Temporal anonymity in the AMS scenario without a TTP

Sigurd Eskeland
Norwegian Computing Center
0314 Oslo, Norway
sigurd.eskeland@nr.no

ABSTRACT

Smart meters provide fine-grained electricity consumption reporting to electricity providers. This constitutes an invasive factor into the privacy of the consumers, which has raised many privacy concerns. Although billing requires attributable consumption reporting, consumption reporting for operational monitoring and control measures can be non-attributable. However, the privacy-preserving AMS schemes in the literature tend to address these two categories disjointly — possibly due to their somewhat contradictory characteristics.

In this paper, we propose an efficient two-party privacy-preserving cryptographic scheme that addresses operational control measures *and* billing jointly. It is computationally efficient as it is based on symmetric cryptographic primitives. No online trusted third party (TTP) is required.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**;

ACM Reference Format:
Sigurd Eskeland. 2018. Temporal anonymity in the AMS scenario without a TTP. In *12th European Conference on Software Architecture: Companion Proceedings (ECSA '18), September 24–28, 2018, Madrid, Spain.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3241403.3241462

1 INTRODUCTION

Traditional offline meters require manual readings that are supplied to the electricity suppliers on a coarse-grained basis, typically every month. By the introduction of advanced metering systems (AMS), smart meters allow two-way communication and automatic consumption reporting at short time intervals to the head-end systems of the electricity providers. (In the remainder of this paper we refer to electricity provider as *utility*). Availability of fine-grained measurements[1] increase the utilities' control of electric consumption and network loads, which allows utilities and grid operators to maximize their control and monitoring of consumed electricity with regard to billing and operational control measures, such as load monitoring and load management. At times when the collective consumption reaches peaks or lows in the distribution networks, it is desirable to smooth the peaks and lows to even the load distributions. *Demand response* is such a measure for load management, which are programs that offer consumers economic incentives in order to adapt their usage of electricity in response to wholesale market price signals.

Fine-grained measurements also allows dynamic billing regimes in accordance with hour-to-hour variable tariffs, which is not possible with traditional meters. In essence, the motivation for introducing smart meters is their capability of fine-grained measurements that provides increased and more precise billing and operational control.

Realtime monitoring and registration of electric usage constitute invasive factors into the privacy of the consumers, and there has been raised considerable concerns about the erosion of privacy that this causes [1].

Operational control measures (load monitoring, load management) and variable-tariff billing require fine-grained measurements, but the billing operation is carried out on a coarse-grained basis, like every month. Operational control measures are not concerned about the consumption of individual users, but rather total loads on individual lines and units in the network. Although there are control units at all levels in the power distribution grid, additional control is achievable by collecting fine-grained consumption measurements from users. As long as it is assured that individual measurements do not originate from specific identifiable users but from a specific group of users, cf. *anonymity sets* [2], the privacy of the individual users is protected. For instance, each user could be identified according the substation they are connected to, which is a number of users for each substation.

Attribution is the ability to identify the originator of a message that has been sent. Two key observations in the AMS scenario are that:

(1) Operational control measures do not require attributable consumption reporting.
(2) Billing must be attributable.

Privacy is attainable if measurements are non-attributable, while in order to carry out billing, measurements must be attributed to the pertaining users. These characteristics are therefore somewhat contradictory. Most papers that address privacy in the AMS scenario focus on privacy-preservation with regard to either operational control or billing. Few authors address both cases combined. Those that do, do this in such a way that billing and operational control are handled disjointly. By this we mean that the proposed privacy measures for both areas are disjoint, resulting in hybrid schemes (e.g., [3, 4]).

Smart meters report merely quantities of consumed electricity. AMS measurements are perhaps less sensitive in nature than other

[1]The terms *measurement* and *consumption value* are used interchangeably in this paper.

ECSA '18, September 24–28, 2018, Madrid, Spain

ACM ISBN 978-1-4503-6483-6/18/09…$15.00
https://doi.org/10.1145/3241403.3241462

types of personal data, like personal health data, information about imprisonments and penalties, economical misconduct, etc. Electricity consumption data are rather transitory in nature and may therefore only carry limited sensitivity or have even no interest as time passes, while the sensitivity levels of the latter keep rather steadily up as time passes. Measurements that are non-recent do not reveal current actions and activities in households, and may therefore have less interest and sensitivity. AMS measurement sensitivity is therefore limited by a time factor.

Contribution. In this paper we propose a two-party privacy-preserving cryptographic scheme that involves a smart meter and the utility. There is no online third trusted party (TTP). The scheme addresses operational control measures *and* billing jointly. The goal is to protect user privacy with regard to the utility for both operational control measures *and* billing. The proposed scheme assures time-bound non-attributable fine-grained consumption measurements in correspondence with operational control. By the time of billing, the reported consumption measurement values are made attributable to the utility by action of the smart meter. By this measure, user privacy is assured within a periodical basis. The scheme is computationally efficient as it is based on symmetric cryptographic primitives.

2 RELATED WORK

2.1 Background

In the literature, most privacy-preserving schemes in the AMS scenario relate to privacy in the context of electric consumption measurement, and address privacy in conjunction with operational control measures or billing. A given AMS privacy-preserving scheme may address one or both categories.

AMS privacy-preserving schemes are designed to be aligned with characteristics such as

(1) Attribution
(2) Frequency

Attribution pertains to whether measurements are attributable to a specific smart meter and user or not. Measurements must be attributable for the utility to carry out billing, unless the billing is carried out at the user side, for instance by trusted devices such as trusted platform modules (TPM). As noted, attribution is not necessary for operational control purposes. Attribution is equivalent to the privacy properties *linkability* and *unlinkability*. There is linkability when measurements are attributable to a specific smart meter, and unlinkability when not. In the privacy literature, unlinkability (non-attribution) is a typical privacy goal.

Frequency refers to the frequency of measurements and reporting, such as coarse-grained and fine-grained. This is a rather conditional and functional property that influences the degree of privacy in cases where measurements are attributable.

2.2 Related work

As noted in the introduction, operational control measures do not require attributable consumption reporting, while billing must be attributable. These characteristics are somewhat contradictory, and most papers that address AMS privacy address either privacy-preserving operational control or privacy-preserving billing. In this section, we will briefly review some privacy-preserving AMS schemes for both categories. For a survey, see for instance [5].

2.2.1 (Attributable) privacy-preserving billing. In the AMS scenario, billing assumes fine-grained measurements. The overall privacy goal is to give users assurance that their measurements are not made attributable to the utility, while the utility does not necessarily trust the end users. In the literature, essentially three approaches are proposed:

(1) Meter-side billing computation by means of trusted platform modules
(2) Utility-side correctness verification of meter-side billing computations by means of homomorphic cryptographic commitments
(3) Utility-side billing computation by means of a trusted third party

User privacy is obtained as long as measurements are not attributed to the user. The two first approaches suggest billing computation at the smart meter, which hides measurements from the utility. Privacy is therefore assured, but requires that the billing computations are correct (i.e., assurance that the user did not cheat) and that the transmission of the billing amount is secure. In the third approach, attributable measurements *are* disclosed, but by sending them to a TTP that does not reveal them to the utility, privacy is obtained with regard to the utility.

Petrlic et al. [6] proposed to use trusted platform modules (TPM) integrated in smart meters for billing computation. No measurements are sent from the meter. The goal is to ensure the utility that the billing operations are correctly carried out, since the utility does not necessarily trust the users. This requires that price information must be securely transmitted from the utility and that the resulting amount information is securely transmitted from the TPM to the utility.

Billing computation correctness verification pertains to meter-side billing computation when no TPM is used, and is based on cryptographic commitments. As before, the goal is to ensure the utility that the billing operations are correctly carried out, since the utility does not necessarily trust the users. Instead of sending measurements to the utility, the smart meter provides a proof (i.e., a commitment) to the utility for each measurement value, without revealing the actual measurement. At the end of the billing period, the meter computes and sends the billing amount to the utility. The already received commitments act as proof that the bill was computed correctly, providing assurance that the user did not cheat. Hence, the received billing amount is verifiable to the utility.

The idea is that for each measurement c, the smart meter sends a commitment C that is computed from c and a secret random value r. Given a commitment C it is hard to compute c and r. At the time of billing, the smart meter computes and releases the dot-product r' of the random values and tariff vector. Due to homomorphicisms of commitment schemes, the utility uses r' conjunction with each commitment C and the tariff vector to verify that the billing price is correct. Commitment-based billing schemes are proposed in [7] and [8].

Billing could alternatively be carried out by the assistance of a trusted third party (TTP). A straight-forward variant is that the smart meters authenticate and forward their consumption values

to the TTP, which then computes the charging price that it forwards to the utility. Efthymiou et al. [3] proposed using a TTP for both billing and operational control measures. Each smart meter is assigned two distinct long-term identifiers — one anonymous identifier (pseudonym) for fine-grained (high-frequency) measurement reporting and one non-anonymous "regular" identifier for coarse-grained (low-frequency) measurement reporting. Since the TTP that knows the mapping between these two identifiers, the TTP becomes a focal point of trust, with disadvantages such as vulnerability to insider threats.

2.2.2 (Non-attributable) privacy-preserving operational control. The following approaches have been proposed for privacy-preserving operational control:

(1) Privacy-preserving aggregation
(2) Group signatures
(3) TTP (pseudonyms)

The overall privacy goal is to give users assurance that their measurements are not made attributable to the utility. Non-attribution requires that there must exist a number of possible meters that measurements can originate from, which is related to the terms *anonymity sets* and *anonymity networks*. As previously noted, an other suggested approach is including an online trusted third party that both users and utility trust in.

A secondary goal that is sometimes not explicitly highlighted in the privacy literature, is to provide the utility assurance that received measurements are authentic. Schemes that assume anonymity sets, such as privacy-preserving aggregation schemes and group signatures, may give the utility assurance that measurements (or sums of measurements) originate from a confined group of users. In this paper, this property is addressed in Section 3.2 under authenticity and unforgeability.

Privacy-preserving aggregation schemes are secure-sum schemes that are non-attributable and that provide consumption aggregates from groups of smart meters. Aggregation schemes should assure privacy despite certain numbers of colluding parties, including the utility. There are mainly two types of privacy-preserving aggregation schemes:

(1) Distributed/partial aggregation
(2) Centralized aggregation

Distributed aggregation refers to that each smart meter randomly splits measurement values and distributes the partial measurements to the other meters, so that each meter computes a partial sum. The partial sums are eventually transmitted to the utility [9–11] or to the other meters [12] that compute(s) the total sum by aggregating the partial sums. The mentioned aggregation schemes use homomorphic encryption such as the Pailler scheme as a cryptographic primitive. A problem is that such schemes generally do not explicitly give the utility authenticity assurance, which makes them susceptible to attacks such as replay attacks unless relevant security measures are taken, for instance by digital signatures or message authentication codes (MAC).

In centralized privacy-preserving aggregation, only a centralized entity such as the utility carries out the sum computation. Since it is not trusted, the measurements are encrypted in such a way that the utility is unable to obtain individual measurements. In the scheme of Joye et al. [13], the secret key of the utility is randomly split into n secret shares that are unknown to the utility, and where each meter holds a share that it uses to encrypt measurements with. Due to its homomorphic property, the utility computes the sum using its secret key. Since the scheme assumes a fixed group of meters, joining or leaving meters require a full key/share redistribution for all meters. The scheme in [14] overcomes this disadvantage, but requires a trusted third party. Both schemes employ timestamps and have therefore non-reusability/freshness assurance.

Group signatures provide proof that the signer is associated with a group, but does not reveal the identity of the signer. Group signature schemes have a feature that allows a group manager to reveal the original signer. For the purpose of operational control measures, group signatures provide unlinkability for smart meters that continually transmit fine-grained measurements to a utility [15, 16]. Group signatures can also be used for billing, but then the utility's billing center has the authority to reveal signers [17], in which case the billing center has the equivalent role of a trusted third party and becomes a focal point of trust. Another downside is that group signatures are computational intensive.

Some authors propose using pseudonyms as a means for anonymization and privacy [18]. In order for a pseudonym to be trustable, it must be verifiable. This could be realized by anonymous certificates, which requires a trusted third party. Schemes using anonymous certificates are found in [3, 6]. Downsides are that this requires a trusted third party that knows the pseduonym/meter-relation, and that certificate-based pseudonyms are static, which may cause weakened unlinkability. Another disadvantage is that certificates requires asymmetric cryptography which is considerable more computational intensive than symmetric cryptography.

3 THREAT MODEL AND PROPERTIES

In this section we introduce a threat model, which is essential to what properties are necessary to for the scheme These properties are then introduced next. The goal is a scheme that is resistent to these threats.

3.1 Threat model

The main goal is to preserve user privacy with regard to the utility. This is a privacy goal that is asymmetric, since the utility does not submit personal information to the users. In the metering scenario, a possible threat is that some users may attempt to cheat their electricity suppliers. Since the utility requires correct measurements, a second goal is to assure the utility that measurements are authentic considering cheating users or adversaries. Threats we consider relevant are:

- Honest-but-curious utility
- Dishonest users
- External adversaries

We assume an *honest-but-curious* utility that do not deviate from the defined protocol, but will attempt to learn all information possible from the received messages. Smart meter systems rely on wireless communication, which constitutes an insecure communication channel. An advanced user may therefore be capable to

replay former messages or to create valid messages with false consumption values for the purpose of cheating the utility. This is equivalent with an active external adversary that is able to modify messages that are in transmission.

We assume that cryptographic keys are securely stored in the smart meter and are inaccessible to any user (or adversary) w.r.t. reading and writing.

3.2 Privacy properties

Anonymity is the state of being not identifiable within a set of subjects. Anonymity may be defined as unlinkability between an identifier of a subject, that is a sender, and the messages that are sent by that subject. More specifically, we can describe the anonymity of a message such that it is not linkable to any identifier, and the anonymity of an identifier as not being linkable to any message [2].

Temporal unlinkability This is a privacy property that prevents that measurements can be attributed to specific smart meters until a given time. At the end of the billing period and at the behest of the smart meter, the utility is given the capability to attribute measurement messages to the corresponding smart meters. The measurements remain non-attributable to any other party than the utility.

Authenticity and unforgeability At the end of the billing period, the utility must have assurance that each measurement message is *authentic*. An authentic message has the following characteristics:

- It originates from the alleged meter
- It has not been altered

To achieve this, the authentication mechanism must be unforgeable.

Non-reusability/freshness Assurance that a measurement message is unique and recent.

Integrity protection is a security measure that provides integrity, i.e., a means of detecting if messages have been altered by an adversary during transmission.[2] Message authentication (also known as *data origin authentication*) is the property of assurance that a given entity is the original source of received data. Message authentication gives assurance of data integrity, but not the other way around. This is because that if there is no data integrity assurance then we cannot be sure that data received has not been changed by an attacker in transit and it would not be possible to have any assurance about the originator of the data. See for instance Martin [19, Chapter 1.3]. The authentication mechanism must be *unforgeable* to prevent a user or an adversary from computing cryptographically valid authentication codes for false measurement messages.

Message authentication codes (MACs) and digital signatures are generic authentication mechanisms that allow a recipient to correctly verify the originator. These security measures alone do not provide assurance of the recentness or freshness of received messages, which is necessary to prevent replay attacks.

Non-reusability/freshness is the assurance that a message originated *recently* from an authenticable smart meter at the time it was received. This gives assurance against replay attacks and that a message is new and not used before, and assumes measures such as nonces, counters or timestamps in conjunction with an authentication mechanism. This is equivalent to *entity authentication*, which is normally associated with cryptographic protocols for user authentication and key establishment, and which is assurance of "liveness" — that a given entity is currently active in a communication session.

A common security property is confidentiality, which is assurance that data cannot be viewed by an unauthorized entity that may be eavesdropping on communications. This is not addressed explicitly in this paper, which focuses on privacy. However, due to the *temporal unlinkability* privacy property, it is prevented that communicated measurements can attributed to specific smart meters, except to the utility at billing time. Confidentiality is in this regard weakly provided. Utilizing cryptographic measures such as public key encryption provide confidentiality.

4 THE TEMPORAL ANONYMITY AMS SCHEME

4.1 Protocol specification

The scheme has two phases — installation and operation. The installation phase may refer to the time of production or the time of roll-out, when long-term cryptographic keys are stored at the smart meters.

Installation. Each smart meter SM_i and the utility U preshare a long-term secret symmetric key k_{iU}.

Operation. The operational phase constitute recurrent sessions that each equals a billing period T and that has a duration of, for instance, one month. Each session has an *initial step* followed by fine-grained *measurement reporting* at fixed time intervals $1 \leq t \leq p$, for instance every hour, where t is a counter or a timestamp, and p is the number of intervals of each period T. The billing period is completed by a *billing computation* step.

In order to complete billing computation at the end of T, it is necessary that the utility U continuously stores all the messages it receives during T in a *measurement table*.

In order to have anonymity, there has to exist an *anonymity set*, which is the set of all possible subjects. The larger an anonymity set is and the more evenly distributed that the members of that set are, the stronger is the anonymity [2]. In the AMS context, an anonymity set is a group of smart meters that report to the same utility, which assumes that each smart meter is assigned an anonymity set. The measurement table is consistent with a anonymity set, and the size of the anonymity set would therefore determine the size of the measurement table.

In practice, the group of smart meters corresponding to an anonymity set could be those that are associated and communicates with a concentrator. The concentrator is an intermediate communication point that forwards messages between a cluster of smart meters that are within radio range of the concentrator, and the utility's head-end system.

Initial step. At the start of each new billing period T, each smart meter SM_i randomly generates a secret temporary anonymity token at_{iT}, which applies to that billing period T only. Each message that

[2]Since digital messages are merely bit sequences, these measures do not *prevent* alteration of data, but provide a means of detecting intended (or unintended) message altering.

SM_i sends is identified by a unique non-attributable message identifier mid_{it}. All non-attributable message identifiers are deduced by means of the temporary anonymity token at_{iT} in conjunction with a hash function (cf. Eq. 1).

Measurement reporting. At each time interval $t, 1 \leq t \leq p$, each SM_i reports the current measurement to the utility. First, it computes the non-attributable message identifier

$$mid_{it} = h(at_{iT}, SM_i, t, T) \tag{1}$$

where h denotes a secure hash function. Since hash functions have a oneway security property, it is prevented that the secret anonymity token at_{iT} can be revealed given the pertaining non-attributable message identifiers mid_{it}.

The SM_i sends the message

$$SM_i \rightarrow U: \quad mid_{it}, c_{it}, t, ac_{it} \tag{2}$$

to U, which stores it in the measurement table, and where c_{it} is the consumption value and $ac_{it} = h(at_{iT}, mid_{it}, c_{it}, t, T)$ authenticates the message contents. Note that since this message is not attributable, it contains no information about the sender.

Billing computation. At the end of the billing period T, the utility needs to attribute each measurement received during T to the pertaining smart meter. To do this SM_i encrypts and sends at_{iT}, as

$$SM_i \rightarrow U: \quad SM_i, E_{k_{iU}}(SM_i, T, at_{iT}) \tag{3}$$

to U, where E denotes encryption using a secure symmetric cryptographic algorithm. Since k_{iU} is shared by only U and SM_i, upon decryption U gets assurance that the message originated from SM_i and applies to the billing period T.

By means of at_{iT}, the utility U computes

$$\text{mid}'_{it} = h(at_{iT}, SM_i, t, T) \quad \text{for} \quad 1 \leq t \leq p \tag{4}$$

and searches for these values in the measurement table. For each match, i.e., $mid'_{it} = mid_{it}$, the utility marks the corresponding entry with SM_i as the originator.

Next, the contents of each received measurement message must be authenticated. The utility computes the authentication code

$$ac'_{it} = h(at_{iT}, mid_{it}, c_{it}, t, T) \tag{5}$$

using at_{iT}, and checks whether $ac'_{it} = ac_{it}$. A match indicates that the measurement message is authentic and that it originated from SM_i at time interval t during billing period T.

When all entries in the measurement table linked to SM_i have been identified, the utility computes the amount b_T to be charged for that period. This computation is a dot-product of the measurement vector $\mathbf{c}$ and the tariff rate vector $\mathbf{r}$:

$$b_T = \mathbf{c} \cdot \mathbf{r} = \sum_{t=1}^{p} c_{it} r_{it} \tag{6}$$

where r_{it} is the tariff rate for SM_i at time t.

4.2 Notes

The non-attributable message identifiers mid_{iT} reference each consumption message (cf. Eq. 2). When SM_i releases the temporary anonymity tokens at_{iT} by the end of the pertaining billing period T, the utility is able to correlate the pertaining messages that it has received during T to SM_i in order to compute the bill.

This should not be confused with cryptographic commitments, e.g. [20], which are a means for verifying the correctness of a computation that was carried out by some other entity when releasing a decommitment value. Another significant difference is that commitments are homomorphic, and have no identifying and authenticating properties.

It could be pointed out that temporary anonymity tokens are somewhat similar in nature to pseudonyms. A difference is that pseudonyms are normally public, while the anonymity tokens are secret and eventually revealed to the utility. Another difference is that pseudonyms are usually static, while the anonymity tokens have temporal applicability.

4.3 Security analysis

The scheme is based on the following cryptographic hardness assumptions:

(1) The *pre-image resistance* property of hash functions assures that given a hash value h' it is difficult to find any input m, where $h' = h(m)$.
(2) The following hardness properties of a secure symmetric cryptographic algorithm E are relevant for the scheme:
   (a) Resistance to *known plaintext attacks* assures that given a plaintext m it is not possible to find the ciphertext c', where $c' = E_k(m)$.
   (b) Given an adversary that has a number of plaintexts/ciphertexts encrypted by the same key. Resistance to *known ciphertext attacks* assures that given another ciphertext c' it is not possible to find the plaintext m or the secret key k, where $c' = E_k(m)$.

A presupposed security assumption that should be pointed out is that temporary anonymity tokens at_{iT} must be random in a sufficiently large search space. If not, an attacker could successfully find at_{iT} by brute-force searches which would break the scheme.

The following shows the how the privacy properties stated in Section 3.2 are ensured in agreement with the stated hardness assumptions.

Temporal unlinkability. Each measurement message (cf. Eq. 2) are broadcasted and can be known by any eavesdropper. It contains the message identifier mid_{it} that is computed from the randomly selected temporary anonymity token at_{iT}, which is only known by the smart meter SM_i until it is securely released to the utility U at billing time (Eq. 3). Since at_{iT} is random, successful brute-force searches are prevented. Therefore, in agreement with hardness assumption 1, it is prevented that the hash function input corresponding to mid_{it}, i.e., (at_{iT}, SM_i), can be revealed given any number of pertaining anonymous message identifiers mid_{it}. It is therefore prevented that measurement messages can be associated with SM_i given that at_{iT} is unknown. Temporal unlinkability is therefore assured.

Authenticity and unforgeability. At billing time, the utility U decrypts the ciphertext received in Eq. 3 using k_{iU}, and obtains $(SM_i,$

T, at_{iT}). The ciphertext, which contains the temporary anonymity token at_{iT}, is authentic if SM_i is valid and T is as expected.

Due to the randomizing property of hash functions, each non-attributable message identifier mid_{it} has high entropy and is equivalent to an unpredictable, pseudo-random value. By means of at_{iT}, the utility restores each pertaining mid_{it}. Looking up these values in the measurement table, each match identifies the corresponding measurement messages that have been sent by SM_i during the billing period T. Due to the high entropy, the probability of false matches is negligible (cf. hardness assumption 1). A matching mid_{it} value found in the measurement table means that it is therefore authentic.

Lastly, by means of at_{iT} and ac_{it}, the utility is able to authenticate measurement messages with regard to (mid_{it}, c_{it}, t, T).

Consider the following possible attack cases:

(1) Given a number of measurement messages (cf. Eq. 2) for a given billing period T and SM_i, a user or adversary could attempt to obtain at_{iT} for each (mid_{it}, ac_{it}) of those messages. If successful, the user could subsequently submit altered measurement messages to the utility having cryptographically valid (mid'_{it}, ac'_{it}) based on at_{iT}.
Since at_{iT} is random and has a high entropy, it is prevented that at_{iT} can be revealed given any number of (mid_{it}, ac_{it}) by brute-force searches and in agreement with hardness assumption 1.

(2) Given a measurement message (cf. Eq. 2), a user or adversary could attempt to replace it by a partly modified message whose modified content agree with the authentication code ac_{it} of that message.
According to hardness assumption 1, the pre-image resistance property of hash functions assures that given a hash value h' it is difficult to find any input m, where $h' = h(m)$. Therefore, this attack is prevented.

(3) A user or adversary could select an arbitrary at'_{iT}, whereof he or she can deduce cryptographically valid (mid'_{it}, ac'_{it}) in order to submit fake measurement messages to the utility.
Not knowing the secret key k_{iU}, the user would then have to compute a cryptographically valid ciphertext $E_{k_{iU}}(SM_i, T, at'_{iT})$ in agreement with Eq. 3, containing a valid identifier SM_i, a valid timestamp T and that at'_{iT}. This attack is prevented in agreement with hardness assumption 2a.

In agreement with the hardness assumptions of the cryptographic algorithms, the utility is therefore assured that the pertaining measurement messages originate from SM_i and pertains to the time interval t of billing period T. Hence, authenticity and unforgeability is assured.

Non-reusability/freshness. This is assured in agreement with the previous analysis *(authenticity and unforgeability)* by means of the timestamps/counters t, T.

Since k_{iU} is shared by only the utility and SM_i, it is prevented that the temporary anonymity token at_{iT} can be disclosed to eavesdroppers — in agreement with hardness assumption 2b. This confines the knowledge of specific users' consumption to the utility only.

5 CONCLUSION

Fine-grained consumption measurements provide increased operational monitoring and control and more precise billing, but constitute an invasive factor into the privacy of the consumers. In this paper, we have proposed a two-party privacy-preserving cryptographic scheme that addresses operational control measures *and* billing jointly. In contrast, the privacy-preserving AMS schemes in the literature tend to address these two categories disjointly — possibly due to their somewhat contradictory characteristics.

Electricity consumption data are rather transitory in nature and may therefore only carry limited sensitivity or have even no interest as time passes. Measurements that are non-recent do not reveal current actions and activities in households. AMS measurement sensitivity is therefore limited by a time factor. The proposed scheme assures that fine-grained consumption measurements are non-attributable during the billing periods. By the time of billing, the reported measurement values are made attributable at the utility by action of the smart meter, and are then eligible for billing computation. This assures user privacy within a periodical basis.

The proposed scheme is computationally efficient as it is based on symmetric cryptographic primitives. No online trusted third party is required.

6 ACKNOWLEDGEMENTS

This work was partially supported by the project IoTSec – Security in IoT for Smart Grids, with number 248113/O70 part of the IKTPLUSS program funded by the Norwegian Research Council.

REFERENCES

[1] Patrick Collinson. Is your smart meter spying on you? The Guardian, https://www.theguardian.com/money/2017/jun/24/smart-meters-spying-collecting-private-data-french-british, 24 June 2017. Accessed: 2018-06-20.
[2] Andreas Pfitzmann and Marit Hansen. Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology. Technical report, TU Dresden, 2005.
[3] Costas Efthymiou and Georgios Kalogridis. Smart grid privacy via anonymization of smart metering data. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 238 – 243, 11 2010.
[4] F. Borges, D. Demirel, L. Böck, J. Buchmann, and M. Mühlhäuser. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In *2014 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6, June 2014.
[5] S. Finster and I. Baumgart. Privacy-aware smart metering: A survey. *IEEE Communications Surveys Tutorials*, 16(3):1732–1745, Third 2014.
[6] Ronald Petrlic. A privacy-preserving concept for smart grids. In *Sicherheit in vernetzten Systemen: 18. DFN Workshop*, pages B1–B14. Books on Demand GmbH, 2010.
[7] Marek Jawurek, Martin Johns, and Florian Kerschbaum. Plug-in privacy for smart metering billing. In *Proceedings of the 11th International Conference on Privacy Enhancing Technologies*, PETS'11, pages 192–210, Berlin, Heidelberg, 2011. Springer-Verlag.
[8] Alfredo Rial and George Danezis. Privacy-preserving smart metering. In *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society*, WPES '11, pages 49–60, New York, NY, USA, 2011. ACM.
[9] Flavio D. Garcia and Bart Jacobs. *Privacy-Friendly Energy-Metering via Homomorphic Encryption*, pages 226–238. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
[10] Tobias Klenze. Privacy strategies in smart metering. 2014.
[11] Tassos Dimitriou and Mohamad Khattar Awad. Secure and scalable aggregation in the smart grid resilient against malicious entities. *Ad Hoc Netw.*, 50(C):58–67, November 2016.
[12] Zekeriya Erkin and Gene Tsudik. *Private Computation of Spatial and Temporal Power Consumption with Smart Meters*, pages 561–577. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
[13] Marc Joye and Benoît Libert. *A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data*, pages 111–125. Springer Berlin Heidelberg, Berlin,

Heidelberg, 2013.

[14] Iraklis Leontiadis, Kaoutar Elkhiyaoui, and Refik Molva. *Private and Dynamic Time-Series Data Aggregation with Trust Relaxation*, pages 305–320. Springer International Publishing, Cham, 2014.

[15] S.H.M. Zargar and M.H. Yaghmaee. Privacy preserving via group signature in smart grid. In *Proceedings of the Electric Industry Automation Congress (EIAC)*, February 2013.

[16] H. Kishimoto, N. Yanai, and S. Okamura. An anonymous authentication protocol for smart grid. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 62–67, March 2017.

[17] D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu. An enhanced public key infrastructure to secure smart grid wireless communication networks. *IEEE Network*, 28(1):10–16, January 2014.

[18] S. Afrin and S. Mishra. An anonymized authentication framework for smart metering data privacy. In *2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, Sept 2016.

[19] Keith M. Martin. *Everyday cryptography: Fundamental Principles and Applications*. Oxford University Press, Oxford, 2012.

[20] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '91, pages 129–140, London, UK, UK, 1992. Springer-Verlag.