European Journal of Computer Science and Information Technology
Vol.3, No.4, pp.21-30, November 2015
Published by European Centre for Research Training and Development UK (www.eajournals.org)

A LIGHTWEIGHT PRIVACY AND INTEGRITY PRESERVING DATA COMMUNICATION IN SMART GRID

Omaimah Bamasag

Department of Computer Science
Faculty of Computing and Information Technology
King Abdulaziz University, Jeddah, Saudi Arabia

ABSTRACT: *Smart Grid facilitates real-time communication network between the user and the grid company by smart terminals, which utilizes bidirectional data transmission and information control. In Smart Grid, the smart meters play important role by measuring the amount of electricity consumption and sending various information to the power generators and substations. The communication of such information raises privacy concerns from the users about their private information leakage. Therefore, Confidentiality and integrity of smart meter readings are important as altering such data can lead to incorrect billing and false energy usage approximations. In order to insure the security of communication in Smart Grid, we propose the use of ID-based signcryption scheme using bilinear pairing and time factor. It satisfies the requirements for secure communication. It is also efficient, which makes it suitable for low power, low storage sensors in home appliances devices.*

KEYWORDS: Smart Grid Security, ID-based Signcryption, lightweight confidentiality.

INTRODUCTION

Statistics [1] showed that there is a drastically increase in the demand on power supply worldwide. For example, [2] stated that from 1950 to 2008, energy production and consumption in the US increase approximately two and three times, respectively. The public/commercial services, industry and residential areas are the most demanding areas for electricity in the US in 2008. As a result, the National Institute of Standards and Technology (NIST) developed the standards for the next-generation electric power system, commonly referred to as the Smart Grid [4].

The traditional power grids use one-way communication to carry power from a few central generators to a large number of users or customers. They are enhanced with communication networks to provide real-time two-way communication capability between users and different entities in the grid (as shown in Fig.1) to establish a dynamic and interactive infrastructure with new energy management capabilities, such as advanced metering infrastructure (AMI) [5] and demand response [6].

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

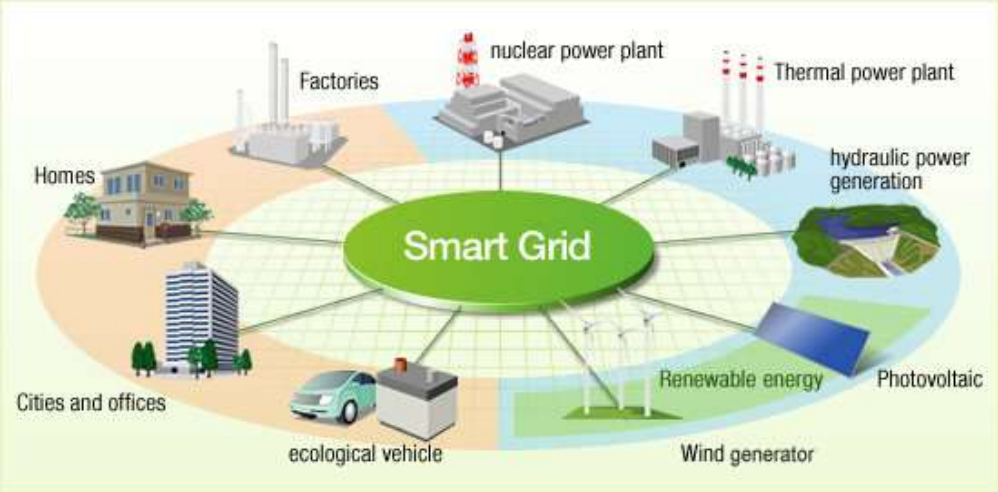

Figure 1. Smart Grid

The evolution of Smart Grid depends not only on the growth of power equipment technology, but also on the advancement of sophisticated computer monitoring, analysis, optimization, and control from central utility locations to the distribution and transmission grids. Therefore, a smart information subsystem is employed to facilitate information generation, modeling, integration, analysis, and optimization in the context of the Smart Grid [8].

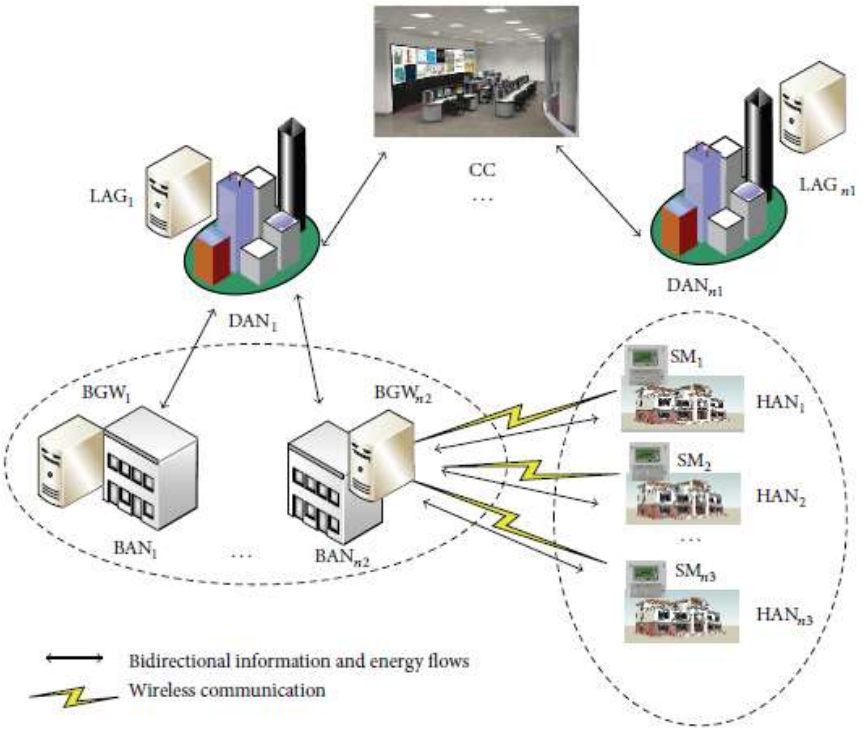

Figure 2. Smart Grid Architecture

As shown in Figure 2, smart grid is divided into a number of hierarchical networks, which is comprised of control center (CC), district area network (DAN), building area network (BAN), and home area network (HAN).The CC covers $n1$ DANs. For the sake of simplicity, we assume that each DAN comprises $n2$ BANs and each BAN comprises $n3$ HANs. Each HAN is assigned

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

a smart meter (SM) enabling an automated, bidirectional communication between the CC and the HAN users. Meantime, each BAN is equipped with a gateway (BGW) and each DAN is equipped with a local aggregator (LAG). And each SM can directly communicate with LAG via the BGW.

A smart meter (SM) collects fine-grained power consumption information of the home appliances, i.e. dishwasher, TV, and the refrigerator, during a short time slot and sends it to authorized entities, i.e. CC through LAG, for monitoring and billing purposes. Also, smart meters have the ability to disconnect –reconnect remotely and control the user appliances and devices to manage loads and demands within the future "smart-buildings" [8]. The focus of this paper is to provide secure data transmission from home appliances to SM, and from SM to CC via LAG.

From a consumer's side, smart metering offers a number of advantages, i.e., the ability to estimate bills and thus manage their energy consumptions. It'll also allow operators to manage the grid more efficiently. The suppliers will be able to realize real-time pricing, thus forecast their customers' demand more accurately. As a result the grid's reliability and efficiency can be improved.

However, unauthorized and uncontrolled access to this information may put users' privacy at risk. Entities that have access to it may, for example, use non-intrusive load monitoring (NILM) techniques [10] to build individual users' electricity consumption patterns, thus breaching their privacy. The more fine-grained the data are, the greater the risk for users' privacy is. Therefore, providing confidentiality, integrity, and source authentication are of utmost important to achieve secure Smart Grid communication.

In this paper we propose the use of ID-based signcryption scheme [19] for privacy and integrity and authentication preserving communication in Smart Grid. We introduce the use of timestamp in the scheme to ensure message freshness and not replayed by an attacker. The rest of this paper is organized as follows. Section II outlines the security requirements to be fulfilled by the scheme. Section III reviews the related work. The ID-based signcryption scheme is described in Section proposed CLSC scheme is given in section III. Section IV provides background information and describes ID-signcryption. Section V shows how to employ ID-based signcryption in Smart Grid network. Section VI evaluates the security properties in terms of addressing the requirements listed in section II. Finally, Section VII conclude the paper and gives directions for future work.

SECURITY REQUIREMENTS

This section presents the security requirement that a data communication protocol in Smart Grid should stratify.

- **Confidentiality of users' data**: Only authorized entities (Transmission System Operators, Distributed Network Operators, Suppliers) can access users' data.
- **Message source authentication**: The message receiver should be able to authenticate the identity of the message sender, i.e. ensuring that the message was sent from the expected source.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

- **Integrity**: is to ensure that the data has not been tampered with or changed while being transmitted over networks and stored by the entities.
- **Unforgeability**: No entity other that the rightful owner of a private key should be able to generate a valid signature, i.e. signcryption, on a message to be transmitted.
- **Public verifiability**: any entity, with an access to the scheme's public parameter, should be able to verify the sender's signature on the transmitted message.
- **Freshness**: is to ensure that the sender has just sent the message to the receiver for the first time, i.e. it was not replayed. Fulfilling this requirement protects the protocol against the Replay attack.

RELATED WORK

In a smart grid, the utility company considers the correctness of the calculated bills as the most important issue. However, from the customer's point of view, privacy is the main concern. Researchers have designed privacy-preserving data aggregation protocols using advanced cryptographic techniques such as zero knowledge proof and homomorphic encryption. Bohil and colleagues [12] proposed a privacy model for smart metering, in which a trusted third-party proxy is introduced to collect meter readings from individual customers and aggregate data before forwarding it to the utility company.

There are a number of proposals on the use of a homomorphic cryptosystem for privacy-preserving data aggregation. For example, Li et al. [13] proposed an in network aggregation scheme that uses SMs to aggregate users' encrypted data en-route for an authorized entity, but their scheme only protects against passive attacks. Deng et al. [14] overcame this by signing each encrypted data. Li et al. [15] further improved the work in [14] by using the Boneh-Lynn-Shacham (BLS) signature scheme that allows a batch verification of signatures. To reduce overheads, Lu et al. [16] proposed a scheme that packs user's multidimensional data into a single encrypted one, whereas Ruj et al. [17] proposed a decentralized aggregation method. Existing homomorphic encryption to achieve privacy preserving is based on the computational expensive operations, which may not be desirable for smart grids with limited resources in terms of both bandwidth and computation. On other hands, several researchers focused on privacy preserving aggregation in different conditions by using multiparty computation [20, 21], differential privacy [22], and the aggregated pseudostatus variation [23].

Signcryption, now an international standard for data security (ISO/IEC 29150, Dec 2011), was invented by Zheng and disclosed to the public at CRYPTO 1997 [24]. It is a cryptographic primitive by which confidentiality is provided through encryption and authenticity is achieved through digital signature, seamlessly at the same time. Performing these two services simultaneously is far more efficient that performing each separately. This allows smaller devices, such as radio frequency identifiers (RFIDs) and wireless sensor networks, to perform high-level security functions. Therefore, signcryption is very suitable for key management in Smart Grid and other resource constrained networks.

Adi Shamir introduced the concept of identity based cryptography IN [25]. The idea of identity based cryptography is to enable a user to use any identity-related string (such as name, Identity number, Email address, etc.) as his public key. Identity based cryptography serves as an

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

efficient alternative to Public Key Infrastructure (PKI) based systems. ID-based signcryption was first studied by Malone-Lee et al. [26]. As ID-based cryptography does not require public key authentication, it has a higher efficiency of computing and communications, and more suitable for Smart Grid communication security. In order to further improve the safety and efficiency of the Smart Grid communication, this paper provides the use of secure signcryption algorithm based on the identity and timestamps. Timestamps is introduced to ensure message freshness, hence, combat against replay attack. The computation and transmission costs of the algorithm are small, which addresses the needs of the Smart Grid that having distributed management and resource-constrained environment.

PRELIMINARIES

In this section, we review some background knowledge including the bilinear pairing and Diffie- Hellman problem. We also provide the generic mode and security notions necessary to build our signcryption scheme in this section. We refer the reader to [13-15] for a discussion of how to build a concrete instance using super singular curves and compute the bilinear map.

Bilinear pairings and Diffie-Hellman problem

We briefly review the bilinear pairing. Let G_1 denote an additive group of prime order p and G_2 be a multiplicative group of the same prime order. Let $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping with the following properties:

(1) Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all $P, Q \in G_1$, and $a, b \in Z_q^*$

(2) Non-degenerate: $\hat{e}(Q, R) \neq 1$, for some $Q, R \in G_1$.

(3) Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any P, Q G_1.

The security of our scheme relies on the hardness of the Diffe-Hellman (CDH) problem.

ID-based signcryption

An ID-based signcryption scheme [19] consists of the following four probabilistic polynomial time (*PPT*) algorithms:

Setup: Given a security parameter 1^k, private key generator (PKG) uses this algorithm to generate *Params* the global public parameters and master secret key S and a corresponding public key P_{pub} as follows:

- Let $(G_1, +)$ be a cyclic additive group generated by P, the computational Diffie-Hellman (CDH) problem in G_1 is to compute abP given aP, bP.
- Define G_1, G_2 and $\hat{e}$ as follows: G_1 and G_2 are two groups of the same prime order p, a bilinear mapping $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the computational bilinear Diffie-Hellman (CBDH) problem in $(G_1, G_2, \hat{e})$ is to compute $\hat{e}(P, P)^{abc}$, given (P, aP, bP, cP).
- Let H_1, H_2 and H_3 be three cryptographic hash functions where H_1: $\{0, 1\}^* \rightarrow G_1$, H_2: $\{0, 1\}^n \times G_1 \times G_2 \rightarrow \{0, 1\}^n$, H_3: $\{0, 1\}^n \times \{0, 1\}^n \times G_1 \rightarrow \{0, 1\}^n$

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

- PKG chooses a master secret key $S = Z_q^*$, keeps S secret and computes $P_{pub} = SP$. The system's public parameters *Params* are (G_1, G_2, q, n, P, P_{pub}, $\hat{e}$, H_1, H_2, H_3, H_4).

Extract: Given *Params*, to generate a secret key for a user with identity $ID \in \{0,1\}^n$, PKG computes $K_{ID} = SQ_{ID}$, where $Q_{ID} = H_1(ID)$.

Signcrypt: To send a message m to user B with identity ID_B, user A with identity ID_A obtains the ciphertext σ by computing *Signcrypt* $((m, T), K_A, ID_B)$, where T is the current time of the machine, following the steps below:

- Choose $x \in Z_q^*$
- Compute $U = xP$
- Compute $\alpha = \hat{e}(P_2, Q_B)^x$
- Compute $\beta = H_2((m, T), \alpha, U)$
- Compute $C = (m, T) \oplus \beta$
- Compute $r = H_3(C, U, \beta)$
- Compute $V = xP_{pub} + rK_A$

The ciphertext is $\sigma = (C, U, V)$

Unsigncrypt: When receiving $\sigma = (C, U, V)$, B computes *Unsigncrypt* (σ, ID_A, K_B) as follows:

- Compute $\alpha = \hat{e}(U, K_B)$
- Compute $\beta = H_2((m, T), \alpha, U)$
- Recover $(m, T) = C \oplus \beta$
- Compute $r = H_3(C, U, \beta)$
- Accept the message if and only if :
    - The equation holds, $\hat{e}(P, V) = \hat{e}(U, P_{pub})\hat{e}(P_{pub}, Q_A)^r$
    - The time stamp T is within a range acceptable and agreed upon by the sender and the receiver.

  Otherwise, output "Invalid".

SECURE DATA COMUNICATION IN SMART GRID USING ID-BASED SINGCRYPTION

This section explains the deployment of the ID-based signcryption scheme, introduced in Section V1, in customers data transmission in Smart Grid network.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

- **Setup**

During the manufacture of a device *x*, e.g. smart meter, smart TV, utility server, etc., *Params* is embedded into each device. ID_x is unique identification number of each device (e.g. serial number). PKG uses this ID_x to generate a device-specific key and embeds it into the device as well. Each home appliance device is also equipped with ID_{SM}, SM is equipped with *ID* of all home appliances it is connected with and also with the ID_{LAG}.

- **Home appliance**

At a specific timeslot *t*, each smart home appliance *A* signcrypts its electricity consumption reading using its key K_A and SM's ID_{SM}: $\sigma_A = Signcrypt(m_A, K_A, ID_{SM})$, and sends σ to SM

- **SM**

Upon receiving the ciphertext σ_A from the home appliances, SM will unsignrypt each received ciphertext σ_A, individually, (σ_A, K_A, ID_{SM}) and reveal the message m_A for the purpose of monitoring and load balancing, and then, after a positive verification, signcrypt the received readings m_{Ai} from all appliances as a bulk $\sigma_{SM} = Signcrypt((m_{A1}, m_{A2}, m_{A3}, .., m_{An}), K_{SM}, ID_{LAG})$, to be sent to *LAG*, as in the previous step.

- **LAG**

Upon receiving the ciphertext message σ_{SM} from SM, *LAG* unsignrypts it to reveal the readings and verify their origin. Upon positive verification, *LAG* would perform the required operations on the data and forward it to CC in the same way as above.

SECURITY EVALUATION

In this section, we evaluate the security performance of the proposed scheme. Most of these results are based on the elliptic curve discrete logarithm problem (ECDLP). ECDLP is a computational infeasible problem [4].

- **Confidently**

The attacker to decrypt the ciphertext σ_X requires the secret key *S*. As regards, the attacker just knows the point P_{pub} and *P*, if attacker tries to obtain the secret key *S*, it must solve the ECDLP. On the other hand the attacker does not have knowledge of the designated recipient's ID-based private key K_X. As previously mentioned, this problem is computational infeasible.

- **Authentication**

The recipient unsigncrypt the ciphertext σ_A and gets the plaintext m. It can use Eq. (1) to authenticate the origin of received message, i.e. it has been originated and sent by the claimed sender.

$$\hat{e}(P, V) = \hat{e}(U, P_{pub})\hat{e}(P_{pub}, Q_A)^r \qquad (1)$$

Here, the inclusion of Q_A, which is the hash of the *ID* of the sender *A*, insures the authentication property. Hence, the proposed scheme is resistant to the man in the middle (MITM) attacks

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

- **Integrity**

Integrity of the unsicrypted message is ensured by the positive outcome of the verification in equation (1). That is done by the inclusion of *r*, calculated at the receiver side, as it contains the hash of the revealed *m* and together with the hash of the m at the sender β. A positive outcome of this verification ensures that no changes/modifications have been to m in transit.

- **Unforgeability**

If the attacker wants to forge valid $\sigma = (c, U, V)$, it should have the private key of sender K_A and the secret parameter *x*. Assume that the attacker with eavesdropped link channel, generates a forged $\sigma' = (c', U', V')$, for C' to match the original C, the attacker should know β**,** which, in turn, requires him to know α. The attacker cannot compute $\alpha\, \hat{e}(P_2, Q_B)^x$ without knowing the secret parameter *x*, for which he needs to solve the ECDLP. Therefore, our scheme satisfies unforegability.

- **Public verification**

Given (σ_A, K_A, ID_{SM}) anybody can verify the signature by checking equation (1) condition using public *Params,* without a need for the private key of *A* or *B*. Therefore, our proposed scheme provides the public verification properties.

CONCLUSION

In this paper, we have introduced the use of ID-based signcryption scheme based on the bilinear pairings for secure and privacy preserving Smart Grid Communication. This scheme allows a secure and efficient transmission of customer electricity consumption data in Smart Grid by performing encryption and signature in one algorithm. It also protects against replay attack by using Timestamps on the messages to be sent. The security evaluation of the scheme shows that it satisfies confidentiality, integrity, authentication, unforgeability, and freshness for the transmitted data, which are crucial for sensitive customers data transmission in Smart Grid. The future work will include formal proof of the security properties. In addition, the scheme will be implemented using a suitable simulation tool to measure its performance.

REFERENCES

[1] International Energy Agency IEA, 'Key World Energy Statistics', 2013, available from http://www.iea.org/publications/freepublications/publication/KeyWorld2013.pdf [5 Nov 2014].

[2] Lu, G., De D., Song W.-Z., 'SmartGridLab: A laboratory-based smart grid testbed', *Proceedings of IEEE Conference on Smart Grid Communications*, 4-6 October 2010, Gaithersburg, MD, USA, pp. 143-148.

[3] Huang A., Crow M., Heydt G., Zheng J., Dale S., 'The future renewable electric energy delivery and management (FREEDM) systems: the energy internet', *Proceedings of the IEEE*, vol. 99, no. 1, 2011, pp. 133–148.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

[4] NIST, The Smart Grid Interoperability Panel Cyber Security Working Group, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, 2010, Available from http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf. [31 October 2014].
[5] Sui H, Wang H., Lu M.-S., Lee W.-J, 'An AMI system for the deregulated electricity markets', *IEEE Transactions on Industry Applications* vol. 45, no.6, 2009, pp. 2104–2108.
[6] LeMay M. , Nelli R., Gross G., Gunter C.A., 'An integrated architecture for demand response communications and control' , *Proceedings of 41th Hawaii International Conference on System Sciences (HICSS' 08)*, 2008, pp. 174-183.
[7] Navigant Research, Smart Grid Technologies, Transmission Upgrades, Substation Automation, Distribution, Smart Grid IT and Communications Networking, and Smart Metering: Global Market Analysis and Forecasts, 2014.
[8] Amin M., Hasan M., Roy R., 'Roadmap to Smart Grid Technology: A Review of Smart Information and Communication System', *International Journal of Control and Automation*, Vol. 7, No. 8, 2014, pp. 407-418.
[9] Farhangi H., 'The path of the smart grid', *Power and Energy Magazine*, IEEE, Vol. 8, No. (1), 2010, pp. 18-28.
[10] Quinn E., 'Privacy and the new energy infrastructure', *Social Science Research Networks (SSRN)*, 2009.
[11] Li D., Aung Z., Williams J., Sanchez A., 'P3: Privacy Preservation Protocol for Automatic Appliance Control Application in Smart Grid', *IEEE Internet of Things Journal*, Vol. 1, No. 5, 2014, pp. 414-429.
[12] Bohil J., Sorge C., Ugus O., 'a Privacy Model for Smart Metering', *Proceedings of 2010 IEEE Conference on Communications Workshops (ICC)*, pp.1-5.
[13] Li F., Luo B. and Liu P., 'Secure information aggregation for smart grids using homomorphic encryption'. *Proceedings of the First IEEE International Conference on Smart Grid Communications SmartGridComm*, 2010, pp. 327-332.
[14] Deng P. and Yang L., ' A secure and privacy-preserving communication scheme for advanced metering infrastructure', *In Innovative Smart Grid Technologies ISGT, IEEE*, 2012, pp. 1-5.
[15] Li F. and Luo B., 'Preserving data integrity for smart grid data aggregation', *Proceedings of IEEE Third International Conference on Smart Grid Communications SmartGridComm*, 2012, pp. 366–371.
[16] Lu R., Liang X., Li X., Lin X., 'Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, Issue 9, 2012, pp. 1621-1631.
[17] Ruj S. and Nayak A., 'A decentralized security framework for data aggregation and access control in smart grids', *IEEE Transactions on Smart Grid*, Vol. 4, Issue 1, 2013, pp. 196-205.
[18] Mustafa M., Zhang N, Kalogridis G, Fan Z., 'DESA: A Decentralized, Efficient and Selective Aggregation Scheme in AMI', *Proceedings of Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2014, pp. 1-5.
[19] Li, Z., Xu, X., Fan, Z., "Lightweight Trusted ID-Based Signcryption Scheme for Wireless Sensor Networks", International Journal on Smart Sensing and Intelligent Systems, Vol. 5, No., 4, December 2012, pp. 799-810.
[20] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," *Computer Networks*, vol. 57, no. 7, pp. 1699–1713, 2013.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

[21] C. Rottondi, G. Verticale, and C. Krauك, "Distributed privacypreserving aggregation of metering data in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1342–1354, 2013.
[22] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factoraware privacy-preserving aggregation in smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 598–607, 2014.
[23] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1722–1733, 2012.
[24] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)≪cost(signature) + cost(encryption), advances," in *Proceedings of the Advances in Cryptology (CRYPTO '97)*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 165–179, Springer, 1997.
[25] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology-CRYPTO' 84, LNCS 196, Springer, 1984, pp.47-53.
[26] J. Malone-Lee, "Identity based signcryption," Cryptology ePrint Archive. Report 2012/098, 2002, Available from: http://eprint.iacr.org/2012/098.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)