Exploring Linkable Ring Signatures to Ensure Anonymity and Authenticity in Survey Research: A Methodological Design Proposal and Architectural Model

Francisco das Chagas[1], Emerson B. Tomaz[1], Allysson Allex Araújo[2]

[1]Universidade Federal do Ceará (UFC)
Campus de Crateús
Crateús, Ceará – Brasil

[2]Universidade Federal do Cariri (UFCA)
Centro de Ciências e Tecnologia (CCT)
Juazeiro do Norte, Ceará – Brasil

franciscochaves@alu.ufc.br, emerson@crateus.ufc.br,
allysson.araujo@ufca.edu.br

Abstract. *Survey research holds significant importance in various areas related to Information Systems (IS), spanning from academia to the business context and public governance. However, it is common for many research endeavors to face challenges related to data authenticity, whether due to unauthorized access by individuals or incorrect responses stemming from a lack of anonymity for participants. This paper presents an ongoing research endeavor aimed at developing a web application based on Linkable Ring Signatures scheme capable of enabling the anonymous authentication of participants in surveys. In particular, the objective of this paper lies in the methodological design proposal and an architectural model. Regarding the contributions for IS research and practice, we introduce a novel architectural model based on the Linkable Ring Signature to ensure anonymous authenticity in survey research. We also emphasize the importance of fostering trust in survey participation and its design/process.*

1. Introduction

Survey research is a descriptive method employed to gather data from a representative sample of the target population [Mathiyazhagan and Nandan 2010]. Surveys are utilized when researchers seek to inquire into the attitudes, opinions, beliefs, behaviors, or characteristics of a sample or population [Creswell and Guetterman 2018]. This research endeavor is prevalent across different domains, including businesses, academic institutions, healthcare facilities, and governmental agencies, serving as a means for data collection and evaluation of their respective entities. Consequently, survey research emerges as a highly used and valuable data collection approach, offering clear benefits by aiding in the depiction and exploration of variables and constructs of interest.

However, a challenge often faced when designing survey research is ensuring anonymity and authenticity. In this regard, anonymity is understood as the state of not being identified within a group of subjects [Pfitzmann and Hansen 2000]. In some scenarios, preserving anonymity is of substantial importance because it ensures that participants' information will be treated cautiously and encourages their participation. On the other hand, user authenticity refers to verifying a user's identity to access a system or service [Gaharana and Anand 2015]. Without proper authentication, participants from undesired groups may engage in the survey, resulting in inaccurate data.

Reconciling the need for anonymity and participant authenticity is a challenging task. Anonymity is necessary to protect the participant's identity and ensure that they remain unidentified. On the other hand, authenticity requires verifying the participant's identity. For instance, in the context of Information Systems (IS), a company may send an anonymous online questionnaire to collect data on the usability of their internal system. However, since the questionnaire is anonymous, it can be easily shared by malicious users with unauthorized individuals. This issue poses a challenge for leadership in determining whether responses are from genuine users. Moreover, to encourage honest feedback, participants must feel secure in providing their opinions without fear of any repercussions. Hence, it is essential to balance these aspects to foster open and truthful participation, ultimately leading to better decision-making processes in the future.

To address the challenge of enabling anonymous authentication, Rivest *et al.* (2001) proposed a Ring Signature scheme. However, this scheme lacks the capability to ascertain whether two signatures were issued by the same participant, a shortcoming that, if employed in survey research, may introduce the risk of a participant submitting responses multiple times. In response to this limitation, Liu and Wong (2005) proposed a Linkable Ring Signature scheme wherein it was feasible to verify whether two signatures were issued by the same group member. Based on these related works, we advocate that this scheme could be useful to enable the anonymity and authenticity in survey research, including how to deal with possible repeated entries by participants within a group.

Motivated by the aforementioned rationale, this study is part of an ongoing research endeavor aimed at developing a web application based on the Linkable Ring Signature to enable participant anonymization and authenticity in survey research, thus preserving the privacy and credibility of information. Specifically, this paper seeks to discuss the methodological design and architectural model underlying the proposed web application under development, which are considered preliminary results of this research project. In contrast to the ANONIZE system [Hohenberger et al. 2014], our closest related solution, our approach stands out by exploring Linkable Ring Signatures rather than token-based technology, primarily due to their ability to differentiate among the cohorts submitting the survey. Furthermore, our architecture was designed to make its extensibility and adoption by the community more accessible.

This paper offers contributions from three key dimensions, which hold particular value for both academia and practice within IS domain. From a *technological* dimension, we introduce a promising architectural model (along with its methodological design) grounded in the Linkable Ring Signature scheme to ensure anonymity and authenticity. In terms of *process*, we contribute to heightening awareness regarding the necessity of developing a solution that facilitates anonymity and authenticity in survey research. Concerning *people*, we engage in a discourse surrounding the expectation of trust regarding survey participation or conduct. By acknowledging the interplay and alignment among these dimensions, our contribution goes beyond technical implementation to encompass valuable social implications, including the challenge of "Methodologies and Technologies for Citizen Participation" outlined in the I GranDSI-BR [Boscarioli et al. 2017].

2. Research Method

The methodological scope of this study is qualitative and descriptive, coupled with Design Science Research (DSR). In this regard, Figure 1 provides an overview of our methodological design, structured into five stage suggested by Vaishavi and Kuechler (2004). The first stage entails **Awareness of the Problem**, involving an ad-hoc analysis of scientific and grey literature. The **Suggestion** phase involves the creation of a *tentative design* in the form of an architectural model of the web solution (*instantiation artifact*) to be developed. The **Development** stage encompasses the implementation of the artifact itself, involving: i) the *Application Programming Interface* (API) composed of the Ring Signature algorithm and responsible for all rules; ii) the structuring of the database to store research data and participants' public keys; iii) the integration of all created modules. **Evaluation** will be conducted through a qualitative analysis based on scenarios to investigate the artifact's suitability, delving into potential use cases and the technical measures undertaken to address them [Hevner et al. 2008]. The aim is to assess the technical viability of the solution in fulfilling its proposed objective and its capacity to handle adverse scenarios. In this sense, implementation details and empirical evidence from the analysis based on proposed scenarios will be discussed. Finally, the last stage is the **Conclusion**, where all acquired knowledge is critically discussed alongside research findings.

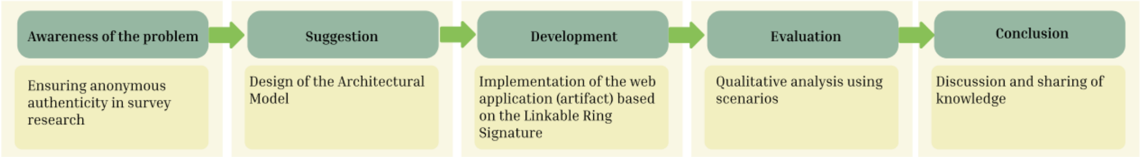
Awareness of the problem
Ensuring anonymous authenticity in survey research
Suggestion
Design of the Architectural Model
Development
Implementation of the web application (artifact) based on the Linkable Ring Signature
Evaluation
Qualitative analysis using scenarios
Conclusion
Discussion and sharing of knowledge

Figure 1. Methodological Design based on DSR [Vaishnavi and Kuechler 2004].

The following details are provided regarding the scenarios for **Evaluation**:

- *Scenario #1 - Solution achieves its objective*: The entire workflow of the solution works as expected. That is, the researcher can collect and analyze data without any inconsistencies, and participants respond to the survey without malicious intent and with full awareness of their responses;
- *Scenario #2 - Researcher attempts to determine who was responsible for a specific response*: The Linkable Ring Signature scheme complicates the identification of the individual responsible for a particular response. This issue is due to the aspect of Signer Anonymity, wherein even if a researcher possesses knowledge of t private keys within a group of n users, they will not be able to identify the user with a probability greater than $1/(n-t)$ [Liu and Wong 2005];
- *Scenario #3 - Individuals attempting to respond to the survey more than once*: The application should only allow one response to the survey, after which the form should expire. Even if a user manages to circumvent this system, it is possible to verify through the Linkable Ring Signature scheme whether a user has submitted the survey more than once;
- *Scenario #4: Unauthorized individuals respond to the survey:* Occurs when one or more authorized users share the keys creation link with other users, enabling them to create their own access keys to the survey form. To mitigate this problem, the application should send single-use links exclusively to authorized users. Thus,

each link allows for the creation of only one public-private key pair. Hence, if an authorized user clicks the link and creates their keys, even if they share the link, the unauthorized user cannot create the key pair necessary to access the form.

3. Architectural Model and Workflow of the Proposed Solution

The architectural model proposed in this work takes the form of a web application based on the Model-View-Controller (MVC). The architecture comprises two major modules: an interface for user interaction with the application and an Application Programming Interface (API) responsible for all logic and database connectivity. Consequently, all business rules are contained within the back-end of the application, with the interface being responsible for presenting the visual and intuitive aspect of the solution.

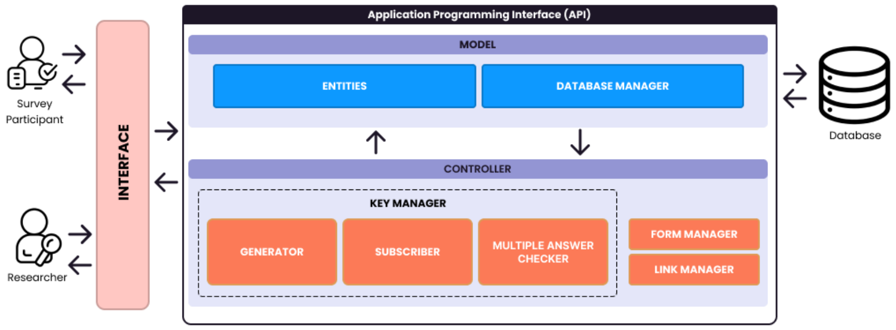

Figure 2. Architectural model of the proposed solution.

The `Interface` layer was decoupled by the complex business rules. In this context, this layer represents the front-end of the application, involving all visual and intuitive aspects of the system.This layer is responsible for making calls requesting data processing in the API and subsequently displaying the results to the user. This processing task is accomplished using HTTPS requests that are received by the `Controller` layer.

The `Controller` layer is accountable for directly handling user requests. This layer processes the received data and forwards it to subsequent layers, potentially either to the `Model` layer in the event of data alteration or to the `Interface` when there is a need for page visualization. Within the scope of this application, the `Controller` encompasses three primary components: **Form Manager**, **Link Manager**, and **Key Manager**. The **Form Manager** deals directly with survey form creation by the researcher. Once the researcher has formulated the survey questions, this component transmits the data to the model layer, which subsequently directs it to the database. Conversely, the **Link Manager** is responsible for disseminating links to participants. Upon the researcher's creation of the form, they can dispatch a single-use link to each participant for them to generate their key. Once all participants have their keys, the researcher can then furnish the form link to the participant. Consequently, all of these actions are directly associated with the **Link Controller** component. Lastly, the **Key Manager** holds three principal responsibilities: generating key pairs, signing form responses, and verifying if a participant has responded to the form more than once. Each of these processes leverages the concepts put forth by Liu and Wong (2005):

- The key generation process employs the algorithm $(x, y) \leftarrow Gen(1^k)$, where a security parameter k is provided, resulting in the generation of the private key x and the public key y;

- For the signature process, the algorithm $\sigma \leftarrow Sig(1^k, 1^n, x, L, m)$ is employed. This algorithm utilizes a security parameter k, the size of the participant group n, the private key x of the respondent, a list L containing the n public keys of the participants (including that of the respondent), and the survey responses m;
- For the verification of which group submitted the survey, the verifier employs the algorithm $1/0 \leftarrow Ver(1^k, 1^n, L, m, \sigma)$, taking as inputs the security parameter k, group size n, a list L of n public keys, message m, and the signature σ, returning 1 or 0 to accept or reject, respectively. This verification is mandated for any message m, any $(x, y) \leftarrow Gen(1^k)$, and any L that includes y.
- Following the submission of responses, checks are conducted to identify whether there are signatures issued by the same participant. For this, the boolean algorithm $1/0 \leftarrow Link(1^k, 1^n, L, m1, m2, \sigma 1, \sigma 2)$ is employed. This algorithm utilizes a security parameter k, the size of the participant group n, a list L of public keys, a pair of survey responses $m1, m2$, and a pair $\sigma 1, \sigma 2$ of signatures to verify if this pair of responses was signed by the same participant, returning 1 or 0.

Finally, the `Model` layer encompasses two primary components: the **Database Manager** and the **Entities**. The **Database Manager** is tasked with database operations, including data queries and modifications. For instance, retrieving public keys to be utilized by the **Key Controller** component in the signing of a survey, saving a participant's public key, and storing survey responses. Each of these operations constitutes a request originating from the `Controller` layer. The **Entities** component is responsible for encapsulating the abstraction of each element within the context our data. For example, a Form is an abstraction of an entity that contains questions and answers. Data validation rules are included within entity definitions. Moreover, the software development is already in progress, as evidenced by our GitHub repository[1]. We have structured our software design in line with our architectural model and have successfully completed the implementation of the Generator and Subscriber components from the **Key Manager**.

Given the understanding of our architectural model, we may advance to explain the general workflow of our proposed solution (as synthesized in Figure 3):

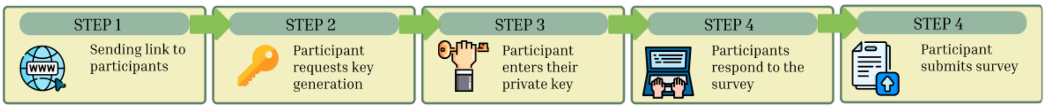
STEP 1
Sending link to participants
STEP 2
Participant requests key generation
STEP 3
Participant enters their private key
STEP 4
Participants respond to the survey
STEP 4
Participant submits survey

Figure 3. Workflow of the proposed solution.

In **Step 1**, the researcher, already knowing the participants who will be involved in the study, individually forwards the link to each of them. This link will lead to a page responsible for generating the participant's private and public keys. Subsequently, the participant will retain their private key, while their public key will be stored in a database. Following this procedure, the link will expire, thus allowing for single-user access only. This measure is adopted to prevent malicious participants from sharing the link with others, thereby enabling the creation of additional keys and, consequently, unauthorized participation. **Step 2** will occur at a later time when the participants are already in possession

[1] `https://github.com/Chagas823/lrs-survey`

of their private keys. In this context, the researcher sends the link containing the survey. In **Step 3**, the participant receives the survey link and inserts their private key. Finally, in **Step 4**, the participant completes the survey form and submits it signed by the Linkable Ring Signature scheme. Upon submission, the system verifies whether the participant has already responded to the survey. If not, the responses are then sent to the database.

4. Final Remarks, Contributions for IS, and Next Steps

This article presents a methodological design proposal and an architectural model to ensure anonymity and authenticity in survey research. To achieve this goal, our solution incorporates the concept of Linkable Ring Signature. Based on the proposed architecture and methodology, this solution demonstrates prominence across both industry and academia. Hence, this paper presents contributions from three fundamental dimensions relevant to both academia and the IS market. *Technologically*, we introduce a novel architectural model to survey research based on the Linkable Ring Signature scheme. In the context of *process*, we advocate for the development of solutions that facilitate anonymity and authenticity in surveys. Regarding *people* perspective, we delve into a relevant social discussion surrounding the expectations of trust inherent in survey participation. Regarding the limitations of our proposal, it is important to note that extensive participation in the survey using Linkable Ring Signatures may lead to slower computational processes. Our next step involves proceeding with the Development, Evaluation, and Conclusion stages established on the methodological protocol grounded in *Design Science Research*.

References

Boscarioli, C., de Araujo, R. M., Maciel, R. S., Neto, V. V. G., Oquendo, F., Nakagawa, E. Y., Berrnardini, F. C., Viterbo, J., Vianna, D., Martins, C. B., et al. (2017). I GranDSI-BR: Grand research challenges in information systems in Brazil 2016-2026.

Creswell, J. and Guetterman, T. (2018). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 6th Edition*.

Gaharana, S. and Anand, D. (2015). Dynamic id based remote user authentication in multi server environment using smart cards: A review. *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 1081–1084.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2008). Design science in information systems research. *Management Information Systems Quarterly*, 28(1):6.

Hohenberger, S., Myers, S., Pass, R., et al. (2014). Anonize: A large-scale anonymous survey system. In *2014 IEEE Symposium on Security and Privacy*, pages 375–389. IEEE.

Liu, J. K. and Wong, D. S. (2005). Linkable ring signatures: Security models and new schemes. In *Computational Science and Its Applications (ICCSA 2005)*, pages 614–623. Springer.

Mathiyazhagan, T. and Nandan, D. (2010). Survey research method. *Media Mimansa*, 4(1):34–45.

Pfitzmann, A. and Hansen, M. (2000). Anonymity, unobservability, and pseudonymity — a proposal for terminology. volume 2009, pages 1–9.

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to leak a secret. In *7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast*. Springer.

Vaishnavi, V. and Kuechler, W. (2004). Design science research in information systems. *Association for Information Systems. Available at http://desrist.org/design-research-in-information-systems*.