), a standard non-interactive $\Sigma$-protocol, leaks no information due to its zero-knowledgeness (in the random oracle model). Finally, the tag $\tau$ itself is created from $\mathcal{G}(event)^L$. Since $L$ is never shown in plain and is protected by the perfect hiding property of the Pedersen commitment, it again leaks no information about the survey participant. In fact, our construction provides a stronger level of privacy. Specifically, if the user never participate in the same survey more than once, his participation across different surveys are not relatable under the decisional Diffie-Hellman assumption. That is, given $event_1$, $event_2$, $\mathcal{G}(event_1)^L$ and a value $\tau^*$, it is computationally hard to tell if $\tau^* = \mathcal{G}(event_2)^L$ or not. Recall that our system is built on bilinear groups with pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ such that the DDH problem is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$.
3. **Security against Linkability Attack.** Each authorized user in our system is given only one "certified signing key" only and thus for each survey, he or she can only generate one unique tag $\tau$. This is due to the fact that the non-interactive zero-knowledge proof $\Pi_\tau$ is sound (i.e. the attacker cannot produce a fake proof) and the signature from [1] is unforgeable (i.e. the attacker cannot produce a fake certified signing key).

4. **Unlinkability (for different users) Attack.** Two surveys are linked if they share the same tag $\tau$. In order to use a tag, the attacker has to produce the zero-knowledge proof $\Pi_\tau$. That is, the attacker either produces a fake proof or has to know the value of $L$ that is used to generate $\tau$. The former is computationally impossible under the soundness property of the zero-knowledge proof $\Pi_\tau$. The latter is computationally impossible under the discrete logarithm assumption.

### 5.3 A Practical Example

Here we briefly describe how to deploy our system in a company. Assume there is a multinational corporation ABC, which is working in the cosmetics business arena. The human resources department (HR) acts as the AA to carry out the **Setup** phase. When a new staff joins this corporation, the HR issues his/her secret key by executing **User Key Generation** phase. The attribute set may contain the following items: sex, marital status, location, date of birth and department. Suppose the marketing department of ABC intends to introduce a new night cream product into its Japanese market product line. Part of the feasibility study involves conducting an online survey to find out the preference of Japanese women in the Japanese market. As a preliminary step, the marketing department would like to conduct the survey to the staff of ABC before gathering responses from the public. To do this, firstly the marketing department will act as the SC. In this scenario, the targets are very clear, namely Japanese female staffs. All the Japanese female staffs can use their secret key to sign the completed online form by using **Survey Submission** algorithm using the attribute "female" and "Japanese". The signed and completed form may be sent back to the server through an anonymous channel. The marketing department executes **Validity Checking** to check the validity of each survey. It discards any survey which has not been signed by the attribute "female" and "Japanese", and those who are linked (that means duplicated copies).

### 5.4 Performance Analysis

**Generic Analysis.** We give the performance analysis of our concrete instantiation described in Section 5.1. We first give a generic analysis, which varies for different attribute sets and signing policies. We only count the time required for exponentiation and pairing. Other operations such as hashing, group addition, integer addition/multiplication etc. are insignificant compared with exponentiation and pairing. For exponentiation, we further optimize for those bases which are constant. It allows the use of some pre-processed data for faster computation. For pairing, we also optimize for those such that one of the pairing elements is a constant. We put our analyzed result in Table 2. We use $t_{max}$ to represent the maximum width of the monotone span program, $|\mathcal{A}|$ to represent the number of attributes a user has, $t$ and $\ell$ to represent the width and length of the monotone span program converted from the signing claim policy respectively.

**Table 2.** Operations required

| | ASetup | AttrGen | Sign | Verify |
|---|---|---|---|---|
| Group $\mathbb{G}_1$ / $\mathbb{G}_2$ exponentiation (pre-processed) | $6 + 2\ t_{max}$ | 3 | 12 | 0 |
| Group $\mathbb{G}_1$ / $\mathbb{G}_2$ exponentiation (no pre-processed) | 0 | $2 + \lvert\mathcal{A}\rvert$ | $2 + 2\ \ell + t\ell$ | $6 + t\ell$ |
| Group $\mathbb{G}_T$ exponentiation (pre-processed) | 0 | 0 | 7 | 7 |
| Group $\mathbb{G}_T$ exponentiation (no pre-processed) | 0 | 0 | 0 | 2 |
| Pairing (1 element is a constant) | 0 | 0 | 0 | $5 + t$ |
| Pairing (both elements are not constant) | 0 | 0 | 0 | $2 + t\ell$ |

**Concrete Example.** Next we analyze the efficiency of our scheme using the simulation result from jPBC [21] for the following devices:

– A desktop equiped with Intel(R) Core(TM)2 Quad CPU Q6600 2.40GHz, 3 GB RAM, Ubuntu 10.04 as the simulation device.

We measured the performance using a 160-bit secret key in elliptic curve cryptosystem (ECC). It is generally believed that a 160-bit secret key in ECC provides stronger security than a 1024-bit key in RSA. We use the example described in Section 5.3 to illustrate the exact running time and communication overhead. In the example, we assume the following attributes:

– Sex: {Male}, {Female}
– Marriage Status: {Single}, {Married}, {Divoice}
– Office Location: {United States}, {United Kingdom}, {Australia}, {Japan}, {China}
– Year of Bith: $\{\leq 1960\}$, $\{1961 - 1970\}$, $\{1971 - 1980\}$, $\{1981 - 1990\}$, $\{> 1990\}$
– Department: {Sales}, {Finance}, {Logistic}, {Human Resources}

Now it plans to carry out some surveys based on the following different cases:

1. All staffs who are based in Japan.
2. All Female staffs who are Married.
3. All Male staffs who are based in Australia and working in the Sales department.
4. All Female staffs who are Single, born after 1990 and based in Japan.
5. All Male staffs who are Married, based in United States, born between 1971-1980 are working in the Finance department.
6. All staffs who are based in *either* Australia *or* China and working in the Sales department.
7. All Female staffs who are based in United Kingdom and working in *either* Finance *or* Human Resources department.

The simulation result is shown in Table 3. The unit for running time is $ms$ while the unit for public parameter $APK$, secret key and signature is *byte*.

**Table 3.** Performance

| Case | Size of $APK$ | **Ur. Key Gen.** running time | Size of se. key | **Survey Subm.** running time | Size of signature | **Val. Check** running time |
|---|---|---|---|---|---|---|
| 1 | 880 | 138.667 | 220 | 127.052 | 480 | 225.915 |
| 2 | | | | 182.828 | 520 | 333.185 |
| 3 | | | | 350.156 | 560 | 506.893 |
| 4 | | | | 517.484 | 600 | 747.12 |
| 5 | | | | 721.996 | 640 | 1053.839 |
| 6 | | | | 294.38 | 540 | 399.65 |
| 7 | | | | 443.116 | 580 | 606.631 |

## 6 Other Applications

We note that the protocol described in this paper is specifically designed for online survey systems. However, we do not eliminate the possibility to apply our scheme (or modified version) in other environments if they find it suitable. We list some of the potential applications:

Electronic Voting (E-Voting) [7, 11, 5, 13, 12, 19] is introduced to replace existing punched-card and mechanical voting systems. With e-voting, one can cast ballots from the comfort of his/her home or from mobile devices like cellular phones or iPads, and this is a great convenience to people, especially those disabled and aging population. On the other hand, e-voting also introduces a wide range of privacy and security issues. As an example, tallying authorities want to be assured that a ballot is from a voter satisfying certain requirements and any eligible voter can vote only once (to eliminate double-voting), but due to privacy concerns voters want to prevent tallying authorities from telling who they are.

One of the solutions is using linkable ring signatures [18, 20, 3, 10, 31, 4, 17]. Like normal ring signatures, linkable ring signatures provide signer anonymity but one can verify whether or not two ring signatures were signed using the same key. In the scenario of e-voting, the voter first creates a group of eligible voters and then produces a linkable ring signature on the ballot. Such a signature ensures the tallying authority that the ballot is from an eligible person in the group but does not tell who the actual voter is, due to the anonymity of ring signatures. Any double voting will be detected since the signature is linkable.

E-voting based on linkable ring signature has demonstrated several practice-friendly properties, but a closer look discovers a subtle issue to be addressed, namely how to tell if someone else is eligible for the voting when one forms a group of eligible persons. This issue can be easily solved in some cases, e.g., "any female staff is eligible for voting", but not if the requirements include "anyone with monthly income less than $1,000". It is very unlikely that such privacy information is publicly known, or an entity wants to share it with others. In such cases, it would be difficult to form a group with a large number of eligible persons, and this could put the privacy of the actual voter at risk.

Another disadvantage of linkable ring signature based e-voting system is the requirement for voters to know the identities or public keys of all eligible voters, especially in the case when the number of voters is very large. It is

certainly a desirable choice if one can vote anonymously without the need to find other eligible persons, and this reminds us of attribute-based signatures. Each entity in attributed-based signatures is given a private key according to the attributes he/she possesses. One can use the private key to sign the ballot, and the resulting signature only shows that it is from a person satisfying certain attributes (e.g., the voting requirements). Compared with ring signatures, the advantage of attribute-based signatures is that there is no need to form a group of eligible persons, and thus issues like "Does Alice satisfy voting requirements?" are eliminated. However, we still need to detect double-voting if attribute-based signatures are used in e-voting, and this would require the linkability in ABS.

Smart Grid [24] is a form of electricity network utilizing modern digital technology. The most distinctive feature in smart grid is its two-way capabilities for data communication: Not only the grid controller can issue commands to intelligent devices, consumers and devices can also send data to grid controllers. This feature brings controllers and consumers with an in-depth insight of energy usage, which would lead to a more efficient electricity system.

Attribute-based signature seems to be a promising approach to address the aforementioned issue. Each entity is given a private key according to the attributes he/she possesses. One can sign the energy consumption data using his/her own private key, and such a signature can convince the service provider that the data is from a person satisfying certain attributes, without the need to seek other consumers with similar attributes. It is a natural requirement that each data is counted only once in statistical reports, and an attribute-based signature scheme with linkability will better suit that situation. More importantly, smart grid usually comprises big data for analysis. Attribute-based protocol allows a constant complexity for authentication, which is independent to the number of users in the system. Thus it is particularly suitable in this scenario.

Vehicular Ad Hoc Networks (VANETs) allow wireless communications between vehicles and roadside infrastructures. Chen *et al.* [9] addressed the problem of reliability of information exchange between vehicles. Suppose that a car driver Bob receives a message from another vehicle reporting some traffic jam a few miles away, he has no idea whether the message is true or not. At the beginning, he attempts to ignore it. But shortly after that he receives several messages (say $n$) reporting the same traffic jam. If this number $n$ is a reasonably large number and these messages are sent by $n$ different vehicles, this information is likely to be true, as it seems unlikely that any $n$ vehicles would collude to lie. However, all these messages are sent anonymously due to privacy concern, how can Bob find out whether $n$ received messages are sent by $n$ different legitimate vehicles without discovering the identities of these vehicles? The authors proposed a solution using Threshold Anonymous Announcement (TAA) service.

TAA allows every vehicle to obtain a token from a trusted party. One may broadcast an anonymous message to other vehicles signed by this token so that anyone received this broadcast message may know that it is from a legitimate vehicle yet the identity is unknown. At the same time, TAA provides linkability. That is, if a vehicle sends the same message twice, the receiver will be

able to know these two messages are sent by the same vehicle. So it is easy to distinguish whether $n$ messages are from $n$ different vehicles. However, their scheme only provides linkability to the same message from the same signer. If the signer slightly changes the message, e.g., change from "`The city area is very congested now.`" to "`Now the city area is very congested.`", they appear as two different messages and thus cannot be linked. That is, a receiver cannot distinguish whether these two messages are sent by the same signer.

Using linkable ring signature may resolve this issue, because linkable ring signature provides event-based linkability. In a single event (e.g., traffic congestion announcement in the city area), any two signatures generated by the same singer will be linked, no matter the two signed messages are the same or not. Nevertheless, linkable ring signature requires the signer to know the identities of all legitimate vehicles in the area, which is impossible. An event linkable attribute-based signature provides a better solution because it does not require anyone to know other legitimate vehicles, while providing event-based (instead of message-based) linkability. Simultaneously anonymity of the signer is also preserved.

## 7 Conclusion

In this paper, we provided a new insight to preserve accuracy and privacy in online survey systems simultaneously. The new insight comes from our proposed system. We proved the security of it. The performance analysis is also given to show that our system is efficient and practical. In addition to online survey systems, we further suggested several other applications that can make use of our new system, including e-voting, smart-grid and vehicular ad hoc networks. We believe our system is particular suitable for handling big data as the complexity remains constant, regardless to the number of users.

## References

1. M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. In P. Rogaway, editor, *CRYPTO*, volume 6841 of *LNCS*, pages 649–666. Springer, 2011.
2. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *CRYPTO 2000*, volume 1880 of *LNCS*, pages 255–270. Springer, 2000.
3. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In *ISPEC*, volume 4464 of *LNCS*, pages 79–92. Springer, 2007.
4. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Secure id-based linkable and revocable-iff-linked ring signature with constant-size construction. *Theor. Comput. Sci.*, 469:1–14, 2013.
5. J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections (Extended Abstract). In *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 544–553. ACM Press, 1994.
6. X. Boyen. Mesh Signatures. In M. Naor, editor, *EUROCRYPT*, volume 4515 of *LNCS*, pages 210–227. Springer, 2007.

7. D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, Feb. 1981.
8. D. Chaum and E. van Heyst. Group Signatures. In *EUROCRYPT 91*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.
9. L. Chen, S.-L. Ng, and G. Wang. Threshold Anonymous Announcement in VANETs. *IEEE Journal on selected areas in communications*, 29(3):605–615, 2011.
10. S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust Receipt-Free Election System with Ballot Secrecy and Verifiability. In *NDSS*. The Internet Society, 2008.
11. A. Fujioka, T. Okamoto, and K. Ohta. A Practical Secret Voting Scheme for Large Scale Election. In *AUSCRYPT 91*, pages 244–260. Springer, 1992. LNCS No. 718.
12. J. Groth. A Verifiable Secret Shuffle of Homomorphic Encryptions. In *PKC 2003*, volume 2567 of *LNCS*, pages 145–160. Springer, 2003.
13. M. Hirt and K. Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 539–556. Springer, 2000.
14. A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In *WPES 2005*, pages 61–70. ACM Press, 2005.
15. Kwik Survey. KwikSurveys: Offical Free online survey and questionnaire tool. http://www.kwiksurveys.com/.
16. J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren. Attribute-Based Signature and Its Applications. In D. Feng, D. A. Basin, and P. Liu, editors, *ASIACCS*, pages 60–69. ACM, 2010.
17. J. K. Liu, M. H. Au, W. Susilo, and J. Zhou. Linkable ring signature with unconditional anonymity. *IEEE Trans. Knowl. Data Eng.*, 26(1):157–165, 2014.
18. J. K. Liu, V. K. Wei, and D. S. Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In *ACISP 2004*, volume 3108 of *LNCS*, pages 325–335. Springer, 2004.
19. J. K. Liu and D. S. Wong. A Restricted Multi-show Credential System and its Application on E-Voting. In *ISPEC 2005*, volume 3439 of *LNCS*, pages 268–279. Springer, 2005.
20. J. K. Liu and D. S. Wong. Enhanced security models and a generic construction approach for linkable ring signature. *Int. J. Found. Comput. Sci.*, 17(6):1403–1422, 2006.
21. B. Lynn. The Java Pairing Based Cryptography Library (jPBC), 2010. http://libeccio.dia.unisa.it/projects/jpbc/.
22. H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-Based Signatures. In *CT-RSA*, volume 6558 of *LNCS*, pages 376–392. Springer, 2011.
23. My3q. FREE Online Survey Questionnaire Research by my3q. http://www.my3q.com/.
24. N. I. of Standards and Technology. NIST IR 7628: Guidelines for Smart Grid Cyber Security. Technical report, http://csrc.nist.gov/publications/PubsNISTIRs.html, 2010.
25. T. Okamoto. Receipt-Free Electronic Voting Schemes for Large Scale Elections. In *Workshop on Security Protocols 97*, volume 1361 of *LNCS*, pages 25–35. Springer, 1997.
26. T. Okamoto and K. Takashima. Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model. In *Public Key Cryptography*, volume 6571 of *LNCS*, pages 35–52. Springer, 2011.
27. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001.

28. S. F. Shahandashti and R. Safavi-Naini. Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. In B. Preneel, editor, *AFRICACRYPT*, volume 5580 of *LNCS*, pages 198–216. Springer, 2009.
29. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO 84*, volume 196 of *LNCS*, pages 47–53. Springer, 1984.
30. Survey Monkey. SurveyMonkey: Free online survey software and questionnaire tool. http://http://www.surveymonkey.com/.
31. T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou. Efficient linkable and/or threshold ring signature without random oracles. *Comput. J.*, 56(4):407–421, 2013.

## A Details of $\Pi_\tau$

$\Pi_\tau$ can be constructed in the random oracle model using 19 elements.

Let $\mathfrak{g}_1, \mathfrak{g}_2$ be generators of $\mathbb{G}_1$ and $\mathfrak{h}_1, \mathfrak{h}_2$ be generators of $\mathbb{G}_2$. They can be regarded as part of TPK. The signer randomly chooses $x_1, \ldots, x_6 \in_R \mathbb{Z}_p$, computes: $X_1 = \mathfrak{g}_1^{x_1}\mathfrak{g}_2{}^{x_2}$, $X_2 = R\mathfrak{g}_1^{x_2}$, $X_3 = S\mathfrak{g}_1{}^{x_3}$, $X_4 = \mathfrak{g}_1^{x_4}\mathfrak{g}_2^{x_5}$, $X_5 = K_{base}\mathfrak{g}_1^{x_5}$, $Y_1 = T\mathfrak{h}_1^{x_6}$. The signer also randomly chooses $\rho_1, \ldots, \rho_{13} \in_R \mathbb{Z}_p$ and computes: $\mathfrak{T}_1 = \mathfrak{g}_1^{\rho_1}\mathfrak{g}_2^{\rho_2}$, $\mathfrak{T}_2 = \mathfrak{g}_1^{\rho_4}\mathfrak{g}_2^{\rho_5}$, $\mathfrak{T}_3 = X_1^{-\rho_6}\mathfrak{g}_1^{\rho_7}\mathfrak{g}_2^{\rho_8}$, $\mathfrak{T}_4 = X_4^{-\rho_{11}}\mathfrak{g}_1^{\rho_9}\mathfrak{g}_2^{\rho_{10}}$, $\mathfrak{T}_5 = \hat{e}(\mathfrak{g}_1, V)^{\rho_2} \cdot \hat{e}(\mathfrak{g}_1, H)^{\rho_3} \cdot \hat{e}(\mathfrak{g}_1, W)^{\rho_5}$, $\mathfrak{T}_6 = \hat{e}(X_2, \mathfrak{h}_1)^{-\rho_6} \cdot \hat{e}(\mathfrak{g}_1, Y_1)^{-\rho_2} \cdot \hat{e}(\mathfrak{g}_1, \mathfrak{h}_1)^{\rho_8} \cdot \hat{e}(U, \mathfrak{g})^{\rho_{12}} \cdot \hat{e}(U, \mathfrak{h})^{\rho_{13}}$, $\mathfrak{T}_7 = X_5^{\rho_{11}}\mathfrak{g}_1^{-\rho_{10}}$, $\mathfrak{T}_8 = \mathcal{G}(event)^{\rho_{12}}$. Then, the signer computes $k = \mathcal{H}(\mathfrak{T}_1 \ldots || \mathfrak{T}_8 || X_1 || \ldots || X_5 || Y_1 || m || event || \Upsilon)$ and computes:

$$z_1 = \rho_1 - kx_1, \quad z_2 = \rho_2 - kx_2, \quad z_3 = \rho_3 - kx_3,$$

$$z_4 = \rho_4 - kx_4, \quad z_5 = \rho_5 - kx_5, \quad z_6 = \rho_6 - kx_6,$$

$$z_7 = \rho_7 - kx_1x_6, \quad z_8 = \rho_8 - kx_2x_6, \quad z_9 = \rho_9 - kx_4r_0,$$

$$z_{10} = \rho_{10} - kx_5r_0, \quad z_{11} = \rho_{11} - kr_0, \quad z_{12} = \rho_{12} - kL, \quad z_{13} = \rho_{13} - kr_L.$$

Parse $\Pi_\tau$ as ($k$, $X_1$, ..., $X_5$, $Y_1$, $z_1$, ..., $z_{12}$). It consists of 5 elements in $\mathbb{G}_1$, one element in $\mathbb{G}_2$ and 13 elements of $\mathbb{Z}_p$.

To verify $\Pi_\tau$, the verifier computes: $\mathfrak{T}'_1 = X_1^k\mathfrak{g}_1^{z_1}\mathfrak{g}_2^{z_2}$, $\mathfrak{T}'_2 = X_4^k\mathfrak{g}_1^{z_4}\mathfrak{g}_2^{z_5}$, $\mathfrak{T}'_3 = X_1^{-z_6}\mathfrak{g}_1^{z_7}\mathfrak{g}_2^{z_8}$, $\mathfrak{T}'_4 = X_4^{-z_{11}}\mathfrak{g}_1^{z_9}\mathfrak{g}_2^{z_{10}}$,

$$\mathfrak{T}'_5 = \left(\frac{\hat{e}(X_2, V)\hat{e}(X_3, H)\hat{e}(X_5, W)}{\hat{e}(G, Z)}\right)^k \cdot \hat{e}(\mathfrak{g}_1, V)^{z_2}\hat{e}(\mathfrak{g}_1, H)^{z_3}\hat{e}(\mathfrak{g}_1, W)^{z_5},$$

$$\mathfrak{T}'_6 = \left(\frac{\hat{e}(G, H)}{\hat{e}(X_2, Y_1)}\right)^k \hat{e}(X_2, \mathfrak{h}_1)^{-z_6}\hat{e}(\mathfrak{g}_1, Y_1)^{-z_2} \cdot \hat{e}(\mathfrak{g}_1, \mathfrak{h}_1)^{z_8}\hat{e}(U, \mathfrak{g})^{z_{12}}\hat{e}(U, \mathfrak{h})^{z_{13}},$$

$\mathfrak{T}'_7 = Y^k X_5^{z_{11}}\mathfrak{g}_1^{-z_{10}}$, $\mathfrak{T}'_8 = \tau^k\mathcal{G}(event)^{z_{12}}$. Accept the proof if and only if:

$$k \stackrel{?}{=} \mathcal{H}(\mathfrak{T}'_1 \ldots || \mathfrak{T}'_8 || X_1 || \ldots || X_5 || Y_1 || m || event || \Upsilon).$$