An Identity Privacy Preserving Incentivization Scheme for Participatory Sensing

Martin Connolly
Dept. of Information Systems
Cork Institute of Technology
Ireland
Email: martin.connolly@cit.ie

Ivana Dusparic, Mélanie Bouroche
School of Computer Science & Statistics
Trinity College Dublin
Ireland
Email:{ivana.dusparic, melanie.bouroche}@scss.tcd.ie

Abstract— **Participatory sensing is a paradigm through which mobile device users (or participants) collect and share data about their environments. The data captured by participants is typically submitted to an intermediary (the service provider) who will build a service based upon this data. For a participatory sensing system to attract the data submissions it requires, its users often need to be incentivized. Such an incentivization mechanism typically requires users to at least partially disclose their identity to be able to reward them. This, however, might deter privacy conscious users from participating. Therefore, an incentivization mechanism needs to support anonymous data submission and rewarding. In addition, inference attacks can illegitimately gain further information about participants through linking data submissions or tracing rewards. This paper presents Identity Privacy Preserving Incentivization (IPPI), a decentralized peer-to-peer exchange that preserves identity privacy by enabling anonymous and unlinkable data submission and anonymous and untraceable reward allocation. This is achieved through the modification and extension of the concept of decentralized trading for cryptocurrencies to make payments (i.e. rewards) sent to a recipient (i.e. the participant) untraceable. Furthermore, the use of the Diffie-Hellman Exchange Protocol is modified to enable participants to create their own untraceable reward currency in the form of tokens to which the service provider can then assign value. The preservation of identity privacy is demonstrated by way of proof. The performance of the approach is also evaluated.**

Keywords—participatory sensing, identity privacy, privacy preserving, incentive mechanism, incentivization

I. INTRODUCTION

Participatory sensing is a form of crowdsourcing whereby individuals and communities submit scalar and/or multimedia data from mobile devices such as personal smart phones. The submitted data can be GPS coordinates revealing location or trajectory, a sensed data measurement or multimedia content such as photos, sound clips or video. The wide range of data that can be captured by participatory sensing is reflected in the diversity of its applications including, among others, smart cities [1], air pollution exposure [2] and health [3].

Participatory sensing has wide applicability but has issues of concern in the areas of privacy and incentivization. Participants may inadvertently compromise their privacy when interacting with a participatory sensing application as readings may unintentionally reveal sensitive information pertaining to their identity such as who they are, where they are and what they are doing in terms of their behaviour and habits. The incentivization of participants is also required by participatory sensing services to attain the critical mass of valuable data that is needed to make applications meaningful and useful.

While privacy and incentivization are important areas of research in participatory sensing, they have potentially conflicting goals. Service providers of participatory sensing applications want to receive as much useful data as possible at as low a reward level as possible. To achieve this, they offer financial and other tangible incentives to gain a critical mass of participants. In contrast, while users may wish to participate in a participatory sensing community, they may not be willing to do so at the expense of their privacy if a negligible return is offered. The fundamental challenge, therefore, is to reward participants for data submissions without their revealing who they are when receiving and spending the reward. Moreover, any such reward mechanism will need to facilitate incentive compatibility to ensure that the service provider does not provide rewards for non-truthful data submissions.

The conflicting nature of incentivization and privacy thus leads to a number of challenges. An incentivization approach that requires user identity to assign rewards will not attract submissions from privacy conscious users. In addition, participant identity and behaviour can be traced both when the rewards are allocated by the service provider and when they are spent. The use of a pseudonym as an identifier does not address the concerns of such users as, through the linking of data submissions, they are still subject to inference attacks revealing their location, habits and behaviour. The quality and relevance of the service provider's dataset will thus not attain its potential if data is only submitted by a subset of the population.

Privacy and incentivization both have the potential to prevent a participatory sensing dataset from reaching critical mass on an ongoing basis and from achieving the level of data quality required to create meaningful and timely information for both the service provider and data consumers. The issues pertaining to privacy preservation and incentivization are the motivation for Identity Privacy Preserving Incentivization (IPPI), a scheme whose goal is to both incentivise participants and preserve their identity privacy.

IPPI provides a means of incentivization and reward allocation that preserves the identity of participants and prevents the illegitimate acquisition of further knowledge about participants without their consent. To achieve this, a

peer-to-peer decentralized exchange model has been developed. This exchange modifies the concept of a cryptocurrency **OrderBook** to enable participants to anonymously make data submissions in exchange for a reward from the service provider. Reward tokens and data submissions are published by participants on the OrderBook with service providers validating these data submissions. The use of the Diffie-Hellman Exchange Protocol is modified to ensure reward untraceability.

II. Related Work

This section considers relevant work in the state of the art. Section A discusses approaches that address privacy preserving incentivization for participatory sensing while Section B explores the media that can be used for reward allocation.

A. Privacy Preservation & Incentivization

There are a number of approaches in the current state of the art that consider both privacy and incentivization [4-8] with pseudonyms, trusted third parties and tokens being used to achieve identity privacy.

The SPPEAR (Security & Privacy-Preserving Architecture for Participatory-Sensing Applications) architecture uses both pseudonyms and trusted third parties to enable the privacy preserving provision of incentives for participants [4]. This architecture introduces a number of components including, among others, an Identity Manager for authentication management. Another pseudonym-based privacy protection scheme with incentives [5] also introduces a third party component, in this case a privacy management certification centre. A token-based method (referred to in this approach as a certificate) and symmetric key cryptography are used to achieve privacy preservation. While both approaches provide some degree of identity privacy, their use of pseudonyms does not address the potential for inference attacks as, while the user's identity is protected, their habitual behaviour, locations and trajectories can be traced using the pseudonym. Moreover, the introduction of third party components by these approaches are additional potential points of privacy vulnerability. For example, an intrusion into SPPEAR's Identity Manager would reveal all participant identities.

A token-based system without pseudonyms is also used in the state of the art to achieve incentivization and privacy goals [6]. In this case, the tokens are used to conduct communication between the subscriber (participant) and collector (service provider) with the authors envisaging that the outlined credit tokens will be converted into a financial reward. The process of obtaining a credit token is achieved by the participant using a Blind Signature Scheme. However, while this approach does not use pseudonyms, it is still vulnerable to similar types of inference attacks, specifically, a credit-based inference attack that is highlighted by the authors themselves.

In other approaches in the state of the art, the use of pseudonyms is avoided by using untraceable tokens but the issue of anonymous and untraceable reward allocation is not addressed [7]. In addition, a third party Cloud Provider component is introduced by this approach which leads to a potential privacy vulnerability. In contrast, EPPI [8] does use untraceable tokens to provide privacy preserving reward allocation. Under this approach, anonymous token exchange is achieved using the concept of an exchangeable and untraceable unit bearer currency for participatory sensing called E-Cent. What is termed a mix zone is used to enable participants to anonymously exchange E-Cents, thus ensuring that rewards are not tied to particular data submissions. While this use of untraceable E-Cents does not carry the disadvantages of pseudonyms, the mix zone does require the use of a pseudonym on the part of the participant and, if compromised, this service is itself a potential source of privacy violations. Moreover, the privacy evaluation experiments carried out by EPPI's authors indicate that the approach is, in certain circumstances, vulnerable to inference attacks.

To summarize, the approaches in the state of the art have shortcomings in their addressing of inference attacks and, in some cases, introduce components that could potentially serve as points of privacy vulnerability. To address these shortcomings, IPPI, the approach proposed in this paper, removes the need for the introduction of (potentially privacy compromising) trusted third party components through the use of a peer-to-peer decentralized exchange and avoids the use of pseudonyms by using the concept of a One-Time Key, a cryptographic key that is used only once, for reward allocation without the need to disclose identity privacy. While the concepts underpinning the peer-to-peer decentralized exchange platform model used for cryptocurrencies [9] serves as the inspiration for the model used for IPPI, the platform is modified and extended for participatory sensing, in particular, to address the challenge of making rewards untraceable.

B. Medium for Reward Allocation

The rewards allocated to participants in a participatory sensing system will typically have a tangible value and can be achieved by mapping either reward tokens or a cryptocurrency to an item of value such as public transport credits or WiFi access. To meet the needs of IPPI, the medium for allocating rewards must be unforgeable, only spendable once, mappable to a tangible reward of the service provider's choosing, consistent in its value and robust to inference attacks. Tangible rewards with a financial value are crucial in attracting participation in crowdsourcing systems such as participatory sensing [10] and have been found to be more effective than virtual rewards (such as the earning of points for participation) in incentivizing the contribution of meaningful data [11].

Cryptocurrencies, electronic forms of value exchange, are designed for online purchases, trading and transactions. They use cryptographic methods to protect the integrity of transactions and of the currency itself. However, while cryptocurrencies such as Bitcoin [12] were developed to protect the privacy of those engaging in transactions, its creators point out that the cryptocurrency offers pseudonymity not anonymity. Specifically, the address at which a payee receives Bitcoins acts as a pseudonym with every transaction involving that address being stored in the BlockChain. Thus, users of Bitcoin are vulnerable to inference attacks. While cryptocurrency 'mixer' services can be used to make Bitcoins impossible to trace by enabling users to swap Bitcoins with each other, this necessitates the trusting of what is often an anonymous third party service. The mapping of rewards to the value of a cryptocurrency is also problematic for service providers as the value of the latter can be volatile.

There are other alternatives to cryptocurrency schemes such as E-Cash schemes [13]. However, such schemes would necessitate the involvement of a third party (a bank) which could potentially be a source of privacy violation. For these reasons, therefore, rather than using an existing cryptocurrency or E-Cash scheme, IPPI uses reward tokens. To facilitate the anonymous submission of data in exchange for untraceable rewards, IPPI enables participants to produce their own untraceable reward tokens to which the service provider can assign value without violating the participant's identity privacy. Tokens are mappable to a tangible reward (monetary or non-monetary) and, as they are not vulnerable to external economic events, do not fluctuate in value.

III. IPPI

This section describes the IPPI platform. Section A describes the participatory sensing system and threat model addressed by IPPI. Section B outlines the decentralized exchange platform that underpins the approach while Section C explains how the rewards allocated to participants are made untraceable.

A. System & Threat Model

The two actors in the participatory sensing system model used in IPPI are the service provider and the participant. The goal of the former is to capture data for the purposes of, for example, publication for consumption by other users or for the building of a data set on which statistical analysis is conducted. The service provider initiates data collection campaigns by issuing offers indicating the type and scope of the sensed data being sought (e.g. air quality levels in a particular area of a city between 5pm and 7pm) and the corresponding reward that participants will receive for making data submissions matching the criteria outlined in the offer. Participants can then elect whether or not to respond to an offer. Once captured, data is submitted to the service provider in anticipation of a reward.

While there are many kinds of internal and external attacks that may be carried out in Participatory Sensing systems, the focus of IPPI is on preventing the service provider from potentially using the information it already has to carry out an inference attack to obtain further information which the participant does not wish to disclose. IPPI thus addresses the Semi-Honest Threat Model. In other words, it is assumed that the service provider follows the protocol correctly but will attempt to gain further information by analyzing message contents.

B. Decentralized Exchange Platform

Decentralized cryptocurrency exchanges such as CryptoNote are peer-to-peer networks in which all users share responsibility for payment processing and recording with no central authority or middlemen [9]. This concept of a decentralized exchange presents a number of attributes that facilitate IPPI in its privacy preserving approach. In particular, the peer-to-peer architecture facilitates anonymous and unlinkable data submissions without the need to hold any private data pertaining to participants. Moreover, this is achieved without the introduction of any potentially privacy compromising third party components. This absence of a central server also diminishes the potential for other external attacks such as Distributed Denial of Service (DDOS) as all nodes hosting the network would have to be targets. As IPPI's architecture necessitates the use of peers, these peers can be incentivized to host the service provider's data submission and reward information by receiving a payment or being granted access to the service provided.

While the basic network architecture remains the same, the other core concepts used for decentralized cryptocurrency exchanges are modified for the purposes of IPPI to ensure untraceable reward allocation. The OrderBook, which is used to record expressions of interest by both buyers and sellers of currency trades, is used by the service provider to publish requests for data submissions and allocate rewards, and by participants to make anonymous data submissions and receive untraceable rewards. Offers, which contain details of the data requested and the reward being offered, are published on the OrderBook by the service provider. All participants are aware of the existence of an offer when it is generated and can elect to respond to it by submitting data and a reward token. Rewards are allocated until the desired number of responses is achieved or the offer expires.

Figure 1 presents an overview of the IPPI platform.

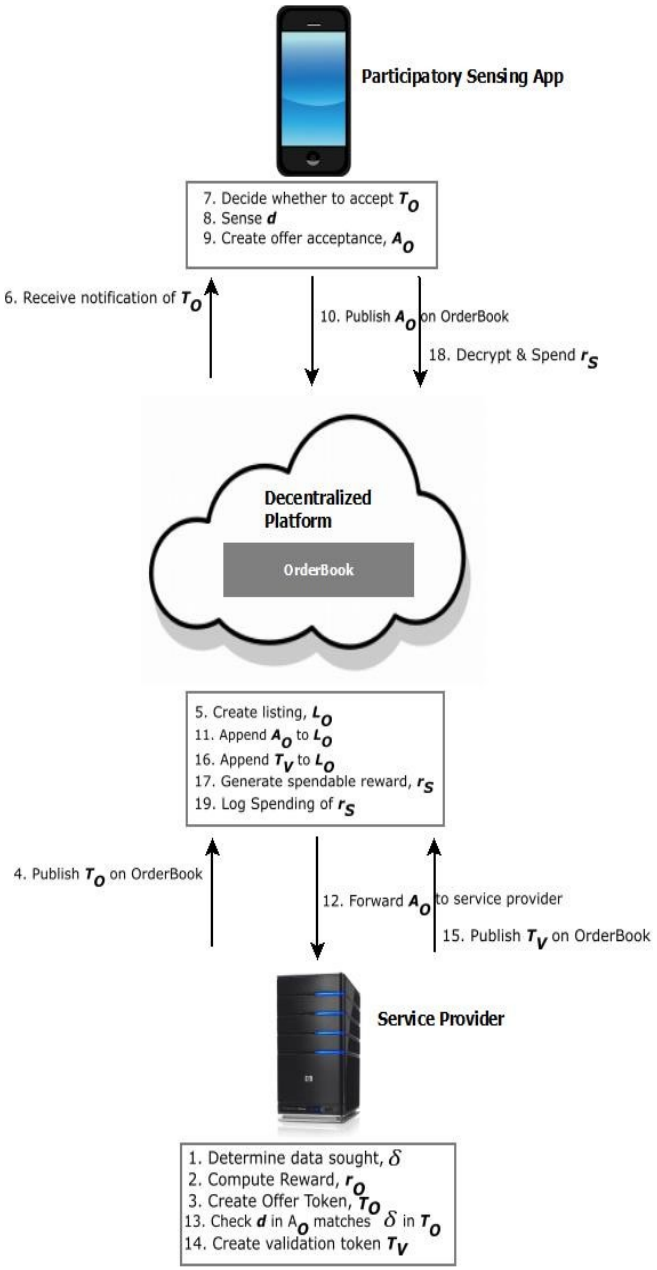

Figure 1: IPPI Decentralized Platform

C. Making Rewards Untraceable

The concept of the One-Time Key, which is used in cryptocurrency exchanges to ensure that multiple payments received by the same payee cannot be linked [9] is modified by IPPI to ensure that the service provider (the equivalent of the payer in a cryptocurrency exchange) does not have access to the participant's real or pseudonymous identity, thereby providing untraceable rewards to participants and preventing inference attacks.

IPPI modifies the use of the One-Time Key's underlying Diffie-Hellman Key Exchange Protocol [14] to create a One-Time Key to provide untraceable rewards. As originally envisaged, Diffie-Hellman Key Exchange enables two parties to establish a shared secret and use this secret to exchange cryptography keys for use in symmetric encryption algorithms such as AES. The Diffie-Hellman protocol is modified for IPPI to enable the participant to publish the public component of the One-Time Key on the OrderBook whilst retaining the private component.

The service provider makes participants aware of its offer by publishing an **offer token, $\boldsymbol{T_O}$** on the order book.

$$\boldsymbol{T_O} = \{\delta, r_O, i_{SP}, i_O\}$$

where $\boldsymbol{\delta}$ comprises the type and granularity of the **data** being sought as well as other conditions such as location, the number of data submissions sought and when the offer expires, $\boldsymbol{r_O}$ is the amount of the **reward** offered, $\boldsymbol{i_{SP}}$ is the ID of the service provider and $\boldsymbol{i_O}$ is the ID of the offer token. The offer token, T_O is published on the OrderBook as part of a **listing, $\boldsymbol{L_O}$,** to which participants' responses are appended.

A participant who accepts the offer token, T_O, then generates a **One-Time Key, $\boldsymbol{K_O}$** and an **offer acceptance**

$$\boldsymbol{A_O} = \{d, a_{K_O}, i_O, i_{A_O}\}$$

where $\boldsymbol{a_{K_O}}$[1] is the **public part** of the generated key K_O and $\boldsymbol{d}$ contains the participant's data submission. A_O also contains the ID of the corresponding offer token, i_O. $\boldsymbol{i_{A_O}}$ is A_O's **unique** ID and is assigned by the OrderBook on receipt of A_O. To ensure untraceability, the participant does not assign any ID to A_O.

A_O is appended to the offer listing, L_O, on the OrderBook and is then forwarded to the service provider who determines whether the data submission merits a reward. This could entail simply verifying that the data submission matches the criteria set out in the offer token, T_O, or could incorporate an incentive compatibility approach to evaluate the truthfulness of the data submitted. In either case, the service provider has no means of determining the identity of the data submitter.

Having evaluated the data, d, in A_O, the service provider generates a **validation token**

$$\boldsymbol{T_V} = \{i_V, i_{A_o}, v\}_{b^*_{SP}}$$

which includes T_V's unique ID, $\boldsymbol{i_V}$, the offer acceptance ID i_{A_o} and a **flag $\boldsymbol{v}$** which denotes whether the data submission merits a reward. The service provider signs T_V using its **private key**, $\boldsymbol{b^*_{SP}}$ and publishes it on the OrderBook. The OrderBook generates a **unique spendable reward ID $\boldsymbol{i_S}$**, and uses the public part of the One-Time Key, a_{K_O} to encrypt a spendable reward token

$$\boldsymbol{r_s} = \{i_S, i_V, r_O\}_{a_{K_O}}$$

which is comprised of i_S, the associated ID of the validation token, i_V and the reward value, r_O. It then appends the validation token T_V and the encrypted spendable reward $\boldsymbol{r_s}$ to the offer listing L_O on the order book.

When a participant wants to spend a reward, it retrieves the encrypted spendable reward $\boldsymbol{r_s}$ from the offer listing, L_O, decrypts it thanks to $\boldsymbol{a^*_{K_O}}$, the private part of the key K_O, and sends it to the OrderBook. The OrderBook checks the validity of the ID provided, i_S, checks that it has not been spent previously and then verifies the signature of the associated validation token, T_V, using the service provider's public key $\boldsymbol{b_{SP}}$, to ensure that the validation token was indeed generated by the service provider. It then permits spending of the reward and, to prevent the problem of double spending, logs it as spent.

While all participants can see that a data submission has been given a reward, only the participant who made the data submission can spend the reward allocated by decrypting the spendable reward, r_s, using the private part of the One-Time Key, $a^*_{K_O}$. Other participants are unable to forge this verification. Moreover, so as to ensure that the service provider cannot change its signature to track spendable rewards, the OrderBook holds an identity certificate signed

```
1   [Service Provider publishes an offer token T_O]
2    // OrderBook operation.
3   Append T_O to offer listing, L_O.
4   [On acceptance of T_O by a participant]
5   Capture d
6   // Generate One-Time Key's public and private parts,
7   Generate a_{K_O} and a*_{K_O} .
8   // Create offer acceptance, A_O.
9   A_O = {d , a_{K_O}, i_O, i_{A_O}}
10  // Participant retains One-Time Key as the private
11  // key, a*_{K_O}, is used to claim reward.
12  // [a_{K_O}, a*_{K_O}] denotes the set of One-Time Keys held.
13  [a_{K_O}, a*_{K_O}] += {a_{K_O}, a*_{K_O}}
14  Publish A_O on OrderBook
15  // OrderBook Operation.
16  L_O+= A_O // Append A_O to L_O
17  Forward A_O to Service Provider
18  // Service Provider Operation.
19  [On receipt of A_O]
20  v = Validate A_O
21  if v then
22     Log allocation of R_O  // allocate the reward
23     T_V = {i_V, i_{A_o}, v}_{b*_{SP}}
24     // Publish T_V on OrderBook by appending it to L_O.
25     L_O+= T_V
26    // OrderBook generates encrypted spendable reward.
27     r_s = {i_S, i_V , r_O }_{a_{K_O}}
28  end if
```

Algorithm 1: Allocating the Reward

[1] The symbols used correspond to those used in [16].

by a peer to confirm that the service provider is the owner of the public key, b_{SP}, used to verify rewards being spent.

Algorithm 1 presents the algorithm used to ensure that participants are allocated untraceable rewards in exchange for an anonymous data submission. The algorithm is initiated when a service provider publishes an offer token and a participant accepts this offer. Algorithm 2 presents the algorithm used when spending the reward. Both algorithms have been implemented and validated in a simulated

```
[Participant wants to spend the reward]
Decrypt r_S using a*_KO
[OrderBook operation]
// Verify that the associated validation token was
// signed by the service provider.
Verify signature of T_V (identified by i_V entry in r_s)
If verification passes then
   Check that i_S is not already recorded as spent
   if i_S is not recorded as spent then
      Permit spending
      Record i_S as spent
end if
```

Algorithm 2: Spending the Reward

participatory sensing environment using the C++ programming language with the Crypto++ library of cryptographic schemes [15] being used to implement the One-Time Key generation and validation and the digital signature scheme.

IV. Evaluation

The robustness of the privacy preservation provided by IPPI is evaluated by proof while its performance is evaluated through an implementation on the Android operating system. Theorems are presented to prove that, under IPPI, participants can make data submissions to the service provider anonymously and receive anonymous, unlinkable and untraceable rewards in exchange for these anonymous data submissions.

A. Privacy Analysis

Theorem 1 Participants make data submissions to the service provider anonymously.

Proof

To obtain the data it needs, the service provider publishes a series of offer tokens $[\boldsymbol{T_O}]$ on IPPI's decentralized OrderBook denoting the data being sought, δ, and the reward being offered, r_O. Each offer token, T_O, is published as a listing, L_O, to which the acceptances of the participants, $[A_O]$, are appended. The OrderBook is accessible to all participants and service providers. A participant can then choose to make a data submission, d, in return for the offered reward, r_O.

When issuing the offer token, T_O, the service provider has no direct communication with any of the participants. Similarly, a participant does not communicate directly with the service provider when publishing the offer acceptance, A_O, which contains the data submission, d. Instead, A_O is appended to the offer listing, L_O, and published on the OrderBook. The offer acceptance, A_O, and its constituent components, i_O, the ID of the offer being responded to, the data submission, d and the public part of the generated key, a_{K_O}, do not contain any link to the participant's identity or any anonymised ID or pseudonym that could be used to identify the participant. In addition, as the offer acceptance's unique ID, i_{A_o}, is only assigned on receipt of the acceptance by the OrderBook, it cannot be traced back to the participant.

The service provider is notified of the data submission when A_O is forwarded to it. While it can access and evaluate the data, d, contained therein, it has no means of linking the submission to the participant's identity. Therefore, the participant makes its data submission to the service provider anonymously without disclosure of identity. ■

Theorem 2 Participants receive anonymous rewards.

Proof

The public part of the One-Time Key, a_{K_O}, is published on the OrderBook as part of the offer acceptance, A_O. A participant's a_{K_O} cannot be traced back to the participant who generated the corresponding One-Time Key, K_O, as it has no relationship with the participant's identity.

The service provider publishes a flag v for A_O on the OrderBook as part of a validation token, T_V, indicating its decision with respect to whether A_O should be rewarded. i_{A_o}, the ID of the offer acceptance, is used to indicate who should be rewarded. Once T_V is published on the OrderBook, an encrypted spendable reward r_s is created for A_O. Only the owner of A_O, can access and consume r_s, as it is the only party that holds the private part of the One-Time Key, $a^*_{K_O}$. Thus, a participant can make a valid data submission and receive an anonymous reward without disclosure of identity. ■

Theorem 3 Participants receive unlinkable rewards.

Proof

A One-Time Key, K_O, is used only for one offer acceptance, A_O, so cannot be used to link a participant's set of offer acceptances, $[\boldsymbol{A_O}]$. In addition, the ID of the spendable reward, i_S, is neither linkable to the participant nor to the public part of the One-Time Key itself, a_{K_O}. Moreover, the service provider cannot connect r_s and its ID, i_S, to a participant or to a_{K_O}. This is because r_s is only decrypted when it is being spent. Therefore, neither a_{K_O} nor the r_s encrypted using a_{K_O} can be used to establish linkages between the data submissions of a particular participant.

The absence of any linkable ID in a participant's set of offer acceptances, $[A_O]$, set of public One-Time Key components, $[\boldsymbol{a_{K_O}}]$ or set of spendable rewards, $[\boldsymbol{r_s}]$ therefore means that the service provider has no means of inferring any data about that participant's behavior and activity. ■

Theorem 4 Participants receive untraceable rewards.

Proof

The service provider has no role in the publishing of the offer acceptance, A_O, or the allocation of the reward offered, r_O. Specifically, the fact that the service provider cannot assign traceable IDs to A_O means it cannot trace participant activity on the participatory sensing system through the assignment of r_O.

A_O has no fixed ID. While the OrderBook assigns a unique ID, i_{A_O}, on receipt of A_O, this ID cannot be used to trace the participant. In addition, as the One-Time Key, K_O, is only used once and then discarded, the service provider has no means of linking participant activity through the publication of the latter's offer acceptances, $[A_O]$. Moreover, the spendable reward, r_s cannot be connected to A_O as it is only decrypted when it is being spent. Therefore, a participant's set of spendable rewards, $[r_S]$, is untraceable. ■

B. Performance Evaluation

	Time (ms)	Power (J)
Submitter (Android Phone)	4	0.023
Peer (Laptop)		
- Verification	0.944	N/A
- Decryption	0.005	N/A
Total (Laptop)	4.949	0.023
Total (Li & Cao [6])	6.004	0.29

Table I: Resource Consumption of Cryptographic Primitives

In addition to implementing the algorithms using C++, IPPI has also been implemented for the Android mobile operating system using the Java programming language with the cryptographic primitives being implemented using the SpongyCastle API [16]. The DSA algorithm using the SHA-1 message digest algorithm is used to specify the digital signature. The peer's verification and decryption primitives are also implemented for the Windows 10 operating system using the Java Programming language and the BouncyCastle API [17]. The latter implementation is carried out as a peer may elect to support the Orderbook on fixed nodes such as a Laptop or PC Server rather than a mobile device. Energy consumption is not measured for this latter implementation as it tends not to be a critical concern for such devices.

Using these implementations, the running time and power consumption of the cryptographic primitives for the submitter and a typical peer are measured on a Samsung Galaxy S7 Edge Android Smartphone and, in the case of the peer, on an 8GB Lenovo T450s ThinkPad Laptop computer. The results of these experiments are presented in Table I.

The running time of the cryptographic primitives for IPPI is evaluated by executing the associated algorithm over 100 times and computing the average time taken. The time taken in the generation of the One Time Key for the submitter is 4ms on average while the time taken for peer verification (when the user wants to spend the reward) and ID decryption operations is under 1ms. This compares favorably to Li and Cao's token-based approach [6] which, on average, takes 21.3% longer.

IPPI's SmartPhone power consumption is 92% lower than Li and Cao's approach. Crucially, it should be noted that the resource consumption totals of 6.004ms and 0.29J for the token-based method pertain solely to the data submitter. In these terms, the resource consumption of 4ms and 0.023J is much less for the data submitter under IPPI as the majority of the cost is borne by the peer.

V. Conclusion

This paper proposes IPPI, a method of allocating untraceable rewards to participants in participatory sensing systems. IPPI is a decentralized exchange platform that enables participants to be rewarded for data submissions without their privacy being compromised while also enabling service providers to capture the data they need to provide an effective service. The approach addresses the fundamental challenge of giving participants untraceable rewards in exchange for anonymous data submissions. Further challenges to be addressed include how to avoid incentivizing untruthful submissions and the need to adapt the level of incentivization proportionally to the data's worth, which might change over time depending on the state of the environment and the current willingness of participants to contribute.

References

[1] R. Szabo, K..Farkas, M. Ispany, A. A. Bencur, N. Batfai, P. Jeszenszky, S. Laki, A. Vagner, L. Kollar, Cs. Sidlo, R. Besenczi, M. Smajda, G. Kover, T. Szincsak, T. Kadek, M. Kosa, A. Adamo, I Lendak, B. Wiandt, T. Tomas, A. Zs. Nagy, and G. Feher, "Framework for Smart City Applications Based on Participatory Sensing", IEEE 4th International Conference on Cognitive Infocommunications (CogInfoCom), 2-5 December 2013, pp. 295-300.

[2] B. Predic, Y. Zhixian, J. Eberle, D. Stojanovic and K. Aberer, "ExposureSense: Integrating daily activities with air quality using mobile participatory sensing", IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 18-22 March 2013, pp. 303-305

[3] A. Clarke and R. Steele, "Targeted and Anonymized Smartphone-based Public Health Interventions in a Participatory Sensing System", 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 26-30 August, pp. 3678-3682

[4] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security & Privacy-Preserving Architecture for Participatory-Sensing Applications", Proceedings of the 2014 ACM conference on Security and Privacy in Wireless & Mobile Networks (WiSec '14), pp. 39-50

[5] J. Zhang, J. Ma, W. Wang and Y. Liu, "A Novel Privacy Protection Scheme for Participatory Sensing With Incentives", IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS), 30 October-1 November 2012, pp. 1017 – 1021

[6] Q. Li and G. Cao, "Providing privacy-aware incentives in mobile sensing systems", IEEE Transactions on Mobile Computing, 2016, Vol. 15, No. 6, pp. 1485-1498

[7] I. Krontiris, and T. Dimitriou, "A Platform for Privacy Protection of Data Requesters and Data Providers in Mobile Sensing", Journal of Computer Communications, 2015

[8] X. Niu, M. Li, Q. Chen, Q. Cao and H. Wang, "EPPI: An E-cent-based Privacy-preserving Incentive Mechanism for Participatory Sensing Systems", IEEE International Performance Computing and Communications Conference (IPCCC), 5-7 December 2014, pp. 1-8

[9] Cryptonote, https://cryptonote.org

[10] M.C. Yuen, I. King and K.S. Leung, "A survey of crowdsourcing systems", Privacy, Security, Risk and Trust (PASSAT) and IEEE Third Inernational Conference on Social Computing (SocialCom), October 2011, pp. 766-773, IEEE

[11] R. Gafni, N. Geri and P. Bengov, "Investigating the effect of tangible and virtual rewards on knowledge contribution in online communities", Online Journal of Applied Knowledge Management, 2014, Vol. 2, No. 2, pp.1-11

[12] S. Nakamoto, 2008, "Bitcoin: A peer-to-peer electronic cash system."

[13] J. Camenisch, S. Hohenberger and A. Lysyanskaya, "Compact E-Cash", Eurocrypt, May 2005, Vol. 3494, pp. 302-321

[14] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, 1976, Vol. 22, No. 6., pp 644-654

[15] Crypto++ Library, http://cryptopp.com

[16] Spongycastle, https://rtyley.github.io/spongycastle/

[17] BouncyCastle, https://www.bouncycastle.org/