A privacy-friendly gaming framework in smart electricity and water grids

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 15, 2017, accepted July 4, 2017, date of publication July 17, 2017, date of current version August 8, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2727552

A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids

CRISTINA ROTTONDI[1] AND GIACOMO VERTICALE[2]

[1]Dalle Molle Institute for Artificial Intelligence, University of Lugano–University of Applied Science and Arts of Southern Switzerland, 6928 Manno, Switzerland
[2]Department of Electronics, Information, and Bioengineering, Politecnico di Milano, 20133 Milan, Italy

Corresponding author: Giacomo Verticale (giacomo.verticale@polimi.it)

The work of C. Rottondi was supported by the enCOMPASS–Collaborative Recommendations and Adaptive Control for Personalised Energy Saving Project through the EU H2020 Programme under Grant 723059.

ABSTRACT Serious games can be used to push consumers of common-pool resources toward socially responsible consumption patterns. However, gamified interactions can result in privacy leaks and potential misuses of player-provided data. In the Smart Grid ecosystem, a smart metering framework providing some basic cryptographic primitives can enable the implementation of serious games in a privacy-friendly manner. This paper presents a smart metering architecture in which the users have access to their own high-frequency data and can use them as the input data to a multi-party secure protocol. Authenticity and correctness of the data are guaranteed by the usage of a public blockchain. The framework enables a gaming platform to administer a set of team game activities aimed at promoting a more sustainable usage of energy and water. We discuss and assess the performance of a protocol based on Shamir secret sharing scheme, which enables the members of the teams to calculate their overall consumption and to compare it with those of other teams without disclosing individual energy usage data. Additionally, the protocol impedes that the game platform learns the meter readings of the players (either individual or aggregated) and their challenge objectives.

INDEX TERMS Smart grids, gamification, serious games, privacy, water conservation, energy conservation.

I. INTRODUCTION

Game-based approaches aimed at stimulating, increasing, or modifying users' activities have recently attracted increasing interest. Such approaches can be categorized as serious games or gamified interactions. The former class includes games meant for a purpose different than pure entertainment [1]. It therefore denotes the case of game experiences aimed at stimulating and engaging the user. Serious games have been successfully included in educational and teaching activities [2] and for health care scopes such as rehabilitation [3], or to raise awareness about critical issues in resource and demand side management [4]–[6]. A subcategory of serious games, the so called persuasive games [7], are specifically designed with the scope of changing people's attitudes and behaviors in a desirable direction (e.g. towards a more sustainable lifestyle, or to increase votes for a political party). Such games include e.g. advertising games, health-related games and social/political advocacy games.

Differently, gamified interactions incorporate "the use of game design elements in non-game contexts" [8]. Like persuasive games, they typically have a persuasive goal, e.g. encouraging a more sustainable usage of water [9] or energy [10] resources, or stimulating drivers to adopt specific expedients to avoid queues of traffic [11].

The empirical evidence of the effectiveness of these game-based approaches has been demonstrated in several studies [12]–[15], which have highlighted that one of the main reasons for their successfulness is the tendency of people towards positive imitation. As a representative case study, the authors of [16] consider the occupants of a block of flats and show that exposing users to the comparison of their individual energy consumption to that of their neighbors impacts positively on their attitude towards energy conservation. Similarly, in smart power grids, utilities may incorporate gamification as a building block of more complex behavioral demand response approaches to perform peak shaving.

Regrettably, online gaming raises numerous privacy concerns about the possibly improper usage of data gathered from the players. The authors of [17] and [18] show how information on physical, mental and social characteristics of the players can be inferred based on collected logs about performed game actions and choices. Reference [19] discusses ethical, trust and privacy issues emerging in the framework of a serious game aimed at reducing traffic jams in Luxembourg.

The relevance of such issues is even more pronounced when gaming data are combined with data related to electricity, water or gas consumption, from which sensitive information about users' habits and lifestyles can be inferred [20], [21].

To overcome the above mentioned privacy concerns, we propose a cryptographic framework for an online gaming portal operated by a third-party entity. The envisioned application scenario is a smart electricity or water grid where the utility adopts a gamified mechanism to influence the consumption patterns of the users in order to indirectly shape their aggregate load (e.g. for peak shaving or load flattening scopes). In our preliminary work [22], we described a privacy-friendly gaming framework where players are grouped in teams and are challenged to maintain the team-aggregated consumption below a threshold defined by the utility. Here, we extend the framework to enable team competitions with the aim of achieving the lowest aggregate consumption. The framework includes:

- a suite of privacy-friendly protocols relying on Shamir Secret Sharing (SSS) scheme, which enable the members of a team to compute their overall resource consumption without communicating individual meter readings, and to compare it to those of other teams without learning the exact consumption amounts;
- a verification protocol relying on Pedersen Commitments, which can be run by the utility to detect whether users have reported false or altered results to the game platform;
- a secure, persistent storage of authenticated commitments based on the blockchain technology.

The remainder of the paper is organized as follows: Section II and III briefly overview the related work and some cryptographic background notions. Section IV introduces the privacy-friendly gaming framework and details the proposed cryptographic protocols. Sections VI and VII respectively evaluate the security and assess the performance of our framework. The final Section concludes the paper.

II. RELATED WORK

A. SERIOUS GAMES FOR ENERGY AND WATER MANAGEMENT

Several serious games have recently been designed to address smart water and electricity grid ecosystems [5], [6], [9], [10], [23]. Reference *et al.* [5] illustrates a game platform for smart grid demand side management. The game aims at regulating the aggregate energy consumption of the community of players, who are let free to self-organize as long as they respect a given set of social rules. It implements both individual and group challenges, which reward the players that manage to achieve predefined objectives. The authors point out the presence of potential privacy leaks due to the collection of energy meter readings of the users, but no countermeasures to alleviate such issue are discussed. Similarly, Gustafsson *et al.* [10] adopt a challenge-based approach in the design of game aimed at reducing energy consumption in households: users are grouped in teams and compete to achieve the lowest team-aggregated electricity usage. A virtual ''community garden'' is proposed by the gameplay described by Rizzoli *et al.* [9]: each user is responsible of a patch of the garden and his/her water consumption (measured by the water meter installed at the user's premises) determines how much water the patch receives: the more water is wasted in the household, the less is given to plants. The players can interact and exchange tips on how to reduce their water usage. Users with the most fluorishing patches are awarded.

Galli *et al.* [23] propose a more evolved water conservation framework based on a gamified web portal: through such portal, the water utility exposes to the users their individual water consumption in real time. Moreover, a system of rewards combining points and badges is adopted to acknowledge water-saving behaviors, learning actions (e.g. watching educational videos offered by the portal), and data provision actions (e.g. providing detail on the individual consumption patterns of water consuming appliances, which can be further processed by the utility for load forecasting purposes). An enhanced version of such framework, this time aimed at energy conservation, is proposed by Fraternali *et al.* [24]. The framework integrates two different gamification elements, i.e. gamified rewards such as points, badges, achievements and redeemable prizes and a serious game, combining a physical board-game with a digital app. The employed game mechanics are goal setting (e.g. personal saving goals are rewarded with bonus points and supermarket vouchers), social comparison and social collaboration (e.g. collecting points in teams for performing energy saving actions, competing with others).

The framework proposed in this paper incorporates similar types of challenges (i.e. multiplayer competitions versus an unmanned challenger or adversary players) and could be easily incorporated in the two above mentioned frameworks. However, our proposed solution leverages a privacy-friendly protocol that allows for the computation of aggregated consumption values without disclosing metering data at single-household granularity, under the assumption that users are augmented honest-but-curious adversaries, (i.e. they adhere to the protocol rules but try to infer additional information from the exchanged data and may provide bogus inputs). Therefore, the protocol provides a verification mechanism aimed at detecting cheating users. To the best of our knowledge, this is the first attempt to include privacy-preserving mechanisms in a third-party serious game service.

B. PRIVACY-PRESERVING DATA COLLECTION IN SMART GRIDS

A closely related research field is privacy-preserving data collection in smart grids. Several aggregation schemes for meter readings have been recently proposed (a comprehensive survey can be found in [25]–[27]), mostly relying on multiparty computation mechanisms (which allow for the collaborative computation of an aggregation function without disclosing the individual inputs of the participants) by virtue of the homomorphic properties of cryptographic schemes such as

the Shamir Secret Sharing scheme [28] (adopted e.g. in [29]) and the Pallier cryptosystem [30] (adopted e.g. in [31]–[33]). In this paper, we use the former scheme. However, differently from [29] and [31], where the share aggregation procedure was respectively executed by a set of intermediate entities called "privacy-preserving nodes" or by the communication gateways of the local residential area and the result of the aggregation was communicated only to the Utility, in this paper the aggregation procedure is collaboratively performed by the users belonging to the same team and the resulting team-aggregated consumption is learned by all the team members. The Utility is in charge of properly choosing the team size, ensuring that it is sufficiently large to protect the privacy of the participants. Similarly to [33], we consider an augmented honest-but-curious player adversarial model, where users may provide altered metering data as input to the game protocol with the aim of winning the game. However, differently from [33], we assume that the players do not deviate from the protocol rules. Moreover, we do not address the issue of faulty/malfunctioning meters, as done in [32].

A few set of operations including comparison, event correlation and entropy computation are known to be implementable with homomorphic schemes [34]. In particular, comparisons protocols have been applied to encrypted consumption measurements in privacy-friendly load scheduling frameworks aimed at defining the time of use of deferrable appliances [35] or the recharge periods of electric vehicles [36]. In our proposed infrastructure, we leverage on similar protocols to enable groups of players to compare their respective aggregate consumptions without learning the exact values achieved by the adversaries.

C. THE BLOCKCHAIN TECHNOLOGY

The blockchain technology has attracted a lot of interest as a potential solution to security issues arising in large environments of non-trusting devices communicating peer-to-peer with limited or no management. A survey of the efforts is available in [37]. Andrychowicz *et al.* [38] discuss a set of distributed protocols over the bitcoin network, including commitments. Our paper leverages a network similar to the bitcoin one for storing the commitments, but does not necessarily deliver bitcoins as prizes. Kosba *et al.* [39] define a blockchain security model that makes it possible to formally prove security of privacy-friendly protocols. In this paper, we use a similar model for describing the security properties of the blockchain.

III. BACKGROUND

A. SHAMIR SECRET SHARING

Threshold schemes are cryptographic protocols that enable the cooperative reconstruction of a secret that was previously shared among multiple parties. In a (w, t)-threshold scheme, the secret is split in w parts (the so-called *shares*), which are given to the participants and can be recovered if at least $t \leq w$ of them collaborate.

The Shamir Secret Sharing (SSS) scheme is a threshold scheme that works as follows. The dealer chooses a prime number Q greater than w and than all the possible secrets ν, uniformly chooses $t-1$ integer coefficients $\rho_1, \rho_2, \cdots, \rho_{t-1}$ in the range $[0, Q-1]$ and computes the s-th share (with s ranging from 1 to w) as the pair (x_s, y_s), where x_s are distinct integer numbers and $y_s = \nu + \rho_1 x_s + \rho_2 x_s^2 + \ldots + \rho_{t-1} x_s^{t-1} \bmod Q$. If t or more shares are made available by the respective holders, the secret can be reconstructed by means of the Lagrange interpolation method. SSS is a *perfectly secure* scheme [40], i.e. for every secret $\nu \in Z_Q$ and any subset of shares $\mathcal{S}$: $|\mathcal{S}| < t$ it holds that:

$$P(M = \nu | \mathcal{S}) = P(M = \nu)$$

where the random variable M indicates the secret chosen by the dealer.

SSS has homomorphic properties: the share of the sum of two secrets can be locally obtained by each participant by summing the corresponding shares of the two addends. Conversely, the multiplication of two secrets requires a collaborative procedure among the share holders, such as the one described in [41]. Comparison of two secrets can be implemented following the procedure described in [42], which enables each party to obtain a share of one bit indicating the comparison result. Both these protocols are secure if the Adversary can corrupt at most $t-1$ parties.

B. PEDERSEN COMMITMENT SCHEME

A commitment scheme is a two-party cryptographic protocol in which one of the two entities chooses a secret input and provides to the counterpart a message, called commitment, which will be used upon disclosure of the secret itself to verify that it was not changed after the generation of the commitment.

Pedersen Commitment Scheme (PCS) [43] works as follows. Let $\mathcal{G}$ be a group of prime order in which the Discrete Logarithm Problem (DLP) is hard. Let h_1 and h_2 be two distinct random generators of $\mathcal{G}$. The dealer chooses an input x and a random number r, then sends $c = h_1^x h_2^r$ to the counterpart. Later, the dealer reveals the pair (x, r) and the counterpart verifies the commitment.

PCS is *computationally binding*, meaning that the dealer must solve a DLP to find a pair $(x', r') \neq (x, r)$ that yields the same commitment. The scheme is also *unconditionally hiding*, meaning that for any pair (x, c) there is exactly one r that maps x into c. Thus, the counterpart learns no information from c about x. In addition, the scheme is homomorphic: given two input pairs, (x, r) and (x', r') such that c is a valid commitment for (x, r) and c' is a valid commitment for (x', r'), then cc' is a valid commitment for $(x + x', r + r')$.

Note that one way of guaranteeing that h_1 and h_2 are generated randomly is using algorithm `PickGroup` in [44]. With this algorithm, the seed of the Cryptographically Secure Pseudorandom Generator serves as a proof that the algorithm was honestly executed.

C. THE BLOCKCHAIN

A blockchain is a log of small messages batched into timestamped blocks, replicated over all the nodes of a network. All the nodes of the network have a public/private keypair for signing messages and are identified by a pseudonym, which may be the public key itself. Each messages is signed by the sender and broadcast to the neighboring nodes. Invalid messages are dropped so that only authenticated messages reach the majority of the nodes.

Periodically, a mining node packages the new messages and includes them in a timestamped block. Such block is then broadcast back to the network. All the messages in a block become persistent and non-repudiable. Which node is responsible for creating a block depends on the kind of network. In our proposed system, we assume either a private cloud, in which the mining nodes accept messages by subscribing nodes, or a pay-per-message scheme in which the messages carry with them a fee that is collected by the mining node.

IV. THE PRIVACY-FRIENDLY GAMIFICATION FRAMEWORK

A. SYSTEM MODEL

As depicted in Figure 1, the gamification framework includes the following entities.

The *Utility* is an entity that manages a public service such as water or electricity supply. It keeps a list of subscribers. It can access the blockchain and has a public pseudonym U.

The *Players* are utility subscribers that use a public service and are equipped with Smart Meters installed at their premises, which convey consumption data to the utility. We will refer to the players as $p_1, \ldots, p_N$, where N is the number of players and will also use p_i as a unique identifier for the ith player.

The *Game Platform* is a third party gaming service that interacts with the players and keeps track of the winning teams.

The *Smart Meter* (SM) is a tamperproof device that measures water (or energy) consumption with a given frequency. We assume that it has (at least) two output channels. The first one is used by the metering company to collect measurements. The second one is used by the meter to send real-time measurements to the customer. This second channel is also used to write information to the blockchain.

The blockchain model we adopt is a simplification of the Hawk model [39], with added considerations regarding the relation between rounds and timestamps. More specifically, we make the following assumptions:

- The blockchain implements a discrete clock that increments in rounds.
- The node that mines a block assigns the new round a timestamp with its local clock. The network makes no effort to guarantee clock syncronization, but we assume that the clock offset w.r.t. the wallclock time is small w.r.t. the round duration.
- Messages sent to the blockchain are public.

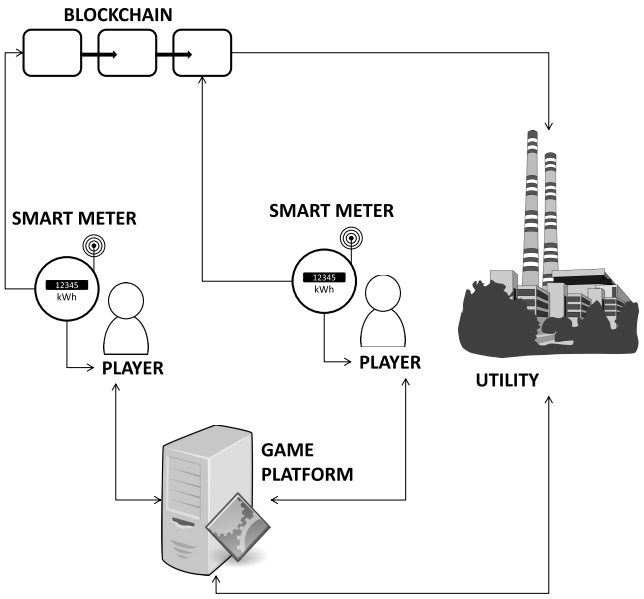

FIGURE 1. The proposed gamification framework.

- Messages received by the blockchain are delivered to all the nodes at the beginning of the following round. An adversary can reorder messages within the same round.
- The blockchain guarantees message integrity and data origin authentication w.r.t. a specific pseudonym.
- The blockchain assigns to each received message a unique identifier.
- Users can make up any feasible number of pseudonyms.

Let A be a pseudonym, d be a general string of data, t be the current timestamp as seen by A. The model relies on the following primitive:

$$\texttt{message}(A, t, d)$$

which stores in the blockchain a public message d from A. If the sender wants to specify a destination node, it can do so by including it in the message itself. The `message` primitive involves no transfer of money and is suitable for a private blockchain, but it can be easily extended to include a storage fee to be collected by the mining nodes.

The message and its timestamp are stored in a block if they are signed by A and the timestamp t is greater than the previous block timestamp and the timestamp of the currently mined node. It is easy to extend this with a tolerance to cope with propagation delays.

In our framework we assume that the SM of player p_i is identified by the blockchain pseudonym, A_i , which the utility can match to a physical device and to a subscription. At the end of each measurement interval t, the meter performs the following operations:

1) collect the measurement x
2) generate a random number r
3) calculate a Pedersen commitment as $c(t) = h_1^x h_2^r$

4) give x and r to the customer
5) perform a store operation to the blockchain:

$$\texttt{message}(A_i, t, c)$$

B. GENERAL DESCRIPTION AND GAME RULES

Players can take part to two different types of games: *team challenges* or *team competitions*. Challenges involve groups of users and consist in keeping the team-aggregated consumption below a given threshold T provided by the Utility. Alternatively, in team competitions multiple teams compete to achieve the lowest aggregated consumption.

In both cases, players are allowed to select the time period of the game among a predefined set of options, ranging from very short (hours) to very long intervals (weeks). After the expiration of the time period B, the Gaming Platform computes the challenge/competition results based on the team-aggregated consumption of the players and awards any prizes.

More in detail, the games proceed according to the following procedure.

1) When a player p_i wants to take part in a new game, it sends a message to the gaming platform G. For the sake of easiness, we consider a gaming platform providing a single game type and a single game duration B, which is long enough to include multiple reporting periods of the meter and multiple blockchain rounds. The extension to multiple concurrent game types and game durations is straightforward.
2) Periodically, G communicates the list of enrolled players to the Utility, U, which groups them in a set of teams and communicates to G the lists of teams and team members, the game start time, t_0, and, for each team,
   - in case of a challenge game, the corresponding threshold to beat;
   - in case of a competition game, the list of players in the adversary team.
3) Once the game starts, the team members calculate their aggregate consumption at regular time intervals. To this aim, all the players compute their individual time-aggregated consumption from the beginning of the game and communicate them to the other team members. Then, the players may decide to modify their future consumption patterns. In case of team competitions, the two competing teams are also allowed to compare their respective team-aggregated consumption.
4) At the end of the game period, all the players of the winning team claim their prize from the gaming platform and provide cryptographic evidence of their victory. Specifically, they provide the aggregate consumption in a way that the utility can use to verify that it is consistent with the commitments stored by the meters in the blockchain.
5) If a cheat is detected, the game platform voids the game; otherwise the gaming platform:
   - declares a winner for the *challenge game* if and only if the team-aggregated consumption is below the threshold T;
   - declares the team with the lower consumption as the winning team for each *competition game*.

   The platform can also record data related to the players' accesses and game activities and elaborate statistics on their performance.

Note that the design of our protocol is agnostic w.r.t. the awarding mechanism (awards may be either monetary or simply representative).

C. TRUST MODEL AND ASSUMPTIONS

Our privacy-friendly gaming framework builds upon the hereby listed assumptions:

1) Communications between the entities taking part to the protocol are authenticated and confidential.
2) The Utility is honest-but-curious: it never deviates from the protocol routine, but tries to obtain the value of individual electricity consumption measurements having finer temporal resolution than the typical billing period (e.g. one month) with the scope of deducing private details from the players' energy consumption patterns.
3) The game platform is also honest-but-curious: it behaves according to the same adversary model of the Utility with analogous goals.
4) The players are augmented honest-but-curious entities, i.e. they obey to the protocol rules but can choose to provide arbitrary inputs (e.g. they may declare lower consumption measurements than the actual ones).
5) Multiple players may form collusions with the aim of learning information about the energy usage of other players or to dishonestly win the game by providing false measurements. The cardinality of a set of colluded users cannot exceed the team size minus 1.
6) The Smart Meters are trusted, tamper-proof devices.
7) The blockchain is considered as a third party that is trusted for correctness and availability, but not for privacy.

D. SECURITY PROPERTIES AND GOALS OF THE PROTOCOL

We express the security properties in terms of Adversary goals. The protocol is secure if the achievement of such goals with non-negligible probability implies the capability of extracting information from an unconditionally secure encryption scheme or of solving a computationally hard problem.

P1 G learns any information about the threshold T, the aggregate consumption, or the consumption of any individual player.
P2 U learns any information on the individual consumption of any player during the execution of the game other than what is implied by the knowledge of the aggregate consumption of each team.

P3 Any collusion of the members of a team provide different measurements than the ones measured by their meter and G considers the outcome of the game as correct.

P4 Any collusion of a subset of members of a team learns any information about the individual consumption of any non-colluded team member.

P5 Any collusion of members of a competing team learns any information about the team-aggregate measurements of the other team in addition to whether it is larger or smaller than their own team-aggregated consumption.

In the next Section, we provide the details of the privacy-friendly protocol governing the interactions between players, game platform and utility.

V. THE PRIVACY-FRIENDLY GAME PROTOCOL

A. THE TEAM CHALLENGE PROTOCOL

We now describe the protocol with reference to the challenge game, in which a single team plays against a threshold.

When initializing the system, the gaming platform chooses and publishes the following parameters:

- The modulus Q_1, for the secret sharing of the consumption measurements and the modulus Q_2, for the secret sharing of the random number used to hide the measurement in the commitment. We use two different moduli because the measurements are much smaller than the random numbers. Since the number of messages in the share comparison protocol is heavily dependent on size of the secret, it is important to keep the share size small.
- A prime number q_1 such that the Decisional Diffie-Hellmann (DDH) problem is hard in $\mathbb{Z}_{q_1}$ and a random primitive root g of $\mathbb{Z}_{q_1}$.
- A subgroup of $\mathbb{Z}_{q_1}$ with order q_2 in which the Discrete Logarithm Problem (DLP) is hard and two distinct random elements of the subgroup, h_1 and h_2.
- A Key Generating Function, (KGF), and a semantically secure symmetric encryption scheme, Enc.

Our proposed privacy-preserving game protocol is divided in the following phases.

Game Setup: During the initial game setup the following protocol is executed.

1. Game Selection

Each player i generates a private session key a_i and enrolls with the gaming platform

$$p_i \rightarrow G\colon p_i, g^{a_i}$$

2. Player List

At regular intervals (e.g. once a day), G forwards to U a list of the N enrolled players and their public key.

$$G \rightarrow U\colon\ (p_1, g^{a_1}) \dots\ (p_N, g^{a_N})$$

3. Team List

The utility generates a private session key a_U and calculates the session key with each player $K_{iU} = \mathrm{KGF}((g^{a_i})^{a_U})$.

The utility forms the teams. Let $\mathcal{L}_j$ be the list of the players that are in team j and T_j be the threshold for team j. For each team j,

$$U \rightarrow G\colon g^{a_U}, \mathcal{L}_j, [\mathrm{Enc}(K_{iU}, p_i, T_j) \quad \forall\, i \in \mathcal{L}_j]$$

4. Game Goals

The gaming platform learns the team composition and forwards to each player the utility public key and the encrypted challenge threshold, which remains hidden to the game platform. For each team j and each player $i \in \mathcal{L}_j$,

$$G \rightarrow p_i\colon g^{a_U}, \mathcal{L}_j, \mathrm{Enc}(K_{iU}, p_i, T_j)$$

Computation of the time-aggregate consumption: At the end of each metering interval, each player calculates the time-aggregated consumption and divides it in a number of shares equal to the team size using the SSS scheme with threshold equal to the team size. Clearly $w = \mathrm{size}(\mathcal{L}_j)$. Let α be the number of metering intervals elapsed from the game start. Each player i collects from the meter the readings $m_i(t_1), \dots m_i(t_\alpha)$, calculates the random polynomial $\mu_i(x)$ such that $\mu_i(0) = \sum_{l=1}^{\alpha} m_i(t_l)$, and evaluates it at x equal to $\mathrm{pos}(1), \dots, \mathrm{pos}(w)$, with $\mathrm{pos}(i)$ being the position of player i in the list $\mathcal{L}_j$.

5. Send Share

Each team member communicates to the gaming platform the shares to be forwarded to the teammates, each one associated to the identifier of the intended recipient. For each team j and for each pair (i, k) such that i, k are in the team j,

$$p_i \rightarrow G\colon p_k, \mathrm{Enc}(K_{ik}, p_i, \mu_i(\mathrm{pos}(k)))$$

6. Forward Share

For each team j and for each pair (i, k) such that i, k are in the team j,

$$G \rightarrow p_k : p_i, \mathrm{Enc}(K_{ik}, p_i, \mu_i(\mathrm{pos}(k)))$$

The metering interval B marks the end of the game period. Thus, in addition to the meter readings, each player also calculates the sum of the random numbers provided by the meter $r_i(t_1), \dots r_i(t_B)$.

Player i calculates the random polynomials $\mu(x)$ and $\rho(x)$ such that $\mu_i(0) = \sum_{l=1}^{B} m_i(t_l)$ and $\rho_i(0) = \sum_{l=1}^{B} r_i(t_l)$ and sends the relevant shares to the other team members.

For each team j and for each pair (i, k) such that i, k are in the team j,

$$p_i \rightarrow G\colon p_k, \mathrm{Enc}(K_{ik}, p_i, \mu_i(\mathrm{pos}(k))$$
$$G \rightarrow p_k : p_i, \mathrm{Enc}(K_{ik}, p_i, \mu_i(\mathrm{pos}(k)))$$

Computation of the team-aggregate consumption: For each team j, each player k of team j calculates the team-aggregate consumption share $\mathrm{pos}(k)$ as: $M(\mathrm{pos}(k)) = \sum_{i \in \mathcal{L}_j} \mu_i(x)$ and sends the result to all the other teammates.

For each pair (k, i) of players in the same team,

$$p_k \rightarrow G\colon p_i, \mathrm{Enc}(K_{ki}, p_k, M_j(\mathrm{pos}(k)))$$
$$G \rightarrow p_i\colon p_k, \mathrm{Enc}(K_{ki}, p_k, M_j(\mathrm{pos}(k)))$$

Each player i in team j reconstructs the secret polynomial and calculates the time- and team- aggregated consumption $M_j(0)$. Based on such information, each user can adapt his/her consumption behavior.

At the end of the game period, a similar subprotocol allows each player k to calculate the time- and team- aggregated random number $R_j(0)$.

Verification: At the end of the game period, if $M_j(0) < T_j$, then team j wins the challenge.

7. Send Game Outcome

All the players i in a winning team j send a message to the gaming platform claiming their prize and provide the time- and team- aggregated consumption and random number for verifying the truthfulness of their claim. These numbers are encrypted for the Utility to make them hidden from the gaming platform.

For each player i in the winning team j,

$$p_i \rightarrow G\colon p_i, \mathrm{Enc}(K_{iU}, M_j(0) \| R_j(0))$$

8. Forward Game Outcome

The platform forwards these messages to the utility for opening the commitment.

For each player i in the winning team j,

$$G \rightarrow U\colon p_i, \mathrm{Enc}(K_{iU}, M_j(0) \| R_j(0))$$

9. Final Outcome

For each team j claiming victory, the utility collects from the blockchain the commitments from all the meters in the team for all the game period and calculates their product Γ_j. By virtue of the homomorphic properties of the Pedersen commitments, the product Γ_j is equal to $h_1^{M_j(0)} h_2^{R_j(0)}$.

If all the players report the same consumption and random number and the commitment is verified, the utility confirms the victory. Otherwise it reports a failure.

$$U \rightarrow G\colon \text{verification outcome}$$

B. THE TEAM COMPETITION PROTOCOL

In this Section, we extend the Team Challenge Protocol in order to implement a one-against-one competition between two opposing teams selected by the utility to guarantee a fair match. The extension to a competition among multiple teams is straightforward.

Game Setup: The game setup is similar to the challenge protocol, except that the team consumption threshold for team is replaced by the list of members of the competing teams.

1. Game Selection

For each i,

$$p_i \rightarrow G\colon p_i, g^{a_i}$$

2. Player List

$$G \rightarrow U\colon\ (p_1, g^{a_1}) \ldots (p_N, g^{a_N})$$

3. Team List

The utility generates a private session key a_U and calculates the session key with each player $K_{iU} = \mathrm{KGF}((g^{a_i})^{a_U})$.

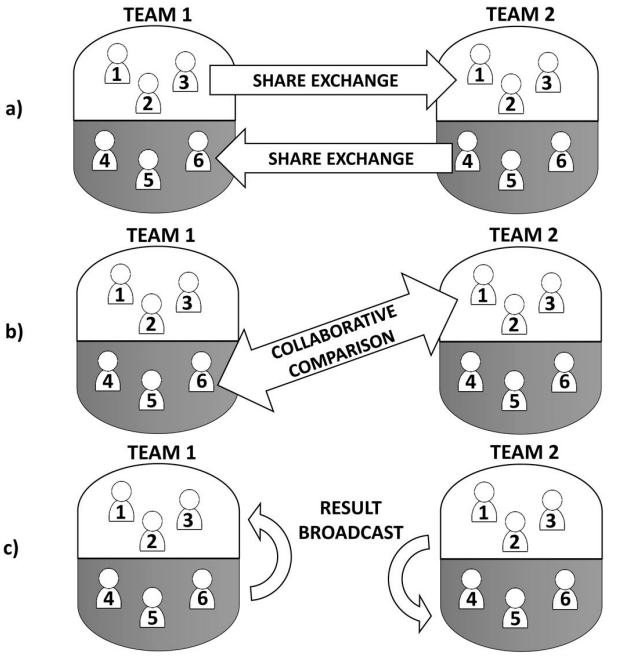

FIGURE 2. Example of the collaborative comparison protocol phases with two teams of 6 players each.

Moreover, it forms the teams and groups them in opposing pairs. Let $(\mathcal{L}_j, \mathcal{L}_{j'})$ be the lists of members of two opposing teams. For each team pair (j, j'),

$$U \rightarrow G\colon g^{a_U}, \mathcal{L}_j, \mathcal{L}_{j'}$$

The gaming platform learns the team compositions and forwards them to each involved player.

4. Game Goals

For each team pair (j, j') and each player i in $\mathcal{L}_j$ or $\mathcal{L}_{j'}$,

$$G \rightarrow p_i\colon g^{a_U}, \mathcal{L}_j, \mathcal{L}_{j'}$$

Computation of the time- and team-aggregated consumption: At the end of each metering interval the players perform the computation of the time- and team-aggregated consumption exactly as in the Team Challenge Protocol to obtain the random polynomials $M_j(x)$ (or $M_{j'}(x)$) representing the respective total consumption.

Comparison of the aggregated consumption: For the sake of conciseness, we discuss the details of the aggregated consumption comparison phase in the case of two competing teams of equal size.[1] The members of each team are divided in two subgroups. Let $\mathcal{M}_j$ and $\mathcal{N}_j$ be the two subgroups containing the first and the second half of the members of team j.[2] Similarly, $\mathcal{M}_{j'}$ and $\mathcal{N}_{j'}$ are the two subgroups of team j'.

As depicted in Figure 2, this subprotocol comprises three steps.

[1] This condition is necessary to ensure that the shares of the aggregated consumption measurements are computed using polynomials of the same degree.

[2] If the size of the team is odd, the additional member is in the first group.

In the first step (see Figure 2(a)), each player $i \in \mathcal{M}_j$ communicates $M_j(\text{pos}(i))$ to the corresponding player in $\mathcal{M}_{j'}$. Similarly, each player $i \in \mathcal{N}_{j'}$ communicates $M_{j'}(\text{pos}(i))$ to the corresponding player in $\mathcal{N}_j$. At the end of this procedure half of the shares of each team are known to the other team. These shares are not sufficient for reconstructing the other team consumption.

In the second step, the players who received a share from the opponent team are engaged in the collaborative comparison procedure (see Figure 2(b)), whereas the remaining ones will be informed about the result of the comparison in the third step. The collaborative comparison is performed according to the protocol described in [42]. At the end of the comparison, the players in $\mathcal{M}_j$ and in $\mathcal{N}_{j'}$ learn a bit indicating which team currently has the lower consumption (see Figure 2(c)).

Then, each player involved in the comparison broadcasts the result to each other team member. According to the result of the comparison, the players may revise their future consumption behaviours.

Verification: At the end of the game period, the two teams calculate their time- and team-aggregated consumption $M_j(0)$, $M_{j'}(0)$ and random numbers $R_j(0)$, $R_{j'}(0)$, and either team j or team j' wins the challenge.

7. Send Game Outcome

All the players i in the winning team send a message to the gaming platform claiming their prize and provide the encrypted time- and team- aggregated consumption and the random number for verifying the claim.

For each player i in the winning team j (or j'),

$$p_i \rightarrow G\colon \text{Enc}(K_{iU}, M_j(0) \| R_j(0)).$$

8. Forward Game Outcome

If the players of the losing team do not falsely claim victory, the gaming platform adjudicates the match. Otherwise, the gaming platform forwards all the messages to the utility for opening the commitments.

For each player i in team j,

$$G \rightarrow U : p_i, \text{Enc}(K_{iU}, M_j(0) \| R_j(0))$$

and similarly for team j'.

9. Final Game Outcome

For each team claiming victory, the utility collects from the blockchain the commitments from all the meters in the team for all the game period and calculates their product. After verifying that the provided consumption is consistent with the commitment, the utility declares the winning team.

$$U \rightarrow G\colon \text{verification outcome}$$

VI. SECURITY ASSESSMENT

The correctness of the protocol is a direct consequence of the correctness of the homomorphic aggregation and comparison protocols.

We now show that the security properties enumerated in Section IV-C are satisfied by the proposed gaming framework. With the only exception of property P5, we provide proofs for the case of team challenge with a single team (the extension to multiple teams and to the case of team competition is straightforward).

We prove properties P1 and P3 in the computational security model. Given an experiment with binary parameter b, the Adversary is any feasible algorithm $\mathcal{A}$ that returns a binary guess b'. The advantage is defined as:

$$\text{Adv} = |\Pr\{\mathcal{A} = 0 | b = 0\} - \Pr\{\mathcal{A} = 0 | b = 1\}|$$

A property is achieved if the Adversary can win the corresponding experiment with a negligible advantage.

We prove properties P2, P4, and P5 in the information-theoretic model. A property is achieved if the Adversary can win the corresponding experiment with probability 1/2.

With respect to P1, we prove that, with the proposed protocol, the game platform G gains information about the threshold T with negligible probability. The proof can be easily extended to the aggregate consumption or the consumption of any individual player.

Algorithm 1 Experiment for Property P1

on input b
G chooses two thresholds T_0, T_1
The team challenge protocol runs using threshold T_b
G outputs a bit b'
G wins if $b = b'$

Theorem 1 (Property P1): The game platform has negligible advantage in winning the experiment in Algorithm 1.

Proof: When running the team challenge protocol, G receives:

- the player identities p_i and their public keys g^{a_i};
- the public key of the utility g^{a_U};
- the list of team members $\mathcal{L}$;
- the encrypted values $\text{Enc}(K_{iU}, p_i, T_b)$ for each player i;
- other encrypted messages.

We prove by contradiction. Suppose that G has non-negligible advantage in winning the experiment in Algorithm 1. The only messages that depend on T_b are the encrypted values $\text{Enc}(K_{iU}, p_i, T_b)$. Therefore, G is able to distinguish message $\text{Enc}(K_{iU}, p_i, T_0)$ from message $\text{Enc}(K_{iU}, p_i, T_1)$ with non-negligible probability. But this contradicts the hypothesis that Enc is semantically secure. ■

Algorithm 2 Experiment for Property P2

on input b
U chooses a team and two series of individual consumption measurements $m_i^0(t)$ and $m_i^1(t)$ for all players in the team and for all time intervals $1 \leq t \leq B$ such that their sum is the same
The team challenge protocol runs using measurements $m_i^b(t)$
U outputs b'
U wins if $b = b'$

Theorem 2 (Property P2): The utility U has probability 1/2 of winning the experiment in Algorithm 2.

Proof: The utility U has access to:

- all the meter commitments $c_i(t)$ stored in the blockchain;
- the player identities p_i and their public key g^{a_i};
- the team-aggregated consumption $M(0)$ and the sum $R(0)$ of the random numbers generated by the meters

The player identities and the ephemeral public keys are independent of the choice of the individual consumption profiles. By construction, the aggregated consumption $M(0)$ is the same regardless to the value of b, thus providing no information on the choice of b. The random number $R_j(0)$ is the sum of several secret random numbers uniformly chosen in a finite group, independently of the choice of the individual consumption patterns.

Assume that $b = 0$, then $c_i(t) = h_1^{m_i^0(t)} h_2^{r_i(t)}$. We now prove that there exists a unique set of random numbers $r_i'(t)$ that can be used to reveal $m_i^1(t)$ as if b were equal to 1.

For each i and for each t, we need to solve the equation:

$$h_1^{m_i^0(t)} h_2^{r_i(t)} = h_1^{m_i^1(t)} h_2^{r_i'(t)} \pmod{q_1} \tag{1}$$

Let α be the unknown discrete logarithm of h_2 with respect to h_1. Then,

$$\alpha r_i'(t) = \alpha r_i(t) + m_i^0(t) - m_i^1(t) \pmod{q_2} \tag{2}$$

Since q_2 is prime and h_1 and h_2 are distinct, then $\gcd(\alpha, q_2) = 1$ and Equation (2) has a unique solution.

We also note that set of random numbers $r_i'(t)$ also sums to $R(0)$. In fact, by multiplying all the instances of Equation (1) for all i and for all t, we obtain:

$$h_1^{\sum_{i,t} m_i^0(t)} h_2^{\sum_{i,t} r_i(t)} = h_1^{\sum_{i,t} m_i^1(t)} h_2^{\sum_{i,t} r_i'(t)} \pmod{q_1}$$

By taking the logarithm of both sides, we obtain:

$$M(0) + \alpha R(0) = M(0) + \alpha \sum_{i,t} r_i'(t) \pmod{q_2}$$

Since $\gcd(\alpha, q_2) = 1$, this equation has the unique solution

$$\sum_{i,t} r_i'(t) = R(0). \pmod{q_2}$$

Since the set of commitments can reveal both sets of measurements, a curious U cannot distinguish between the case $b = 0$ and the case $b = 1$. ∎

Algorithm 3 Experiment for Property P3

A team of players chooses a set of measurements $m_i'(t)$ different from the set of measurements $m_i(t)$ collected by the meters and such that $\sum_{i,t} m_i'(t) < \sum_{i,t} m_i(t)$
The team challenge protocol runs
U performs the verification algorithm
The team wins if U accepts the measurements as valid

Theorem 3 (Property P3): The team has negligible advantage in winning the experiment in Algorithm 3.

TABLE 1. Assumptions on parameter sizes.

Notation	Length (bits)
T_j	24
$t_1, \ldots, t_B$	32
p_i	32
Q_1 and Q_2	32 and 256
q_1	2048

TABLE 2. Message sizes.

Message	Length [bits]
GAME SELECTION	2080
PLAYER LIST	$2080N$
TEAM LIST (challenge)	$2048 + 2264\,\text{size}(\mathcal{L}_j)$
TEAM LIST (competition)	$4160\,\text{size}(\mathcal{L}_j)$
GAME GOALS (challenge)	$2232 + 2080\,\text{size}(\mathcal{L}_j)$
GAME GOALS (competition)	$4160\,\text{size}(\mathcal{L}_j)$
SEND SHARE	224
SEND SHARE (random number)	448
FORWARD SHARE	224
FORWARD SHARE (random number)	448
SEND GAME OUTCOME	640
FORWARD GAME OUTCOME	672
FINAL OUTCOME	1

Proof: The tamper-proof meter of each player i commits to the individual measurements by storing Pedersen commitments $c_i(t) = h_1^{m_i(t)} h_2^{r_i(t)}$ in the blockchain for every time interval t in the game period. By construction, the blockchain guarantees message integrity and authentication. The utility combines the individual commitments obtaining a commitment $\Gamma = \prod_{i,t} c_i(t)$.

In addition, U receives the aggregate consumption $M(0) = \sum_{i,t} m_i'(t)$ and the aggregate random number $R(0) = \sum_{i,t} r_i'(t)$ from the team players.

In order to win, the team needs to provide a pair $(M(0), R(0))$ such that $\Gamma = h_1^{M(0)} h_2^{R(0)}$.

Since PCS is computationally binding, any attacker has negligible probability of finding any such pair different from $(\sum_{i,t} m_i(t), \sum_{i,t} r_i(t))$. ∎

Algorithm 4 Experiment for Property P4

on input b
A set $\mathcal{W}$ of fewer than w colluding players chooses a player i, not involved in the collusion, and two alternative series of individual consumption measurements $m_i^0(t), m_i^1(t)$ such that $\sum_t m_i^0(t) = \sum_t m_i^1(t)$.
The team challenge protocol runs with the non colluded members providing measurements $m_i^b(t)$.
$\mathcal{W}$ outputs b'
$\mathcal{W}$ wins if $b = b'$

Theorem 4 (Property P4): The colluded players have probability 1/2 of winning the experiment in Algorithm 4.

Proof: When running the team challenge protocol, $\mathcal{W}$ receives:

- The public key of the utility g^{a_U}, the list of team members $\mathcal{L}_j$ and the game threshold T_j.

TABLE 3. Traffic Volume per Game Session [bits per execution]. For the sake of easiness, computations are done under assumption that $|P|$ is even an that all teams chose the same game modality (either challenge or competition). In the case of competitions, the set J' includes a half of the teams, each one competing against a team in $J \setminus J'$.

Phase		Player	Game Platform	Utility
1	In	–	$2080N$	–
	Out	2080	–	–
2	In	–	–	$2080N$
	Out	–	$2080N$	–
3 chall.	In	–	$2264N + 2048\|J\|$	–
	Out	–	–	$2264N + 2048\|J\|$
3 comp.	In	–	$4160N$	–
	Out	–	–	$4160N$
4 chall.	In	$2232 + 2080\,\text{size}(\mathcal{L}_j)$	–	–
	Out	–	$2232N + 2048\sum_{j\in J}\text{size}(\mathcal{L}_j)^2$	–
4 comp.	In	$4160\,\text{size}(\mathcal{L}_j)$	–	–
	Out	–	$4160\sum_{j\in J}\text{size}(\mathcal{L}_j)^2$	–
5	In	$448(\text{size}(\mathcal{L}_j) - 1)$	$\sum_{j\in J} 448\,\text{size}(\mathcal{L}_j)(\text{size}(\mathcal{L}_j) - 1)$	–
	Out	$448\,\text{size}(\mathcal{L}_j) - 1)$	$\sum_{j\in J} 448\,\text{size}(\mathcal{L}_j)(\text{size}(\mathcal{L}_j) - 1)$	–
5 (last)	In	$1344(\text{size}(\mathcal{L}_j) - 1)$	$\sum_{j\in J} 1344\,\text{size}(\mathcal{L}_j)(\text{size}(\mathcal{L}_j) - 1)$	–
	Out	$1344(\text{size}(\mathcal{L}_j) - 1)$	$\sum_{j\in J} 1344\,\text{size}(\mathcal{L}_j)(\text{size}(\mathcal{L}_j) - 1)$	–
6	In	involved: $2735264(\text{size}(\mathcal{L}_j) - 1) + 224$, non-involved: 1	$\sum_{j\in J'}\text{size}(\mathcal{L}_j)(2735264(\text{size}(\mathcal{L}_j)-1)+449)$	–
	Out	involved: $2735264(\text{size}(\mathcal{L}_j) - 1) + 1$; non-involved: 224	$\sum_{j\in J'}\text{size}(\mathcal{L}_j)(2735264(\text{size}(\mathcal{L}_j)-1)+449)$	–
7	In	–	$416N$	–
	Out	416	–	–
8	In	–	–	$416N$
	Out	–	$416N$	–
9	In	–	$\|J\|$	–
	Out	–	–	$\|J\|$

- All the shares of the individual measurements delivered to members of the collusion, i.e. $\mu_i(\text{pos}(k))\ \forall k \in \mathcal{W}$, for each time interval.
- All the shares of the secret polynomials $M(x)$ and $R(x)$, which hide the aggregate team consumption and team random numbers.

The player identities and the ephemeral public key of the Utility are independent of the choice of the individual consumption profiles. By construction, the secret polynomials $M(x)$ and $R(x)$ do not depend on b.

At every aggregation round t, the colluded players obtain $|\mathcal{W}|$ shares of either the secret $m_i^0(t)$ or the secret $m_i^1(t)$. Since the secret sharing scheme is unconditionally secure, knowledge of up to $w - 1$ shares provides no information on the shared secret. It follows that the colluded players gain no advantage in winning the experiment. ■

Theorem 5 (Property P5): The players of Team 1 have probability 1/2 of winning the experiment in Algorithm 5.

Proof: The only messages received by Team 1 that depend on b are the messages exchanged in step 4 (Game Goals). The comparison protocol is unconditionally secure against a collusion of at most w players. Since the comparison protocol is performed by half of the members of Team 1, it follows that $\mathcal{A}$ controls at most $w/2$ players. Consequently, $\mathcal{A}$ gains no advantage in the experiment from the knowledge of the protocol messages. ■

Algorithm 5 Experiment for Property P5

on input b
The attacker $\mathcal{A}$ is the set of players of Team 1.
Team 1 chooses its aggregate consumption M_1.
Team 1 chooses two aggregate consumption values M_2^0 and M_2^1 such that $M_2^0 < M_1$ and $M_2^1 < M_1$.
The Team Competition protocol runs with Team 2 providing M_2^b as input.
Team 1 outputs b'
Team 1 wins is $b = b'$

VII. PERFORMANCE ASSESSMENT

In this Section we evaluate the data throughput and computational effort required from each entity participating in our proposed privacy-friendly gaming framework. To this aim, we make the assumption that a standard AES symmetric cryptosystem with Counter mode (CTR)

TABLE 4. List of computational costs.

Notation	Description	Computational Cost (number of multiplications/exponentiations)
$C_{mul}(x)$	cost of a multiplication modulo x	1 multiplication modulo x
$C_e(x)$	cost of an exponentiation modulo x	1 exponentiation modulo x
$C_s(x,w)$	cost of the generation of w shares modulo x	$O(w^2)\cdot C_{mul}(x)$
$C_l(x,w)$	cost of a share Lagrange interpolation modulo x using w shares	$O(w^2)\cdot C_{mul}(x)$
$C_m(x,w)$	cost of a share collaborative multiplication modulo x using w shares [41]	$O(w^2)\cdot C_{mul}(x)$
$C_c(x,w)$	cost of a share collaborative comparison modulo x using w shares [42]	$102x\cdot C_s(x,w)+(177x+3)\cdot C_m(x)+(102x+15)\cdot C_l(x)$

TABLE 5. Node computational load.

	Player	Utility
Setup (challenge)	$(\text{size}(\mathcal{L}_j)+1)\cdot C_e(2048)$	$(N+1)\cdot C_e(2048)$
Setup (competition)	$\text{size}(\mathcal{L}_j)\cdot C_e(2048)$	–
Aggregation	$C_s(32,\text{size}(\mathcal{L}_j))+C_l(32,\text{size}(\mathcal{L}_j))$	–
Aggregation (last round)	$C_s(32,\text{size}(\mathcal{L}_j))+C_l(32,\text{size}(\mathcal{L}_j))+C_s(256,\text{size}(\mathcal{L}_j))+C_l(256,\text{size}(\mathcal{L}_j))$	–
Comparison	$\text{size}(\mathcal{L}_j)\cdot C_e(2048)+C_c(32,\text{size}(\mathcal{L}_j))+C_l(32,\text{size}(\mathcal{L}_j))$	–
Verification	–	$\sum_{j\in J}(\lceil\text{size}(\mathcal{L}_j)\log_2 B\rceil+\lceil\log_2(\text{size}(\mathcal{L}_j))\rceil+1)C_{mul}(2048)+2C_e(2048)$

operation and nonces of 128 bits is implemented in the infrastructure (i.e. on input of a m-bit-long plaintext, the cryptosystem outputs a $m+n$-bits-long cyphertext, where n is the nonce length). Tables 1 and 2 respectively report the sizes of all the parameters required by our privacy-friendly protocol and of every exchanged message.

Additionally, in Table 3 we report the input/output data volumes that are received/sent by the involved entities in each protocol phase. Results show that every player sends/receives data volumes in the order of tenths of megabits, depending on the number of team members. Differently, the utility and the game platform exchange a higher amount of data, due to the quadratic dependency on the size of the teams (e.g. 1000 users grouped in 50 teams of 20 members each lead to data volumes in the order of hundreds of Gbits). We assume that both entities run the game application on dedicated servers with adequate communication capabilities.

Moreover, we report the computational effort required from each involved entity in Table 5 during every phase of the protocol. The computational costs of each operation in terms of multiplications and exponentiations are detailed in Table 4. Results show that the game platform does not perform any computation and uniquely acts as a relay node, whereas the utility is required to perform computations during for the game setup and results verification phases. The computational burden in terms of number of exponentiations shows a linear dependency on the total number of players, whereas the number of multiplications grows logarithmically with the team sizes. However, both phases occur only once during a single game execution and the temporal horizon of each game may span one or several days. Therefore, the protocol guarantees scalability even when several thousands of users are involved (e.g. the citizens of a medium/large-sized town). Finally, at the player side, the highest computational burden is required for the consumption aggregation and comparison. Their computational complexity mainly depends on the number of collaborative multiplications, which grows linearly with the number of team members. However, if the number of players per team is in the order of tens of users and under the reasonable assumption that the SSS modulus is relatively small, a few thousands of modular multiplications are expected to be computed at every comparison round (i.e. a few times per each game execution). Therefore, as long as the team size is limited, the framework scalability is not hindered.

VIII. CONCLUSIONS

In this paper we propose a privacy-friendly gaming platform aimed at engaging users in diminishing the energy/water consumption at their premises. The game implements team challenges against an unmanned adversary or among competing player teams. We also propose a protocol that enables the game execution without disclosing the individual meter readings of the participants.

To detect cheating, the protocol uses a blockchain-based authenticated storage to collect secure commitments by the meters. This way, the users can formally prove to have correctly reported their measurements to the protocol without disclosing the measurements themselves. We assess the security of the proposed framework assuming that the entities behave according to the honest-but-curious

adversarial model. The numerical assessment of the computational load and exchanged data volumes required by the protocol shows that the framework can scale up to several thousands of players.

ACKNOWLEDGEMENTS

The authors would like to thank A. Facchini for the useful discussions and suggestions.

REFERENCES

[1] T. Susi, M. Johannesson, and P. Backlund, "Serious games: An overview," School Hum. Inform., Univ. Skövde, Skövde, Sweden, Tech. Rep. HS-IKI-TR-07-001, 2007.
[2] M. D. Childress and R. Braswell, "Using massively multiplayer online role-playing games for online learning," *Distance Edu.*, vol. 27, no. 2, pp. 187–196, 2006.
[3] D. Thompson *et al.*, "Serious video games for health: How behavioral science guided the development of a serious video game," *Simul. Gaming*, vol. 41, no. 4, pp. 587–606, Aug. 2010.
[4] G. Rebolledo-Mendez, K. Avramides, S. de Freitas, and K. Memarzia, "Societal impact of a serious game on raising public awareness: The case of floodsim," in *Proc. ACM SIGGRAPH Symp. Video Games*, 2009, pp. 15–22.
[5] A. Bourazeri and J. Pitt, "Serious game design for inclusivity and empowerment in smartgrids," in *Proc. 1st Int. Workshop Intell. Digit. Games Empowerment Inclusion*, 2013, pp. 1–5.
[6] T. Hirsch, "Water wars: Designing a civic game about water scarcity," in *Proc. 8th ACM Conf. Designing Interact. Syst. (DIS)*, New York, NY, USA, 2010, pp. 340–343.
[7] I. Bogost, *Persuasive Games: The Expressive Power of Videogames*. Cambridge, MA, USA: MIT Press, 2007.
[8] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: Defining 'gamification,'" in *Proc. ACM 15th Int. Acad. MindTrek Conf., Envisioning Future Media Environ.*, 2011, pp. 9–15.
[9] A. E. Rizzoli *et al.*, "The SmartH2O project and the role of social computing in promoting efficient residential water use: A first analysis," in *Proc. Int. Environ. Modelling Softw. Soc.*, 2014, pp. 1–9.
[10] A. Gustafsson, C. Katzeff, and M. Bang, "Evaluation of a pervasive game for domestic energy engagement among teenagers," *Comput. Entertainment*, vol. 7, no. 4, 2009, Art. no. 54.
[11] R. McCall and V. Koenig, "Gaming concepts and incentives to change driver behaviour," in *Proc. IEEE 11th Annu. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, Jun. 2012, pp. 146–151.
[12] D. Michael and S. Chen, *Serious Games: Games That Educate, Train, and Inform*. New York, NY, USA: Muska & Lipman/Premier-Trade, 2005.
[13] R. Orji, R. L. Mandryk, J. Vassileva, and K. M. Gerling, "Tailoring persuasive health games to gamer type," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2013, pp. 2467–2476.
[14] U. Ritterfeld, M. Cody, and P. Vorderer, Eds., *Serious Games: Mechanisms and Effects*. Evanston, IL, USA: Routledge, 2009.
[15] T. M. Connolly, E. A. Boyle, E. MacArthur, T. Hainey, and J. M. Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Comput. Edu.*, vol. 59, no. 2, pp. 661–686, 2012.
[16] G. Peschiera, J. E. Taylor, and J. A. Siegel, "Response–relapse patterns of building occupant electricity consumption following exposure to personal, contextualized and occupant peer network utilization data," *Energy Buildings*, vol. 42, no. 8, pp. 1329–1336, 2010.
[17] J. Schrammel, C. Köffel, and M. Tscheligi, "Personality traits, usage patterns and information disclosure in online communities," in *Proc. 23rd Brit. HCI Group Annu. Conf. People Comput., Celebrating People Technol.*, 2009, pp. 169–174.
[18] D. Martinovic, V. Ralevich, J. McDougall, and M. Perklin, "'You are what you play': Breaching privacy and identifying users in online gaming," in *Proc. IEEE 12th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Jul. 2014, pp. 31–39.
[19] V. Koenig, F. Boehm, and R. McCall, "Pervasive gaming as a potential solution to traffic congestion: New challenges regarding ethics, privacy and trust," in *Entertainment Computing*. Berlin, Germany: Springer, 2012, pp. 586–593.
[20] G. W. Hart, "Nonintrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.
[21] C. Laughman *et al.*, "Power signature analysis," *IEEE Power Energy Mag.*, vol. 1, no. 2, pp. 56–63, Mar. 2003.
[22] C. Rottondi and G. Verticale, "Enabling privacy in a gaming framework for smart electricity and water grids," in *Proc. Int. Workshop Cyber-Phys. Syst. Smart Water Netw. (CySWater)*, Apr. 2016, pp. 25–30.
[23] L. Galli *et al.*, "A gamification framework for customer engagement and sustainable water usage promotion," in *Proc. 36th IAHR World Congr.*, The Hague, The Netherlands, Jul. 2015, pp. 1–14.
[24] P. Fraternali *et al.*, "enCOMPASS—An integrative approach to behavioural change for energy saving," in *Proc. GIoTS Workshop Energy Efficient Solutions (IoT-EESIoT)*, Jun. 2017, pp. 273–278.
[25] M. Jawurek, F. Kerschbaum, and G. Danezis, "SoK: Privacy technologies for smart grids—A survey of options," Microsoft Res., Cambridge, U.K., Tech. Rep. MSR-TR-2012-119, 2012.
[26] G. Si, Z. Guan, J. Li, P. Liu, and H. Yao, "A comprehensive survey of privacy-preserving in smart grid," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, G. Wang, I. Ray, J. M. A. Calero, and S. M. Thampi, Eds. Cham, Switzerland: Springer, Nov. 2016, pp. 213–223.
[27] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang. (2016). "A survey on privacy-preserving schemes for smart grid communications." [Online]. Available: https://arxiv.org/abs/1611.07722
[28] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[29] C. Rottondi, G. Verticale, and C. Krauss, "Privacy-preserving smart metering with multiple data consumers," *Comput. Netw.*, vol. 57, no. 7, pp. 1699–1713, May 2013.
[30] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1592, J. Stern, Ed. Berlin, Germany: Springer, 1999, pp. 223–238.
[31] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
[32] L. Chen, R. Lu, and Z. Cao, "PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," *Peer-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1122–1132, Nov. 2015.
[33] T. Dimitriou and M. K. Awad, "Secure and scalable aggregation in the smart grid resilient against malicious entities," *Ad Hoc Netw.*, vol. 50, pp. 58–67, Nov. 2016.
[34] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics," in *Proc. USENIX Secur. Symp.*, 2010, p. 15.
[35] C. Rottondi and G. Verticale, "Privacy-friendly load scheduling of deferrable and interruptible domestic appliances in smart grids," *Comput. Commun.*, vol. 58, pp. 29–39, Mar. 2015.
[36] C. Rottondi, S. Fontana, and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging," *Energies*, vol. 7, no. 5, pp. 2780–2798, 2014.
[37] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[38] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multiparty computations on bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 443–458.
[39] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.
[40] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2005.
[41] R. Gennaro, M. O. Rabin, and T. Rabin, "Simplified VSS and fast-track multiparty computations with applications to threshold cryptography," in *Proc. 17th Annu. ACM Symp. Principles Distrib. Comput.*, 1998, pp. 101–111.
[42] T. Nishide and K. Ohta, "Multiparty computation for interval, equality, and comparison without bit-decomposition protocol," in *Public Key Cryptography*. Berlin, Germany: Springer-Verlag, 2007, pp. 343–360.
[43] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology*. Berlin, Germany: Springer, 1992, pp. 129–140.
[44] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 226–240.

CRISTINA ROTTONDI received the master's (*cum laude*) and Ph.D. (*cum laude*) degrees in telecommunications engineering from the Politecnico di Milano in 2010 and 2014, respectively. She is currently a Researcher with the Dalle Molle Institute for Artificial Intelligence, Lugano, Switzerland. Her research interests include cryptography, communication security, design and planning of optical networks, and networked music performance.

GIACOMO VERTICALE received the Ph.D. degree in telecommunications engineering from the Politecnico di Milano in 2003. He is currently an Assistant Professor with the Politecnico di Milano, Italy. His Ph.D. dissertation was on the performance of packet transmission in UMTS. From 1999 to 2001, he was with the Research Center CEFRIEL, where he was involved in the Voice-over-IP and ADSL technologies. He was involved in several European research projects advancing the Internet technology. His current interests focus on the security issues of the Smart Grid and on Network Function Virtualization.