Enabling Privacy in a Gaming Framework for Smart Electricity and Water Grids

Cristina Rottondi* and Giacomo Verticale†
* Dalle Molle Institute for Artificial Intelligence (IDSIA)
University of Lugano (USI) - University of Applied Science and Arts of Southern Switzerland (SUPSI)
cristina.rottondi@supsi.ch
† Department of Electronics, Information, and Bioengineering, Politecnico di Milano, Italy
giacomo.verticale@polimi.it

***Abstract*—Serious games are potentially powerful tools to influence users' preferences and attitudes. However, privacy concerns related to the misuse of data gathered from the players may emerge in online-gaming interactions.**

This work proposes a privacy-friendly framework for a gaming platform aimed at reducing energy and water usage, where players are grouped in teams with the challenge of maintaining the aggregated consumption of its members below a given threshold. We discuss a communication protocol which enables the team members to compute their overall consumption without disclosing individual measurements. Moreover, the protocol prevents the gaming platform from learning the consumption data and challenge objectives of the players. Correctness and truthfulness checks are included in the protocol to detect cheaters declaring false consumption data or providing altered game results. The security and performance of the framework are assessed, showing that scalability is ensured thanks to the limited data exchange and lightweight cryptographic operations.

***Index Terms*—Smart Grid; Gamification; Serious Games; Privacy.**

I. Introduction

During the last years, there has been a significant growth of interest in game-based approaches aimed at motivating, increasing and/or influencing users' activities. Depending on the specific design of the game-based experience, such approaches can be classified in two classes: serious games and gamified interactions. The former category comprises games used for purposes other than entertainment [1], which have been successfully used for teaching, training or raising awareness in domains ranging from education [2] and health care [3] to resource [4] and demand side management [5].

Conversely, gamified interactions are characterized by "the use of game design elements in non-game contexts" [6]. They often have a persuasive goal, like promoting a more sustainable consumption of energy [7] or water resources [8], or to encourage drivers to undertake a particular behaviour in order to avoid traffic jams [9].

Several studies on the usage of these game-based approaches [10], [11] have proven their positive effects on users. For instance, in the context of energy conservation within the dwellers of a block of flats, the authors of [12] provide empirical evidence that the users' awareness of the behaviours of the other occupants has a positive impact on their energy conservation attitudes. In the context of smart power grids, some utilities employ gamification as part of larger behavioral demand response approaches to perform peak shaving.

Unfortunately, the use of online gaming implies the emergence of several privacy concerns related to the characteristics and the exploitation of data collected from the players. In [13], [14], the authors discuss how information on physical, mental and social attributes of the players can be inferred based on collected logs about performed game actions and choices, whereas in [15] the issues pertaining to ethics, privacy and trust which emerge in the context of a serious game aimed at reducing traffic jams in Luxembourg are illustrated. These concerns become even more threatening if gaming data can be combined to data related to resource consumption (e.g. electricity, water or gas usage), which by themselves already provide private information about users [16].

To overcome such issues, in this paper we provide some cryptographic mechanisms for an online gaming platform operated by a third-party service. The game application scenario is a smart electricity or water grid where the utility tries to influence the behaviour of users in order to indirectly shape their aggregate consumption curve (e.g. peak shaving). More in detail, we provide the following novel contributions: i) the definition of a privacy-friendly gaming framework where teams of users undertake challenges aimed at maintaining their overall consumption below a specific threshold set by the utility; ii) a set of privacy-preserving protocols based on Shamir Secret Sharing scheme which allow team members to compute their aggregate consumption without disclosing individual contributions; iii) a verification mechanism based on Pedersen Commitments which is executed by the utility and prevents users from reporting bogus results to the game platform; iv) the performance assessment and security analysis of the proposed framework, under assumption that users are honest-but-curious.

The remainder of the paper is structured as follows: Section II and III provide a short overview of the related literature and of the basic cryptographic background notions, whereas Section IV describes the structure of the privacy-preserving social game framework. The security analysis and performance assessment of the proposed framework are provided in Section V and VI, respectively. Conclusions are drawn in the final Section.

978-1-5090-1161-2/16/$31.00 ©2016 IEEE

II. Related Work

In the last few years, a number of serious games specifically addressing smart electricity and water grid scenarios have been proposed (see e.g. [5], [7], [4], [17], [8]). Reference [5] describes a game platform for demand side management in smart grids. The game applies a self-organised approach to regulate the overall energy consumption using a set of social rules and principles and is implemented through individual or group challenges, where players are rewarded in case of achievement of given objectives. The authors mention the existence of ethics/privacy problems concerning the collection of metering data gathered from the users' smart meters, but does not propose any countermeasure to mitigate such issues. Similar challenge-based approaches are adopted also in Reference [7], which designs a game aimed ad reducing home energy usage and proposes team competitions where groups of users compete in achieving the lowest team-aggregated consumption. Reference [8] proposes a gameplay based on a virtual 'community garden', of which each user owns a patch. Players' water usage measured by the smart meters is reflected in how much water their plants receive: the more water they waste in their household, the less is available for plants. Users compete for the best patch and may exchange tips on how to optimize consumption.

A more complex game mechanism is proposed in Reference [17], which designs a gamified water utility portal that allows users to monitor the water consumption within their household and implements an awarding system which combines points and badges to reward positive behaviors, which include actions aimed at reducing water consumption, learning actions (e.g. engaging educational activities proposed by the portal), and data provision actions (e.g. providing detailed information about the time-of-use of water consuming appliances, which can be exploited by the utility for consumption forecasting).

Our proposed framework adopts a similar type of challenge (i.e. multiplayer competitions versus an unmanned challenger) but includes a communication protocol which avoids the disclosure of individual consumption data in a scenario where players behave according to the honest-but-curious model, (i.e., they try to learn additional information from the observed data). Moreover, the protocol includes a set of checks to detect potential cheating behaviours during the game execution. To the best of our knowledge, this is the first attempt to embed privacy-preserving mechanisms in a serious game platform.

III. Background

A. Shamir Secret Sharing

Shamir Secret Sharing (SSS) scheme belongs to the family of cryptographic threshold schemes, which are designed to enable the collaborative reconstruction of a secret. In a (w, t)-threshold scheme, the secret is divided in w parts called *shares*, which are distributed among the protocol participants and can be reconstructed if at least $t \leq w$ participants cooperate.

The SSS scheme works as follows: let $m \in Z_Q$ be the secret, where Q is a prime number, greater than w and than all the possible secrets. To split the secret in w shares, the dealer chooses $t-1$ integer random numbers $\rho_1, \rho_2, \cdots, \rho_{t-1}$ with uniform distribution in $[0, Q-1]$ and calculates the s-th share of the secret ν, denoted by the pair (x_s, y_s) for $1 \leq s \leq w$, where x_s are distinct integer numbers and $y_s = \nu + \rho_1 x_s + \rho_2 x_s^2 + \ldots + \rho_{t-1} x_s^{t-1} \bmod Q$. The secret can be recovered in presence of at least t shares by using the Lagrange interpolation method. The SSS scheme is homomorphic w.r.t. addition, meaning that sums can be performed directly on the shares, leading to the same result that would be obtained by summing the plaintexts.

B. Pedersen Commitment Scheme

A commitment scheme is a two-party cryptographic protocol by which a party (Alice) chooses a secret input and gives to the other party (Bob) a message, called commitment. At a later stage, Alice reveals the secret and Bob can verify that the secret was not changed after sending the commitment.

Pedersen Commitment Scheme (PCS) [18] 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 $\mathcal{G}$. Alice chooses an input x and a random number $r \in \mathbb{Z}_p$, then sends $c = h_1^x h_2^r$ to Bob. At a later stage, Alice reveals the pair (x, r) and Bob can verify c.

PCS is *computationally binding*, meaning that Alice needs to 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, Bob learns no information from c about x. In addition, the scheme is homomorphic. In fact, 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 $(x + x', r + r')$.

Finally, we observe that one way of guaranteeing that h_1 and h_2 are generated randomly is using algorithm `PickGroup` in [19]. With this algorithm, the seed of the Cryptographically Secure Pseudorandom Generator serves as a proof that the algorithm has been executed honestly.

IV. The Privacy-Friendly Gamification Framework

A. General Description and Game Rules

We consider the scenario depicted in Figure 1, which includes a utility, U, an on-line game platform run by a third party provider, G, and a set of utility subscribers, $\mathcal{P}$. The subscribers are equipped with smart meters installed at their premises, which convey consumption data to the utility.

Players can take part to challenges targeted to groups of subscribers, which consist in keeping the team-aggregated consumption below a given threshold T provided by the utility over a time period B chosen by the users among a predefined set of options (e.g. one day, one week,...). When B expires, the challenge results are computed based on the total consumption of the users and winners are awarded.

More in detail, the game follows the following procedure:

1) When a player p wants to start a new game, he/she selects the game duration $B_p \in \{B_1, \cdots, B_n\}$ (where n is the cardinality of a predefined set of duration options).
2) Periodically, G communicates the players' choices to U, which groups the players in a set of teams J according to

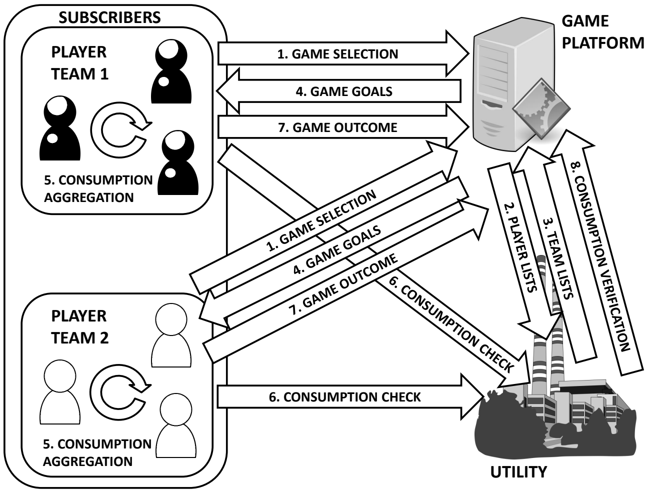

Fig. 1. The privacy-firendly gamification framework

their choices and communicates to G the lists of team members. Moreover, U informs the users about their challenge threshold.

3) Once the game starts, at regular time intervals (e.g. once every few hours or once a day) team members compute their aggregate consumption. To do so, at a given time τ every player p_i calculates his/her individual time-aggregated consumption $m^{\tau}_{p_i}$ from the beginning of the game period up to the current time τ, based on the fine-grained meter readings obtained through the local Home Area Network (HAN) and provides it to the members of his/her team. It follows that each team player will receive the individual consumption data of every other player in the team and will thus be able to compute the team-aggregate consumption. According to the result of the aggregation, the player may alter his/her future behavior (e.g. decreasing his/her consumption).
4) At the end of the game period, each player communicates to G the final team-aggregated consumption. G verifies the correctness of the received results with U (which accesses individual measurements via the secure channel established directly with the meters and may independently compute the team-aggregate consumption).
5) If a cheat is detected, the game is declared not valid, otherwise G declares the winner.

B. Security Assumptions

We make the following assumptions:

1) Communication between the parties involved in the protocol is protected from attacks by external parties by using a secure protocol such as TLS.
2) Each player p_i is provided with a smart meter. The meter is a tamper-proof device sharing a symmetric key with the utility $k^{(m)}_{iU}$. The meter periodically sends measurements to the utility by using some authenticated encryption scheme.
3) The meter can provide consumption readings at arbitrary granularity to player devices within the HAN of the subscriber via a domestic communication channel. The meter can also generate a commitment for such readings by using PCS. Commitments are authenticated by using a symmetric Mac with key $k^{(m)}_{iU}$. This way, a player can voluntary disclose meter readings with any granularity and U can verify the authenticity of such readings.
4) Each player p_i is provided by U with an identification tag ID_p.
5) The utility is a honest-but-curious entity. It executes the protocol honestly, but tries to obtain individual player measurements having finer granularity than the typical billing period (e.g. one month) in order to prevent the inference of sensitive information on the users' habits.
6) The game platform is also honest-but-curious: it executes the protocol honestly, but tries to obtain individual/aggregate consumption measurements and to learn the challenge goals of the teams.
7) The players are augmented honest-but-curious entities, i.e. they execute the protocol honestly but they may freely choose their inputs. For example, they can pretend to have a lower consumption.
8) Multiple players may also collude to learn information about other players' consumption or to win the game providing false measurements. The largest collusion is, at most, the standard team size minus 1.

C. Correctness and Security Definitions

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

P1 G obtains information about the threshold T, the aggregate consumption, or any individual user consumption.

P2 U obtains any information on individual consumption over the game time scale in addition to what is implied by knowledge of the aggregate team consumption.

P3 Any collusion of a subset of the players of a team inputs to the game different measurements than the one reported by their meter and G accepts the game result.

P4 Any collusion of a subset of players of a team obtains information about the individual consumption of any non-colluded user in the team.

D. The Privacy-Friendly Game Protocol

When initializing the system, the gaming platform chooses and publishes the SSS modulus Q, a prime number p such that the Decisional Diffie-Hellmann (DDH) problem is hard in $\mathbb{Z}_p$, a large prime q that is a factor of $p-1$, a random primitive root g of $\mathbb{Z}_p$, two random elements h_1, h_2, of $\mathbb{Z}_p$ having order q, 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: With reference to Figure 1, during the initial game setup the following protocol is executed.

1. GAMESELECTION

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

When a player p_i wants to start a new game, he/she chooses a session secret key $a_i \in \mathbb{Z}_p$ and communicates his/her identification tag ID_i, the session public key, g^{a_i}, and the chosen game period B_i.

2. PLAYERLIST

$$G \to U \colon (ID_1, g^{a_1}, B_1), (ID_2, g^{a_2}, B_2) \dots$$

At regular intervals (e.g. once a day), G forwards to U the tuples (ID_i, g^{a_i}, B_i) for each user p_i requesting for participation to the game. Based on such tuples, U groups the users in an arbitrary number of teams $\mathcal{T}_1, \mathcal{T}_2, \cdots \mathcal{T}_{|J|}$. For each team $\mathcal{T}_j \colon j \in J$, U defines the challenge duration $B_{\mathcal{T}_j}$. Moreover, U chooses the challenge threshold $T_{\mathcal{T}_j}$.

3. TEAMLIST

$$U \to G \colon \mathcal{L}_{\mathcal{T}_j}, g^{a_U}, [\mathrm{gametoken_i} \ \forall p_i \in \mathcal{T}_j]$$

Where $\mathrm{gametoken_i} = \mathrm{Enc}(K_{iU}, ID_i \| \tau_U \| T_{\mathcal{T}_j})$. The utility generates a session secret key, $a_U \in \mathbb{Z}_p$, a public key g^{a_U}, and pairwise symmetric keys with each player $K_{iU} = \mathrm{KGF}((g^{a_i})^{a_U})$. For each team $\mathcal{T}_j$, U generates an ordered team member list $\mathcal{L}_{\mathcal{T}_j} = [(ID_i, g^{a_i}) \colon p_i \in \mathcal{T}_j]$. For each team member p_i in team $\mathcal{T}_j$, U prepends the player identifier ID_i and the current timestamp τ_U to the threshold, then encrypts it with the pairwise key K_{iU} and sends the team lists and the encrypted values to G.

4. GAMEGOALS

$$G \to p_i \colon \mathcal{L}_{\mathcal{T}_j}, g^{a_U}, \mathrm{gametoken_i}$$

For every team $T_{\mathcal{T}_j}$, G learns the team composition and forwards it to each player together with the utility public key and the relevant encrypted token. This way, by deciphering the received message the players obtain the team composition and challenge threshold, but the challenge threshold remains hidden to the game platform.

Computation of the aggregate consumption: If at time τ the computation of the team-aggregate consumption is required, every player p_i divides the value of his/her individual consumption $m^{\tau}_{p_i}$ in shares using the SSS scheme with parameters $w = t = |\mathcal{T}_j|$. For the sake of easiness, we assume that such shares are obtained by evaluating the SSS polynomial at points $x_s = 1, 2, \cdots, |\mathcal{T}_j|$. Player p_i keeps the i-th share $(x_i^{p_i}, y_i^{p_i})$ for him/herself (where i indicates the player position in the ordered list $\mathcal{L}_{\mathcal{T}_j}$) and sends each of the remaining shares $(x_k^{p_i}, y_k^{p_i})$ to the corresponding team member $p_k \in \mathcal{T}_j \setminus \{p_i\}$ (according to the ordering provided in the list $\mathcal{L}_{\mathcal{T}_j}$). Notice that, every time p_i needs to communicate a share to the other team members, he sends to G the following message:

5a. SENDSHARE

$$p_i \to G \colon [ID_k, \mathrm{Enc}(K_{ik}, ID_k \| \tau_{p_i} \| r_{p_i} \| (x_k^{p_i}, y_k^{p_i})) \quad \forall k \in \mathcal{T}_j \colon k \neq i]$$

The message includes the ID of the player p_k to which the k-th share is addressed and the encryption of the k-th share, concatenated to the current timestamp, a random number r_i generated by the meter and the ID of p_k. In turn, G and forwards each share to the addressed player with the following message:

5b. FORWARDSHARE

$$G \to p_k \colon ID_k, \mathrm{Enc}(K_{ik}, ID_k \| \tau_{p_i} \| r_{p_i} \| (x_k^{p_i}, y_k^{p_i}))$$

This way, any direct communication between players is avoided.

Once all the shares have been received, each player p_i computes the i-th aggregate share $(X_i^{\mathcal{T}_j}, Y_i^{\mathcal{T}_j})$ where $Y_i^{\mathcal{T}_j} = \sum_{k=1}^{|\mathcal{T}_j|} y_i^{p_k}$ and broadcasts it to all the team members. Finally, every team member applies the Lagrange interpolation method to decrypt the total team aggregated consumption $M^{\tau} = \sum_{p_i \in \mathcal{T}_j} m^{\tau}_{p_i}$ using his own aggregated share $(X_i^{\mathcal{T}_j}, Y_i^{\mathcal{T}_j})$ and the $|\mathcal{T}_j| - 1$ aggregated shares received by the other members. Once M^{τ} is known, each player compares it to the amount $\frac{\tau}{B_{\mathcal{T}_j}} T_{\mathcal{T}_j}$ and takes appropriate decisions based on the output of the comparison.

Verification of the game results: When the game period $B_{\mathcal{T}_j}$ expires, to verify the correctness of the reported results the meter of each player $p_i \in \mathcal{T}_j$ calculates the commitment $\gamma_i = h_1^{m_{p_i}^{B_{\mathcal{T}_j}}} h_2^{r_{p_i}}$. Note that such commitment is authenticated via a MAC generated by a tamper-proof device. Then, it sends to the player via the local HAN communication channel:

$$\mathrm{meter} \to p_i \colon \tau_{B_{\mathcal{T}_j}}, m_{p_i}^{B_{\mathcal{T}_j}}, r_{p_i}, \gamma_i, \mathrm{Mac}(k_{iU}^{(m)}, \tau_{B_{\mathcal{T}_j}} \| \gamma_i)$$

The result verification is then performed as follows:

6. CONSUMPTIONCHECK

$$p_i \to U \colon \tau_{B_{\mathcal{T}_j}}, \gamma_i, \mathrm{Mac}(k_{iU}^{(m)}, \tau_{B_{\mathcal{T}_j}} \| \gamma_i)$$

Each player forwards the commitment received from the local meter to the utility. U then multiplies the commitments received by all the team members to obtain the amount:

$$\Gamma_{\mathcal{T}_j} = \prod_{p_i \in \mathcal{T}_j} \gamma_i = h_1^{\sum_{p_i \in \mathcal{T}_j} m^{B_{\mathcal{T}_j}}} h_2^{\sum_{p_i \in \mathcal{T}_j} r_{p_i}}$$

Thanks to the homomorphic properties of PCS, the result is equal to the one that would be obtained by *first* summing the individual consumption measurements $m_{p_i}^{B_{\mathcal{T}_j}}$ and *then* hashing the aggregate value.

7. GAMEOUTCOME

$$p_i \to G \colon ID_i, \Gamma_{p_i}, \tau_{p_i}, \epsilon_{p_i}$$

At the end of the game the final result must be communicated to the game platform. To do so, each team member computes the commitment of the final team-aggregated consumption $\Gamma_{p_i} = h_1^{M^{B_{\mathcal{T}_j}}} h_2^{R_{\mathcal{T}_j}}$, where $R_{\mathcal{T}_j} = \sum_{p_i \in \mathcal{T}_j} r_{p_i}$ using the homomorphic PCS. Then it sends them to G together with the current timestamp τ_{p_i} and the challenge result ϵ_{p_i}, which is a bit set to 1 if $M^{B_{\mathcal{T}_j}} \leq T_{\mathcal{T}_j}$, to 0 otherwise.

As truthfulness check, for every player $p_i \in \mathcal{T}_j$, G computes the amount $\epsilon_{tot}^{\mathcal{T}_j} = \sum_{p_i \in \mathcal{T}_j} \epsilon_{p_i}$. If it holds that $\epsilon_{tot}^{\mathcal{T}_j} \neq 0 \wedge \epsilon_{tot}^{\mathcal{T}_j} \neq |\mathcal{T}_j|$ an alarm message is broadcasted to all the team members and the utility and the game is aborted. Moreover, G compares the values Γ_{p_i} received by each team member: if they are not all the same, the verification fails and the game is aborted.

8. ConsumptionVerification

$$U \to G \colon \Gamma_{\mathcal{T}_j}, \tau_U$$

For each team, U communicates to G the amount $\Gamma_{\mathcal{T}_j}$ previously computed and the current timestamp. G compares each value Γ_{p_i} received from the players to the value $\Gamma_{\mathcal{T}_j}$ received from the utility. If they are the same, then the winners are allowed to claim their rewards, otherwise the game is aborted.

V. Security Assessment

We now show that the security properties enumerated in Section IV-B are satisfied by our proposed gaming framework. Note that the correctness of the protocol is a direct consequence of the correctness of the homorphic aggregation protocol.

P1 The game platform G only receives public key parameters or messages encrypted with a symmetric key. To obtain information about the threshold or any consumption, G must be able to break either the Diffie-Hellmann key exchange or the symmetric encryption scheme, both of which are assumed to be hard to break.

P2 The utility U is involved in the verification steps and receives: the individual user commitments γ_i. Thanks to the hiding property of the commitment scheme, the γ_is reveal no information unless $h_2^{r_{p_i}}$ is known.

P3 The commitment scheme is computationally binding, meaning that it is hard to find two different measurements that yield the γ_i. Thanks to the homomorphic properties of the commitment, it is hard to find two different aggregate measurements that yield the same aggregate commitment $\Gamma_{\mathcal{T}_j}$. Since the commitments are authenticated by means of a tamper-proof device, the verification phase can be passed only by presenting the correct aggregate measurement and the correct $R_{\mathcal{T}_j}$.

P4 Under assumption that SSS is a perfect secret sharing scheme, it has been proved in [20] that it ensures unconditionally indistinguishable encryption for any collusion of $t^* < w$ participants. Therefore, assuming $w = |\mathcal{T}_j|$, unless the whole team colludes, each collusion $\mathcal{T}_{j^*} \subset \mathcal{T}_j$ learns no information from the individual shares $(x_i^{p_j}, y_i^{p_j})$ received from the other players $p_j \in \mathcal{T}_j \setminus \mathcal{T}_{j^*}$ during the computation of the team-aggregate consumption.

VI. Performance Assessment

We now assess the performance of our proposed privacy-friendly gaming framework in terms of data throughput and computational burden at each node. In the remainder of this Section, we assume that the infrastructure implements the standard AES symmetric cryptosystem operating in Counter mode (CTR). Note that, on input of a plaintext of m bits, the output of such cheme is $m + n$ bits long, where n is the nonce size. In Table VI we specify the assumptions on the bit length of the protocol parameters. Based on those, Table VI summarizes the sizes of the input/output data exchanged by each entity in every phase of the protocol execution. Results show that the data generated/received at the player side is limited to a few tens/hundreds of kilobytes, depending on the number of team members, thus being compatible also with resource-constrained devices such as portable devices. Conversely, the throughput of the game platform and the utility is more consistent due to the quadratic dependency on the cardinality of the team groups (e.g. 1000 users grouped in 50 teams of 20 members each lead to data volumes in the order of a few tens of Gbits). However, such entities are assumed to run the game application on dedicated servers with properly sized communication capabilities.

TABLE I
Assumptions on parameter sizes

Notation	Length (bits)	Notation	Length (bits)
ID_p	32	size of the subgroup used in commitments, q	256
C_p	1	symmetric encryption nonce size	128
B_p	4	size of the group used in DH and for commitment calculations, p	2048
ϵ_p	1	SSS modulus Q	64
$T_{\mathcal{T}}$	64	τ	32

TABLE II
Traffic Volume per Game Session [bits per execution]

		Input	Output
GameSelection	Player	-	2084
	Game Pl.	$2084 \cdot \lvert P\rvert$	-
	Utility	-	-
PlayerList	Player	-	-
	Game Pl.	-	$2084 \cdot \lvert P\rvert$
	Utility	$2084 \cdot \lvert P\rvert$	-
TeamList	Player	-	-
	Game Pl.	$2336 \cdot \lvert P\rvert + 2048 \cdot \lvert J\rvert$	-
	Utility	-	$2336 \cdot \lvert P\rvert + 2048 \cdot \lvert J\rvert$
GameGoals	Player	$2304 + 2080\lvert\mathcal{T}_j\rvert$	-
	Game Pl.	-	$\sum_{j\in J}(2304 + 2048\lvert\mathcal{T}_j\rvert) \cdot \lvert\mathcal{T}_j\rvert$
	Utility	-	-
Consumption Aggr.	Player	$1344 \cdot (\lvert\mathcal{T}_j\rvert - 1)$	$1344 \cdot (\lvert\mathcal{T}_j\rvert - 1)$
	Game Pl.	$\sum_{j\in J} 1344 \cdot \lvert\mathcal{T}_j\rvert(\lvert\mathcal{T}_j\rvert - 1)$	$\sum_{j\in J} 1344 \cdot \lvert\mathcal{T}_j\rvert(\lvert\mathcal{T}_j\rvert - 1)$
	Utility	-	-
ConsumptionCheck	Player	-	2208
	Game Pl.	-	-
	Utility	$2208 \cdot \lvert P\rvert$	-
GameOutcome	Player	-	2113
	Game Pl.	$2113 \cdot \lvert P\rvert$	-
	Utility	-	-
Consumption Verification	Player	-	-
	Game Pl.	-	$2080 \cdot \lvert P\rvert$
	Utility	$2080 \cdot \lvert P\rvert$	-

Finally, Table IV lists the computational burden at each node occurring during every protocol phase. The details of the computational cost of each operation are provided in Table III. Results shows that the game platform is not involved in any computation. Conversely, the utility performs computations only during the game setup and the results verification phases. The computational effort in terms of number of exponentiations linearly depends on the total number of players,

TABLE III
LIST OF COMPUTATIONAL COSTS

Notation	**Description**	**Computational Cost (number of multiplications/exponentiations)**
$C_m(x)$	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	$O(w^2) \cdot C_m(x)$
$C_l(x, w)$	cost of a share Lagrange interpolation modulo x using w shares	$O(w^2) \cdot C_m(x)$

TABLE IV
NODE COMPUTATIONAL LOAD

	Player	**Utility**
Setup	$2C_e(2048)$	$(\lvert P\rvert + 1) \cdot C_e(2048)$
Consumpt. Aggr.	$(\lvert\mathcal{T}_j\rvert - 1) \cdot C_e(2048) + C_s(64, \lvert\mathcal{T}_j\rvert) + C_l(64, \lvert\mathcal{T}_j\rvert)$	-
Verification	$2C_e(2048) + C_m(2048)$	$\sum_{j\in J}\lceil\log_2\lvert\mathcal{T}_j\rvert\rceil \cdot C_m(2048)$

whereas the number of multiplications exhibits a logarithmic dependency on the cardinalities of the player teams. However, such phases occur only once per game execution and the temporal horizon of each execution spans one or multiple days. Therefore, the protocol ensures scalability even in case of scenarios with several thousands of users (e.g. in case of involvement of all the citizens of a medium/large-sized town). Finally, at the player side, the most demanding phases is the consumption aggregation, where the computational complexity is dominated by the number of exponentiations, linearly depending on the team size. However, assuming that the teams are in the order of tens of users, a few tens of modular exponentiations are expected to be computed at every aggregation 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.

VII. Conclusions

This paper proposes a privacy-enhanced game platform aimed at encouraging players to reduce energy/water consumption in their households. To this aim, the platform implements team challenges against an unmanned adversary. A game communication protocol is described, which enables to execute the game without disclosing any individual consumption measurement and includes a set of correctness checks to detect cheaters. The security assessment of the proposed framework is discussed under assumption of honest-but-curious entities. Numerical evaluations of the computational burden and data exchange required by the protocol show that the framework is scalable up to several thousands of players.

VIII. Acknowledgements

Cristina Rottondi is partially supported by the *SmartH2O: an ICT Platform to leverage on Social Computing for the efficient management of Water Consumption* research project funded by the EU Seventh Framework Programme under grant agreement no. 619172. The authors thank Dr. Alessandro Facchini for the useful discussions and suggestions.

References

[1] T. Susi, M. Johannesson, and P. Backlund, "Serious games: An overview," School of Humanities and Informatics University of 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 Education*, vol. 27, no. 2, pp. 187–196, 2006.

[3] D. Thompson, T. Baranowski, R. Buday, J. Baranowski, V. Thompson, R. Jago, and M. J. Griffith, "Serious video games for health: how behavioral science guided the design of a game on diabetes and obesity," *Simulation & gaming*, 2008.

[4] T. Hirsch, "Water wars: Designing a civic game about water scarcity," in *Proceedings of the 8th ACM Conference on Designing Interactive Systems*, ser. DIS '10. New York, NY, USA: ACM, 2010, pp. 340–343. [Online]. Available: http://doi.acm.org/10.1145/1858171.1858232

[5] A. Bourazeri and J. Pitt, "Serious game design for inclusivity and empowerment in smartgrids," in *First International Workshop on Intelligent Digital Games for Empowerment and Inclusion*, 2013.

[6] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining gamification," in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*. ACM, 2011, pp. 9–15.

[7] A. Gustafsson, C. Katzeff, and M. Bang, "Evaluation of a pervasive game for domestic energy engagement among teenagers," *Computers in Entertainment (CIE)*, vol. 7, no. 4, p. 54, 2009.

[8] A. Rizzoli, A. Castellettib, A. Cominolab, P. Fraternalib, A. D. dos Santos, B. Storni, R. Wissmann-Alvese, M. Bertocchi, J. Novak, and I. Micheelg, "The smarth2o project and the role of social computing in promoting efficient residential water use: a first analysis," *International Environmental Modelling and Software Society (iEM... more*, 2014.

[9] R. McCall and V. Koenig, "Gaming concepts and incentives to change driver behaviour," in *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean*. IEEE, 2012, pp. 146–151.

[10] D. R. Michael and S. L. Chen, *Serious games: Games that educate, train, and inform*. Muska & Lipman/Premier-Trade, 2005.

[11] U. Ritterfeld, M. Cody, and P. Vorderer, *Serious games: Mechanisms and effects*. Routledge, 2009.

[12] 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 and Buildings*, vol. 42, no. 8, pp. 1329–1336, 2010.

[13] D. Martinovic, V. Ralevich, J. McDougall, and M. Perklin, "you are what you play: Breaching privacy and identifying users in online gaming," in *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*. IEEE, 2014, pp. 31–39.

[14] J. Schrammel, C. Köffel, and M. Tscheligi, "Personality traits, usage patterns and information disclosure in online communities," in *Proceedings of the 23rd British HCI group annual conference on people and computers: celebrating people and technology*. British Computer Society, 2009, pp. 169–174.

[15] 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-ICEC 2012*. Springer, 2012, pp. 586–593.

[16] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870 –1891, dec 1992.

[17] L. Galli, P. Fraternali, C. Pasini, G. Baroffio, A. Diniz Dos Santos, R. Acerbis, and V. Riva, "A gamification framework for customer engagement and sustainable water usage promotion," in *E-proc. of the 36th IAHR World Congress, The Hague, the Netherlands*, July 2015.

[18] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in CryptologyCRYPTO91*. Springer, 1992, pp. 129–140.

[19] M. Krohn, M. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in *Security and Privacy, Proceedings. IEEE Symposium on*, May 2004, pp. 226–240.

[20] C. Rottondi, G. Mauri, and G. Verticale, "A protocol for metering data pseudonymization in smart grids," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 5, pp. 876–892, 2015. [Online]. Available: http://dx.doi.org/10.1002/ett.2760