Verifiable Certificateless Signcryption Scheme for Smart Grids

Mohammed Ramadan*, Ghada Elbez, Veit Hagenmeyer
Institute of Automation and Applied Informatics (IAI)
KASTEL Security Research Labs
Karlsruhe Institute of Technology (KIT)
Eggenstein-Leopoldshafen, Germany
(mohammed.ramadan, ghada.elbez, veit.hagenmeyer)@kit.edu

***Abstract*—Smart Grids (SG) are potential replacements for older power grids, capable of adapting and distributing energy based on demand. The recent technological advances and the increased dependence on electrical energy are all factors in the increased need for reliable and efficient energy systems. The complexity of the smart grid arises from using various components and the high requirements for real-time reliable two-way communication. Accordingly, this represents additional security and privacy challenges. In this paper, we proposed a security and efficient certificateless signcryption scheme with flexible verifiability properties using equality test techniques for Advanced Metering Infrastructure (AMI) within the SG; abbreviated CL-SG. The proposed scheme provides privacy-preserving, confidentiality, data integrity, verifiability, and reduces the level of trust in the third party (e.g., central unit, substation, data concentrator, etc.). The performance evaluation regarding security and complexity analysis shows that the proposed scheme is secure and efficient with good functionality to be fully adopted and implemented within SG. Also, an extended future work is presented to add more flexibility and security properties and features to the current proposed model.**

***Index Terms*—Smart Grids, Smart Metering, Certificateless, Signcryption, Equality Test.**

I. Introduction

Energy systems are considered one of the critical infrastructures that any cyber-attacks or data breach can lead to major effects on national security, economy, and society. Securing distributed energy systems such as smart grid (SG) and supervisory control and data acquisition (SCADA) is a challenge, there are significant potential unresolved challenges such as privacy, transparency, data integrity, and confidentiality [1].

The power system is divided into balancing areas that are connected by tie lines to facilitate the exchange of power. Each balancing area has a control center in which the automatic generation control (AGC) application runs as a part of the energy management system (EMS). The AGC received measurements from remote sensors via inter-control center communication protocol (ICCP) [2]. However, there are several attack scenarios on the control system such as scaling, pulse, rump, and random attacks. These attacks aim to modify true measurements in different ways [3].

The general energy systems architecture (See Fig. 1) is the spatial, topological, and functional organization of energy entities and subsystems including energy resources, generation, conversion, transmission, distribution, and storage systems [4].

Advanced Metering Infrastructure (AMI) is widely adopted and integrated within smart grids and smart meter is a core entity in AMI and SG. Advances in the interconnection between the different SG components introduce increasing cyber-attack vectors. In particular, the ability to maintain the confidentiality, integrity, and availability of data is a major challenge. Cryptography is a powerful tool that can be utilized to protect SG and AMI from different cyber-attacks [5].

The security requirements for AMI are mainly due to the vulnerable infrastructure and the difficulties on how to keep data confidential within AMI and the whole power grid as well as providing a trustworthiness metering and communication systems between end-entities central units and customers. Also, impersonating attacks and denial of service attacks (DoS) are well-known vulnerabilities in which the remote command, e.g., connect/disconnect commands can be used for impersonating the central unit by applying a DoS on the smart meter unit [3]. AMI components are distributed in several network topologies and heterogeneous levels including intelligent electronic devices (IED), home area networks (HAN), neighbor area networks (NAN), and wide area networks (WAN). This is challenging when applying authorization and access control techniques. Nevertheless, many other vulnerabilities were found in AMI and smart metering (SM) systems such as structured query language (SQL) injection, DoS, replay, and man-in-the-middle attacks (MITM). Confidentiality and privacy-preserving are among the most important security requirements for AMI and SG [6].

A. Cryptographic background

The proposed CL-SG model is based on certificateless and signcryption primitives with equality test verification. The following paragraphs are some related cryptographic concepts that are been utilized for the proposed CL-SG model.

Identity-based cryptography (IBC) was first introduced in 1985 by Shamir [7]. The basic concept of IBC is that the public

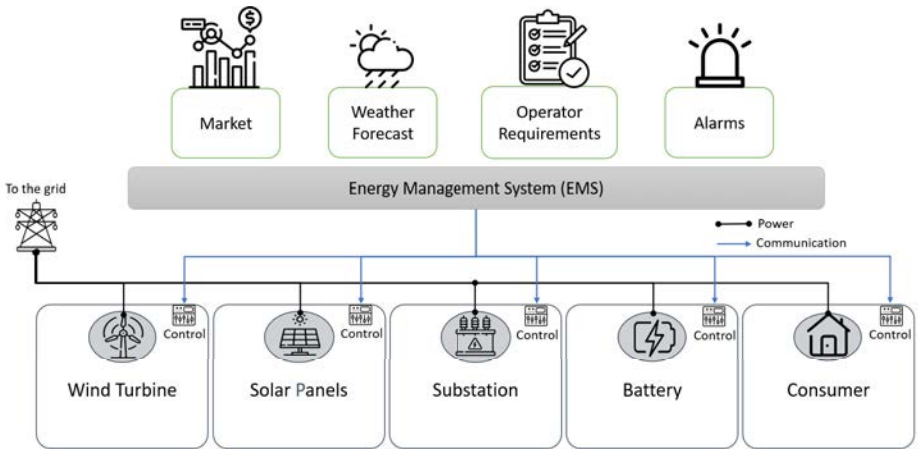

Fig. 1. Energy Management System (EMS) - General Architecture.

key of a user can be an arbitrary string identity (i.e. name, email, address, etc.) that uniquely identifies a specific user and cannot be deniable. Certificateless public-key cryptography (CL-PKC) was first formalized by Al-Ryami and Paterson [8]. The idea of CL-PKC is constructed based on IBC for the public key is users' unique identifiers. However, CL-PKC provides a solution to the well-known key escrow problem, in which the third-party key generation center (KGC) can only issue a partial private key instead of a private key, and the full private key will be extracted from the shared partial private key at a later step.

Signcryption was first introduced by Zheng et al. [9] and found its way into most applications where public key cryptography was used to provide both authentication and confidentiality simultaneously. A proxy signcryption scheme; was first introduced by Gamage et al. [10]; is to realize two functions of public key encryption and proxy signature by a delegation of some computation capabilities within the algorithm to a proxy third party.

The first public key encryption with an equality test (PKEET) was introduced in 2010 by Yang et al. [11], is to enable an equality test process on encrypted data using public keys. In PKEET schemes, each user generates a trapdoor for equality tests to a third party called the equality tester, then can check the equality among several ciphertexts without disclosing confidential information.

B. Related Work

Information and communications technology (ICT) is widely utilized in energy systems. The importance of ICT in energy systems is to provide reliable communication and real-time tracking of power flow including generation and consumption. These needs brought some vulnerabilities to the power grid and attracted research work that is attempting to fill this gap [12]. Besides, the malicious attacks between smart metering units (MU) and central units (CU) by modifying the collected data have been one of the key challenges in SG, such attacks show 6 billion USD of loss only in the United States [13]. This leads to redirecting the focus on research and development regarding secure SG systems.

There are several research works have been conducted to provide security solutions for AMI and SG. For instance, authentication and key agreement protocols (AKA) for distributed SG and SCADA systems have been comprehensively researched recently as in [14]; Zhang et al. proposed a lightweight AKA using symmetric cryptography. This scheme provides anonymity for the smart grid and is proven secure against several attacks such as replay attacks. However, this scheme supports two-party authentications other than authenticating all nodes in the smart grid. Odelu et al. [15] proposed a provably secure authenticated key agreement scheme for the smart grid architecture. However, the scheme has been cryptanalyzed and is vulnerable to ephemeral secret leakage attacks under the Canetti-Krawczyk CK adversary [16]. On the other hand, demand-response in a smart grid is a method to manage and control electricity, also used to help customer reduce their power consumption. Authentication techniques of demand-response that use different demand-response methods when changing the power suppliers by the primary grid is a challenging security requirement and have been investigated recently [17] [18].

Energy management systems (EMS) have a great impact on the advanced energy systems for the functions and operations of energy generation, balancing, control, storage, and distribution considering different energy sources. The EMS relies on advanced information and communication technology (ICT), which leads to security and privacy issues [19]. Several research approaches considered the security of the control system (e.g., SCADA). Mostly, to achieve security by isolation techniques for multiple small-scale management subsystems or in a grid that is connected to the power distribution system. For the security of EMS, Park et al. [20], proposed that the new standards for cyber security should combine the CIA triad with critical safety requirements for industrial control systems (ICS). Furthermore, EMS systems have other security issues, e.g., using outdated software and operating systems,

which multiple vendors do not support. Also, there are several proposed approaches [21] [22] have been proposed regarding the access control for EMS and SCADA systems using, e.g., decision tree-based IDS to detect cyber-attacks.

Also, there some important research works have been proposed for SG utilizing certificateless cryptography within SG [23] [24] as well as using signcryption techniques [25] [26]. These approaches mostly focused on smart grids from a high-level perspective providing confidentiality, authentication, or access control with less flexibility and functionality regarding the system requirements to be actually implemented within SG.

C. Contributions

The proposed scheme is a secure certificateless signcryption with equality test verification. In this paper, we mainly focus on achieving some security properties within smart grids and smart meters such as confidentiality, privacy, authenticity, and verifiability. To the best of our knowledge, there is no scheme that has been proposed to cover these properties; especially verifiability and authorized equality test techniques in SG. The main contributions are stated as follows:

- The proposed CL-SG scheme ensures confidentiality, integrity, and privacy using certificateless signcryption techniques.
- The proposed Cl-SG scheme provides verifiability by allowing end-users to verify the measurement values using a trapdoor algorithm. This is by using different equality test techniques for each entity; e.g., any public entity outside the grid (of-the-grid entity) will be given an authorized verification and equality test, and public equality test for the girds entities (on-the-grid entity), and threshold verifiability will be assigned for the measurements values in MU.
- The proposed CL-SG scheme reduces the trust in third parties; e.g., data concentrators, substations, and central units; using certificateless that any third party can only generate a partial private key instead of the full private key.
- For security, the detailed construction of our CL-SG is secure regarding EU-CMA and IND-OW-CCA2 security definitions.
- For efficiency, the CL-SG scheme is an efficient lightweight cryptosystem regarding the computation cost and communication overhead providing reasonable complexities and minimum handshaking process.
- For general performance, the proposed CL-SG model is secure, efficient, and compatible with smart grids for smart metering systems.
- We proposed a future extended work as a lightweight verifiable attribute-based certificateless signcryption scheme that covers more security properties such as access control, confidentiality, data integrity, authenticity, privacy-preserving, and verifiability. This all-in-one security model will be compatible with SG for both AMI and EMS.

Paper Organization. The rest of the paper is organized as follows. Section II provides paramilitaries regarding some cryptographic definitions and security models. Section III presents our system model within SG. Section IV presents a detailed construction of the proposed CL-SG scheme. Section V presents the performance evaluation of the proposed scheme including correctness, security, and complexity analysis. Then we discussed our proposed model and gave some improvements as extended future work in Section VI. Finally, we conclude and summarize the paper in Section VII.

II. Preliminaries

This section provides some basic cryptographic definitions including bilinear pairing and some hard assumptions that are been used along the paper as long as some security models.

1) Bilinear Pairing: For $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic groups with prime orders p; and a generator R in $\mathbb{G}_1$. A map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is called a bilinear pairing if it fulfills the following properties:

- Bilinearity: For all $P, Q \in \mathbb{G}_1$ and $r, s \in Z_p^*$ $e(rP, sQ) = e(P, Q)^{rs}$
- Non-degeneracy: $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$
- Computability: For all $P, Q \in \mathbb{G}_1$, there always exists an algorithm to compute $e(P, Q)$ efficiently.

2) Diffie-Hellman problem (DHP): Given $(P, P^r, P^s, Q) \in \mathbb{G}_2$), where r, s are chosen randomly $r, s \in Z_p^*$, the DDH problem is to decide whether $Q = P^{rs} \in \mathbb{G}_2$. There no probabilistic polynomial-time algorithm exists to solve the DDH assumption with a non-negligible probability.

3) Computational Diffie Hellman Problem (CDHP): Given $(P, rP, sP \in \mathbb{G}_1)$, where r, s are chosen randomly $r, s \in Z_p^*$, the CDHP problem is to compute rsP. There no probabilistic polynomial-time algorithm exists to solve the CDHP assumption with a non-negligible probability.

4) Bilinear Diffie-Hellman Problem (BDHP): Given $(P, rP, sP, tP \in \mathbb{G}_1)$, where r, s, t are chosen randomly $r, s, t \in Z_p^*$, the CBDHP problem is to compute $e(P, P)^{rst}$. There is no probabilistic polynomial-time algorithm exists to solve the CBDHP assumption with a non-negligible probability.

5) Security Models: Assume a security model between a challenger Ch and an adversary A. Thus, the security of our CL-SG model (certificateless) can be elaborated into two main adversary definitions as follows.

- Type-1 IND-OW-CCA adversary: The adversary *does not have* access to the master key, but *may* replace public keys with values of its choice. Without knowing the trapdoor, the adversary cannot distinguish the challenge cipher-values (C^*) that is the signcryption of the corresponding plaintext values (M) under the definition of indistinguishable and one-way security for adaptive chosen-ciphertext attacks as well as unforgeable for chosen-message attacks.
- Type-2 IND-OW-CCA adversary: The adversary *does have* access to the master key, and *may not* replace the public key. Without knowing the trapdoor, the adversary

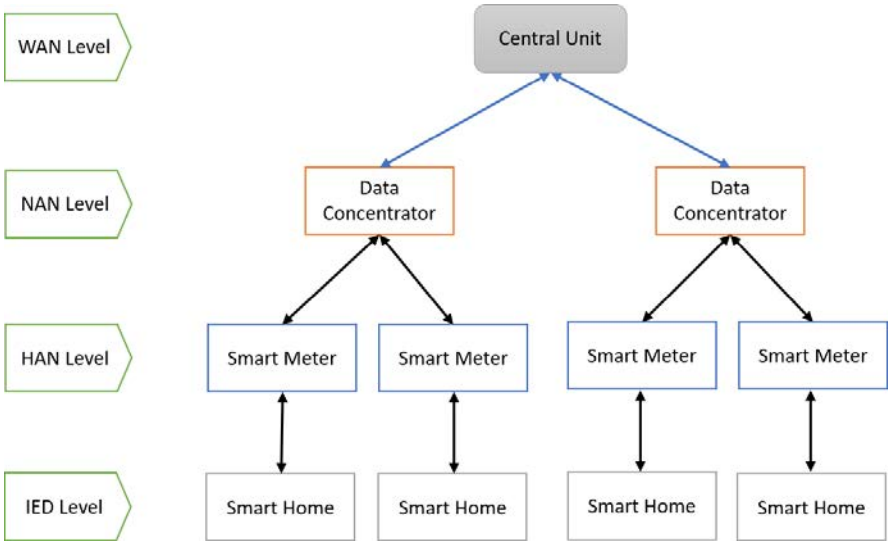

Fig. 2. Advanced Metering Infrastructure (AMI) General Architecture.

cannot distinguish the challenge ciphertext values (C^*) that are the signcryption of the corresponding plaintext values (M) under the definition of indistinguishable and one-way security for adaptive chosen-ciphertext attacks as well as unforgeable for chosen-message attacks.

III. CL-SG: System Model

The proposed CL-SG is a secure metering system for smart grids using certificateless signcryption with an equality test to ensure privacy, verifiability, and reduce the trust in the third party. The signcryption technique with public verifiability allows end-users via a trapdoor to check the ciphertext validity without knowledge of the underlying message and secret private keys, and this way reduces the unnecessary burden on the end-users for processing invalid ciphertexts. The proposed CL-SG involves four parties: Central Unit (CU), Data Concentrator Unit (DU), Smart Metering Unit (MU), and End-user/device (EU). Please refer to Ref. [6] and Fig. 2 for more details about AMI architecture and entities. Also, Fig. 3 illustrates our proposed model description. The proposed CL-SG scheme consists of seven algorithms: *Setup, Partial-KeyGen, Key-Gen, Signcrypt, Unsigncrypt, Trapdoor, and verifiability*, and these algorithms are divided into three phases: *Initial, Metering, and Verifiability* phases as follows.

- ***Initial Phase*:**
  - ***Setup*** (k): This algorithm runs by the third-party (CU). It takes as input a security parameter k and the master secret key s, then returns the public system parameters $params$.
  - ***KeyGen (Partial)*** ($params$, s): This algorithm runs by (DU). It takes the system parameters $params$ and the master secret key s, then generates the partial private key ppk; and sends it to the corresponding entities.
- ***Metering Phase*:**
  - ***KeyGen (Extract)*** ($params$, ppk): This algorithm runs by (EU) and (MS). It takes as input $params$, ppk, then generates the public key and extracts the full private key sk.
  - ***Signcrypt*** ($params$, sk, pk, M): This algorithm runs by (EU) and (DU). It takes as input the public parameters $params$, the meter's public key pk_t, the EU's private key sk_v, and plaintext values M, then returns a signcrypted-values C.
  - ***Unsigncrypt*** ($params$, sk, pk, C): This algorithm runs by (EU) and (DU). It takes as input the systems parameters $params$, the DU's private key sk_t, the EU's public key pk_v, and the signcrypted aggregated data C_{agg}, then returns the plaintext values and accept the M if and only if the signcrypted aggregated values C_{agg} is valid and corresponding to EU ID, pk, sk. Otherwise, returns $Invalid$.

- ***Verifiability Phase*:**
  - ***Trapdoor*** ($params$, sk, pk): This algorithm runs by (EU), (MU), and (DU). It takes as input $params$, sk, then returns different trapdoors T_P, T_A on the corresponding signcrypted data C for different purposes, e.g., for public verifiability and authorized equality test for threshold metering test.
  - ***Verifiability*** ($params$, T, C): This algorithm runs by (EU) and (DU) as an equality test function for the verifiability property. It takes the trapdoors T_P, T_A for the targeted entities and the corresponding signcrypted-values C_{du}, C_{eu}, then returns verification as *Valid/Invalid*.

Note: The EU and DU may verify and compare their measured values with the ones at CU and SM using an authorized trapdoor. Also, an aggregation algorithm could be added by collecting and aggregating all signcrypted and measurement data, then outputs aggregated signcrypted data to be unsigncrypted and verified all at once for better performance.

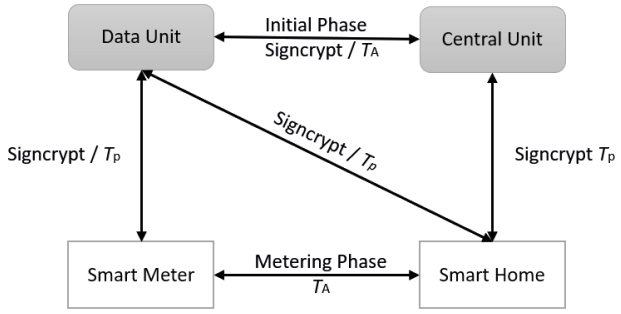

Fig. 3. The proposed CL-SG model.

IV. CL-SG: Detailed Construction

The detailed construction of the proposed CL-SG scheme consists of the following seven algorithms.

- ***Setup***: This algorithm runs by the third-party CU as follows:
  Given the security parameter k, the PKG chooses bilinear map groups $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with prime order q and generator $P \in \mathbb{G}_1$.
  Choose a master $s \in Z_q$, and calculate $P_o = s\ P$.
  Let H_1, H_2, H_3, and H_{mu} be cryptographic hash functions as follows:
  $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$
  $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^*$
  $H_3 : \mathbb{G}_1 \rightarrow Z_q$
  $H_{mu} : \mathbb{G}_2 \rightarrow \{0,1\}^{m \times l}$
  The system parameters:
  $params = (\mathbb{G}_1, \mathbb{G}_2, e, H_1, H_2, H_3, H_{mu}, P, P_o)$
- ***Partial-KeyGen***: This algorithm runs by the third-party DU, it generates the partial private key as follows:
  $Q = H_1(ID) \in \mathbb{G}_1$
  Set partial private key: $ppk = sQ \in \mathbb{G}_1$
- ***KeyGen***: This algorithm runs by MU and EU meter and end-user to generate the public key and extract the full private key as follows:
  Pick random: $a \in Z_q$
  Set public key: $pk_{v/t} = aP_o \in \mathbb{G}_1$
  Set the private key: $sk = asQ_{ID} \in \mathbb{G}_1$
- ***Signcrypt***: Given $params$, the Plaintext $M \in \{0,1\}^*$, and the measured-values $M_{mu} \in \{0,1\}^{m \times l}$. The signcryption algorithm using the corresponding public/private keys is performed by the following steps:
  Pick randoms: $r_1, r_2, r_3 \in Z_q$
  Then compute:
  $C_0 = e(pk, r_1 Q)$
  $C_1 = r_1 P$
  $C_2 = M||r_2 \oplus H_2(C_0)$
  $C_3 = r_1 H_1(M||r_2) + H_3(C_1) \cdot sk$
  $C_4 = M_{mu} \oplus H_{mu}(C_0^{r_3})||M \oplus H_2(C_0^{r_3})$
  The meter outputs the ciphertext: $C = (C_1, C_2, C_3, C_4)$ and sends it to EU and DU for the later unsigncryption and equality test processes, such that C is the signcryption of M.
- ***Unsigncrypt***: Given $params$, ciphertext C. The unsigncryption algorithm between entities EU, MU and CU using the corresponding public/private keys is performed by the following steps:
  Compute: $C_0^{'} = e(sk, C_1)$
  Compute: $M||r_2 = C_2 \oplus H_2(C_0^{'})$
  Check: $e(C_3, P) = e(C_1, H_1(M||r_2)) \cdot e(H_3(C_1) \cdot Q, pk)$. If yes, output V as the plaintext. Otherwise, abort C.
- ***Trapdoor***: Given (C, IDs). This algorithm computes the trapdoors for all entities as follows.
  For public trapdoor: $T_p = H_{mu}, params$
  For authorized trapdoor: $T = r_3 \cdot sk$
- ***Verifiability***: Given the test parameters (C, T). This algorithm runs by any of the SG entities that own the corresponding trapdoors.
  For authorized verifiability, the grid entities must possess the corresponding trapdoor and use a general hash function H_2 as follows:
  Compute: $C_5 = H_2(e(C_1, T))$
  Then check: $C_4 \oplus C_5 = M \rightarrow$ *Valid/Invalid*
  For public verifiability, the grid entities may get C4 and C5 using a special hash function H_{mu} that maps several data into a matrix as follows:
  Compute: $C_5 = H_{mu}(e(C_1, T))$
  Then check: $C_4 \oplus C_5 = M_{mu} \rightarrow$ *Valid/Invalid*

V. Performance

This section defines the consistency of the proposed SL-SG scheme, security definitions, models, and analysis regarding indistinguishability for chosen-ciphertext attack and one-way chosen-ciphertext attack (IND-OW-CCA) as well as for security for the unforgeability under chosen-message attack (EU-CMA).

A. Correctness

The consistency of the proposed scheme can be demonstrated as follows:

- ***Encryption***:
  $C_0^{'} = e(sk, C_1)$
  $= e(asQ, r_1 P)$
  $= e(pk, r_1 Q) = C_0$
  $M^{'}||r_2 = C_2 \oplus H_2(C_0^{'}) = M||r_2$
- ***Signing***:
  $e(C_3, P) = e(r_1 H_1(M||r_2) + H_3(C_1) \cdot sk, P)$
  $= e(r_1 H_1(M||r_2) + H_3(C_1) \cdot asQ, P)$
  $= e(r_1 H_1(M||r_2), P) \cdot e(H_3(C_1) \cdot Q_{ID,asP})$
  $= e(C_1, H_1(M||r_2)) \cdot e(H_3(C_1) \cdot Q, pk)$
- ***Verifiability***:
  $C_4 \oplus C_5 = M_{mu} \oplus H_2(C_0^{r_3}) \oplus H_2(e(C_1, T))$
  $= M_{mu} \oplus H_2(C_0^{r_3}) \oplus H_2(e(C_1, r_3 sk))$
  $= M_{mu} \oplus H_2(e(asP, r_1 Q)^{r_3}) \oplus H_2(e(C_1, asQ)^{r_3})$
  $= M_{mu} \oplus H_2(e(C_1, sk)^{r_3}) \oplus H_2(e(C_1, sk)^{r_3}) = M_{mu}$
  Then outputs $Valid/Invalid$.

B. Security Analysis

The most important and strong security for an equality test technique is to prove the basic scheme regarding indistinguishability for adaptive chosen-ciphertext attack (IND-CCA2) in the random oracle model (ROM) which is suitable for pairing-based/hash-based public-key cryptosystems. Then to prove the full scheme for one-way adaptive chosen-ciphertext attacks (OW-CCA2) by allowing the adversary to enquire the trapdoor for the equality test algorithm. Please refer to b28 for a detailed complete security analysis.

Definition 1: The proposed scheme is secure against indistinguishable one-way adaptive chosen-ciphertext attack (IND-OW-CCA) in the random oracle if A can win against some hard assumptions, e.g., BDHP, with a negligible advantage.

Analysis: Assume A_1 is an adversary trying to break the scheme versus a challenger Ch to solve the hard problem in polynomial time and with a non-negligible advantage; as follows:

- *Initial*: Ch performs the Setup algorithm and generates the system parameters $(params)$. Then send it to the adversary A_1.
- *Phase*1: For all the adversary queries, Ch will maintain a list for the following queries:
- $Hash-$ *queries*: Ch picks randoms, such that these randoms will be used to respond to A_1 for each H_i queries regarding secret parameters, and maintain lists H_{list}.
- *Key-queries*: Ch checks H_{list} for the corresponding public/private key. If exists, Ch sends to A_1. Otherwise, Ch picks randoms and computes/replaces the public key.
- *Signcrypt-queries*: a query on cipher-value C that corresponding to the identities ID_i. If true, then Ch returns M. If not, then Ch checks the corresponding list and outputs M. Then Ch verifies the signature algorithm. If it holds, return M; otherwise, abort.
- *Trapdoor-queries*: Given ID_i, and C. Ch checks H_{List} and computes T for the corresponding C.
- *Challenge*: The Ch checks the $params$ against ID_i and the corresponding plain-value M. If holds, abort. Otherwise, Ch picks randoms and computes the signcryption on M_b, such that $b = 0, 1$, and picks C_i
  Finally, Ch sends the challenge values C^* to A_1.
- *Phase*2: is the same as phase 1, except that A_1 cannot make a query on the challenge/targeted cipher-value C^* and the corresponding secret key.
- *Result*: A_1 outputs the guess $b^* = 0, 1$ with $i_queries$ for H_list and all randoms. Eventually, A_1 failed to recover the challenge cipher-value; with negligible advantage $Pr[M = M^*] = \epsilon$. Thus, Ch could solve the corresponding hard problem with a non-negligible advantage. Then, the proposed CL-SG model is IND-OW-CCA secure.

Definition 2: A signcryption scheme is a logical combination of encryption and signature algorithms. Thus, it is important to prove the signature and verification algorithms in a commonly used security definition such as existentially/strong unforgeability under chosen-message attack (EUF-CMA) in the random oracle. We claim our model is secure if A_2 can win against some hard assumptions with a negligible advantage.

Analysis: Assume A_2 is an adversary trying to forge a signature on a targeted value versus a challenger Ch trying to solve the hard problem in polynomial time and with a non-negligible advantage; as follows:

- *Queries*: Ch performs the initial phase, hash queries, and signcryption queries. Then Ch responds to A_2 for a forgery attempt.
- *Forgery*: A_2 computes and claims the signature over a signcrypted message C is valid iff $ID^* = ID_{entity}$. Then A_2 could break the scheme. Otherwise, Ch checks H_{list} and computes sk, C. If Ch could solve the hard problem with a non-negligible advantage. Then, the CL-SG model is EU-CMA secure.

C. Complexity Analysis

An important concern for energy systems and especially SGs is that some of the grid entities such as end-users, IEDs, IoT devices, mobile devices, etc., may heavily consume power through computation cost and capacity overhead. In the following, we assess the performance of our proposed scheme, mainly for performance evaluation regarding efficiency and functionality.

According to the experiments in [27] [28]. For the running time, we adopted the following settings, *PIV*; *Windows*; *OS* 64 $(bits)$; *RAM*: 1 (GB); *CPU*: 3 (GHz), and the running time for each operation is as follows:

- ECC multiplication: $T_1 = 1.970$ (ms).
- Exponentiation: $T_2 = 2.573$ (ms).
- Bilinear pairing: $T_3 = 5.337$ (ms).
- General hash function: $T_4 = 0.009$ (ms).
- Other lightweight (XOR, addition, etc.) $\ll 0.001$ (ms) (Omitted).

The complexity comparisons are demonstrated in Table. 1 and Fig. 4 show that our proposed CL-SG scheme supports a low computation cost that is equal to $32.631ms$. In comparison to the schemes in [24] [25] [26]; with running time equal to $50.442ms$, $39.161ms$, and $39.141ms$ respectively. Our proposed scheme clearly improves the computation cost by about $10\% - 40\%$ compared to the above-mentioned schemes.

For the communication complexity, we adopted the 80 bit-length security parameter with ECC-160 bit-length [27] [28]. Assuming that $| \mathbb{I}D |=| \mathbb{M} |=| \mathbb{Z}_q |=| \mathbb{G}_1 |=| \mathbb{G}_2 | = 160bits$. Thus, the proposed scheme provides low communication overhead with $480bits$ compared to; for example; Ref [25] with $800bits$. Thus, the communication overhead is been improved by about 40%.

D. Results and Discussions

The security of the proposed model is based on the advantages of the adversary breaking the scheme versus the challenger solving some hard assumptions regarding CAM and CCA attacks in the grid entities. The CU will keep the setup

TABLE I
COMPLEXITY EFFICIENCY COMPARISONS (ms).

Scheme	[24]	[25]	[26]	Ours
Signcrypt	$2T_1 + 8T_2 + T_3 + 2T_4 = 29.879$	$4T_1 + T_2 + T_3 + 3T_4 = 15.817$	$5T_1 + 2T_3 + 4T_4 = 20.560$	$3T_1 + T_3 + 3T_4 = 11.274$
Unsigncrypt	$T_1 + T_2 + 3T_3 + T_4 = 20.563$	$T_1 + 4T_3 + 3T_4 = 23.345$	$5T_1 + 2T_3 + 4T_4 = 20.560$	$4T_3 + T_4 = 21.357$
Total	50.442	39.161	39.141	32.631

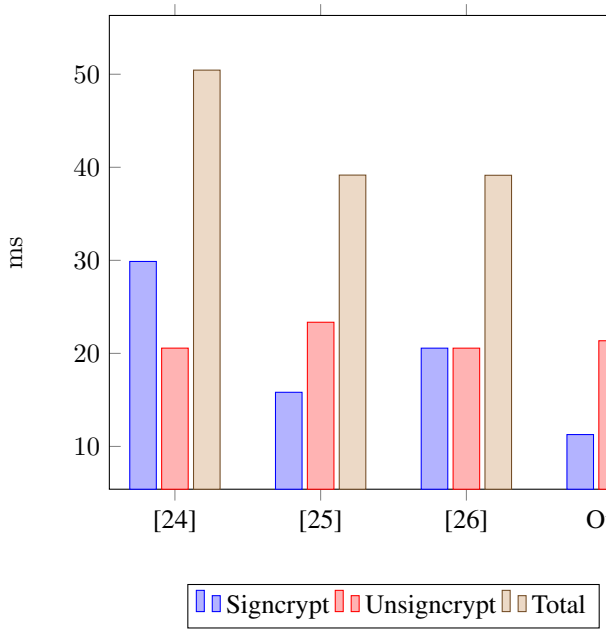

Fig. 4. Complexity efficiency comparisons (ms).

parameters secret including the master key. Any CCA attack on CU will be either trying to get the master key or replacing the public key. Our model is secure regarding Type-1 and Type-2 adversaries. Also, any other on-the-grid entity will be one-way secure using authorized or public or trapdoors [28]. As a result of our proposed model, we consider the equality test techniques using different types of trapdoors as follows:

- All entities can verify the data and identities throughout the grid.
- The AMI entities possess a special trapdoor that is a function in the private key and it is controlled and authorized by CU and EU to protect all sensitive information.
- A public verifiability of other information is granted for all on-the-grids and off-the-grids entities using a public trapdoor.
- The measurement values will be conducted using a threshold trapdoor with authorized equality.

As a result, the security and performance analysis shows that our proposed scheme is efficient, secure, and flexible regarding security versus efficiency and functionality.

VI. FUTURE EXTENDED WORK

The proposed scheme CL-SG is a general model of certificateless signcryption with an equality test providing confidentiality, authenticity, and verifiability, and most importantly, reducing the level of trust in the third party. However, we should consider other security properties such as access control, and also consider a detailed construction of a lightweight cryptosystem for more compatibility with energy systems within EMS and SG. Our future extended work will be a full-scheme-security construction combining both attribute-based and certificateless (ABSC model); described in Fig. 4; with the following considerations.

A. Reduce the level of trust in the third party

Certificateless CL-PKC is considered a good cryptographic primitive for reducing the trust level in the third party by providing untrusted or semi-trusted third-party security models. CL-PKC is the advanced version of identity-based cryptography that solves the well-known security flaw of key escrow in IBC by allowing the third party to only generate a partial private key instead of the full private key. This way, all end-users can generate their private key individually and the same for any trapdoor keys for adding more flexible security features or properties to the main scheme such as an equality test technique.

Setup: it takes as input – a security parameter k. It outputs a master secret key s of attribute authority and public parameters *params*.

KeyGen: it takes as input the entity's access structure (w.r.t. attribute set) AS_{sk} and the attribute authority's master key s. It outputs the entities private key sk.

Signcrypt: it takes as input the access data M and the attribute set (w.r.t. access structure) AS_{sc}, and it outputs the signcrypted data C with access policy AS_{sc}.

Unsigncrypt: it takes as input the signcrypted C which was assumed to be signcrypted under the attribute set (w.r.t. access structure) AS_{sc} and the private key sk for access structure (w.r.t. attribute set) AS_{sk}, and outputs:

The plaintext data M if and only if $f(AS_{sk}, AS_{sc}) = 1$.

Otherwise, outputs $\perp$.

Where the predicate f is predefined (role/rule-based).

Fig. 5. ABSC-based access control for SG.

B. Lightweight Cryptosystem

Intelligent electronic devices (IEDs) and end-users within energy systems (consumers/prosumers, substations, meters, etc.) may have restricted resources regarding power consumption and bandwidth limitations. One of the most significant concerns in energy systems, especially end-users heavily consume this power through the computation cost and communication overhead. Thus, we could consider lightweight cryptosystems by using pairing-free signcryption PKC algorithms as well as using a signcryption scheme that uses the same scheme with logical steps for both a signature and encryption. Thus, giving more security properties and features with minimum computation and communication complexities.

C. Access Control

Attribute-based cryptography (ABC) and attribute-based signcryption (ABSC) can provide role/rule-based access control property for SG by using ciphertext/key policy. However, using only ABC is not enough for some security properties such as privacy-preserving, in which it is required to link the digital signatures with the corresponding identifiers and support anonymity in some cases. Therefore, we can use either the combination of attribute-based with a lightweight certificateless signcryption scheme; or the combination of ABC with zero-knowledge proof (ZKP) in our proposed model to allow an energy service provider (SP) or vendor (prover) to convince his validity to the end-users or any grid entity (verifier) that the SP carries valid credentials for the attributes and the given predicates belong to or a subset of the attributes ($predicates \subseteq attributes$). In other words, the SP can prove to the grid entity that he possesses the requested data and the transmitted data is the input of a signcryption algorithm, and the output is the corresponding signcrypted data.

D. Standardization

An important part of our future work is the investigation and analysis of the IEC 62351 standard, which describes the security recommendations for energy systems. The IEC 62351-8 "role-based access control" will be our main focus together with IEC 62351-9 "key management" and IEC 62351-10 "security architecture guidelines" [29]. These standard considerations play a key role in our future security design due to the wide range of energy vendors with different IEDs and data formats [30]. For our future work, we will adopt these technical recommendations for better protection, integration, and compatibility within energy systems, especially for designing and implementing a cryptosystem that includes the security of substations.

VII. Conclusion

In the present paper, we proposed a signcryption model using certificateless with an equality test technique. The CL-SG is an efficient security model that fulfills major security requirements and properties for energy systems such as privacy-preserving, authentication, data integrity, confidentiality, and verifiability. Therefore, the developed scheme is functional, reliable, and can be practically implemented within SG. Our future directions could be designing and implementing anonymous signcryption schemes using differential privacy, multiparty computation, and private set intersection techniques. Also; as mentioned in the Future Work Section; our extended future work could be a combination of certificateless with attribute-based access control signcryption schemes for SG, AMI, and EMS.

Acknowledgment

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

References

[1] Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Cedric Carter, Patricia Cordeiro, Ifeoma Onunkwo, and Jay Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," Tech. Rep. 12, 2017. Available: https://energy.sandia.gov/download/ 43733/.

[2] R. Landauer, "BlackEnergy: New Jersey Cybersecurity Communications Integration Cell (NJCCIC)," [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/blackenergy.

[3] Paria Jokar, Nasim Arianpoo, and Victor CM Leung, "A survey on security issues in smart grids," Security and Communication Networks, vol. 9, no. 3, pp. 262-273, 2016.

[4] Abir Muhtadi, Dilip Pandit, Nga Nguyen, and Joydeep Mitra, "Distributed energy resources based microgrid: Review of architecture, control, and reliability," IEEE Transactions on Industry Applications, vol. 57, no. 3, pp. 2223-2235, 2021.

[5] Danielly B. Avancini, Joel JPC Rodrigues, Simion GB Martins, Ricardo AL Rabêlo, Jalal Al-Muhtadi, and Petar Solic, "Energy meters evolution in smart grids: A review," Journal of cleaner production, vol. 217, pp. 702-715, 2019.

[6] Mostafa Shokry, Ali Ismail Awad, Mahmoud Khaled Abd-Ellah, and Ashraf AM Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," Future Generation Computer Systems, vol. 136, pp. 358-377, 2022.

[7] Adi Shamir, "Identity-based cryptosystems and signature schemes," In Advances in Cryptology: Proceedings of CRYPTO 84, no. 4, pp. 47-53. Springer Berlin Heidelberg, 1985.

[8] Al-Riyami Sattam S. and Kenneth G. Paterson, "Certificateless public key cryptography," In International conference on the theory and application of cryptology and information security, pp. 452-473. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

[9] Zheng Yuliang, "Digital signcryption or how to achieve cost (signature encryption) cost (signature)+ cost (encryption)," In Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17, pp. 165-179. Springer Berlin Heidelberg, 1997.

[10] Gamage Chandana, Jussipekka Leiwo, and Yuliang Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," In Proceedings of the Twenty Second Australasian Computer Science Conference, Springer, Auckland, pp. 18-21. 1999.

[11] Yang Guomin, Chik How Tan, Qiong Huang, and Duncan S. Wong, "Probabilistic public key encryption with equality test," In Topics in Cryptology-CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings, pp. 119-131. Springer Berlin Heidelberg, 2010.

[12] Zhang Ding, Ching Chuen Chan, and George You Zhou, "Enabling Industrial Internet of Things (IIoT) towards an emerging smart energy system," Global energy interconnection, vol. 1, no. 1, pp. 39-47, 2018.

[13] McDaniel Patrick and Stephen McLaughlin, "Security and privacy challenges in the smart grid," IEEE security privacy, vol. 7, no. 3, pp. 75-77, 2009.

[14] Zhang Liping, Lanchao Zhao, Shuijun Yin, Chi-Hung Chi, Ran Liu, and Yixin Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," Future generation computer systems, vol. 100, pp. 770-778, 2019.

[15] Odelu Vanga, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti, "Provably secure authenticated key agreement scheme for smart grid," IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1900-1910, 2016.

[16] Ran Canetti and Hugo Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," In International conference on the theory and applications of cryptographic techniques. Springer, pp. 453–474, Berlin, Heidelberg: Springer Berlin Heidelberg, 2001.

[17] Kumar, Neeraj, Gagangeet Singh Aujla, Ashok Kumar Das, and Mauro Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6572-6582, 2019.

[18] Odelu Vanga, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti, "Provably secure authenticated key agreement scheme for smart grid," IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1900-1910, 2016.

[19] Sridhar Siddharth, Adam Hahn, and Manimaran Govindarasu, "Cyber–physical system security for the electric power grid," In the Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, 2011.

[20] Park Sanghyun, and Kyungho Lee, "Advanced approach to information security management system model for industrial control system," 2014 - The Scientific World Journal, 2014.

[21] Ahmim Ahmed, Leandros Maglaras, Mohamed Amine Ferrag, Makhlouf Derdour, and Helge Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 228-233. IEEE, 2019.

[22] Ahmim, Ahmed, Makhlouf Derdour, and Mohamed Amine Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," International Journal of Communication Systems, vol. 31, no. 9, e3547, 2018.

[23] He, Debiao, Neeraj Kumar, Sherali Zeadally, and Huaqun Wang, "Certificateless provable data possession scheme for cloud-based smart grid data management systems," IEEE Transactions on Industrial Informatics, vol.14, no. 3, pp. 1232-1241, 2017.

[24] Hu Chunqiang, Jiguo Yu, Xiuzhen Cheng, Zhi Tian, and L. Sun, "CP-ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids," In Mathematical foundations of computer science, vol. 1, no. 1. 2018.

[25] Ahene, Emmanuel, Zhangchi Qin, Akua Konadu Adusei, and Fagen Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9722-9737, 2019.
Ahene, Emmanuel, Zhangchi Qin, Akua Konadu Adusei, and Fagen Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," IEEE Internet of Things Journal, vol.6, no. 6, pp. 9722-9737, 2019.

[26] Sui Zhiyuan and Hermann de Meer, "An efficient signcryption protocol for hop-by-hop data aggregations in smart grids," IEEE Journal on Selected Areas in Communications, vol. 38, no. 1, pp. 132-140, 2019.

[27] Mohammed Ramadan, Yongjian Liao, Fagen Li, Shijie Zhou, and Hisham Abdalla, "IBEET-RSA: Identity-Based Encryption with Equality Test over RSA for Wireless Body Area Network," Springer, Mobile Networks and Applications, MONET, 25 (1), pp. 223–233, 2020.

[28] Ramadan, Mohammed, and Shahid Raza, "Secure Equality Test Technique using Identity Based Signcryption for Telemedicine Systems," IEEE Internet of Things Journal. Vol. 10, Issue: 18, pp. 16594-16604, 2023.

[29] IEC 62351, "Power Systems Management and Associated Information Exchange—Data and Communications Security," International Electrotechnical Commission (IEC): Geneva; Switzerland, 2007.

[30] Hussain SM Suhail, Mohd Asim Aftab, Shaik Mullapathi Farooq, Ikbal Ali, Taha Selim Ustun, and Charalambos Konstantinou, "An effective security scheme for attacks on sample value messages in IEC 61850 automated substations," IEEE Open Access Journal of Power and Energy, 10, pp. 304-315, 2023.