mathematics

Article

The Opening Capability for Security against Privacy Infringements in the Smart Grid Environment

Sungwook Eom [1] and Jun-Ho Huh [2,*]

[1] Department of Electrical Engineering, Pohang University of Science and Technology, Pohang 37673, Korea; sweom@postech.ac.kr
[2] Department of Software, Catholic University of Pusan, Pusan 46252, Korea
* Correspondence: 72networks@pukyong.ac.kr or 72networks@cup.ac.kr; Tel.: +82-51-510-0662

Received: 10 September 2018; Accepted: 2 October 2018; Published: 14 October 2018

Abstract: It is now known that more information can be leaked into the smart grid environment than into the existing environment. In particular, specific information such as energy consumption data can be exposed via smart devices. Such a phenomenon can incur considerable risks due to the fact that both the amount and the concreteness of information increase when more types of information are combined. As such, this study aimed to develop an anonymous signature technique along with a signature authentication technique to prevent infringements of privacy in the smart grid environment, and they were tested and verified at the testbed used in a previous study. To reinforce the security of the smart grid, a password and anonymous authentication algorithm which can be applied not only to extendable test sites but also to power plants, including nuclear power stations, was developed. The group signature scheme is an anonymous signature schemes where the authenticator verifies the group signature to determine whether the signer is a member of a certain group but he/she would not know which member actually signed in. However, in this scheme, the identity of the signer can be revealed through an "opener" in special circumstances involving accidents, incidents, or disputes. Since the opener can always identify the signer without his/her consent in such cases, the signer would be concerned about letting the opener find out his/her anonymous activities. Thus, an anonymous signature scheme where the signer issues a token when entering his/her signature to allow the opener to confirm his/her identity only from that token is proposed in this study.

Keywords: opening capability; security; smart grid; group signature; anonymous signature

1. Introduction

The smart grid is a newly evolving next-generation intelligent power grid, and many technological research works were conducted in different countries over the last decade to increase the efficiency of their power grids. The primary consideration in adopting the smart grid should be protection of the users′ privacy [1–3]. In other words, unlike existing security measures, the smart grid system should basically focus on the security of users rather than suppliers. More personal and specific information can be exposed in the smart grid environment by smart devices or hacking attacks when diverse types of information are combined [4–6]. The major issue of personal information protection in the distribution of smart grid technology is that it is possible to infer a user's behavioral pattern based on his/her energy consumption data by collecting and analyzing more detailed personal data, such as the characteristics of the user's energy usage or the frequency of energy production obtained, by applying the latest electric meters and other related equipment and technologies. In addition, the data read by smart meters inevitably require a certain monitoring or surveillance scheme as they are electronically collected and transmitted, rather than manually processed as in the past. The capacity of a meter capable of assessing consumer patterns or types of appliance depends on the frequency with which it collects data and the types of data being collected. Also, the user's behavior at home can make it is easier to infer his/her activity patterns in other places.

The factors associated with privacy intrusion scenarios in a smart grid environment include the following: (1) information concerning the use of a particular medical device or piece of electronic equipment which indicates their activation times and personal patterns, segmented data pertaining to the power consumption of each household appliance and its measurement location, and detailed information on the use of the appliances or equipment in use at a specific location; (2) the possibility of tracking a physical location through newly consumed energy, for instance, the charging of an electric automobile; (3) the activities in a certain house or building can be inferred from the electronic signature or use time pattern upon activation of a device or piece of equipment, which can form the basis for understanding a specific user's activities. Thus, the collection of a consumer's energy use data by a third party should be limited to the information required to serve the third party's purpose and which is authorized by the consumer.

The anonymous signature scheme comprises a function for authenticating signed messages while hiding the actual identity of the signer, which in itself is a common method in current systems that require the input signature to be authenticated. This scheme was developed by Chaum and Heyst in 1991 [7]. As for the group signature scheme, a member of a certain group is able to attach his/her signature in a message to prove that he is actually a member, and the verifier of the message will be able to confirm that person's membership only, without actually identifying the signer. However, it is possible for the opener, who authenticates the input signature, to identify the signer with the information of the signer previously stored in the system. The opener can be an organization or institution that deals with incidents associated with signatures. The group signature scheme is widely used as an anonymous signature scheme because of its reliability [8]. Despite its reliable performance, however, the security of personal information is called into question as many users consider that the opener has sufficient power to identify the signer and obtain the latter's personal information or information on anonymous activities for other purposes. To resolve this problem, Sakai et al. [9] introduced a complementary scheme by adding an "admitter" to the anonymous signature scheme. Thus, Sakai added the admitter and limited the opener's access to the signer's identification only by obtaining the consent of the admitter. In 2013, Ohara et al. [10] resolved the problem raised by Sakai (2012), which was the admitter's limited amount of token issuance.

The group signature scheme is often used when it is necessary for the authenticator to verify that the signer is a member of a particular group without revealing the actual identity. The real identity of the signer can be disclosed to the authenticator only if there are incidents or disputes that need to be solved. Nevertheless, it is quite clear that the signer will feel the burden of revealing his/her identity or anonymous activities to the authenticator without his/her consent and consider that the authority of the authenticator is too great. Thus, to limit the authority of the authenticator while maintaining the effectiveness of the group signature schemes, an anonymous signature scheme which authorizes the authenticator to identify the signer only with the token issued by the signer him/herself when generating a signature is proposed in this study.

2. Related Research

In a conventional power grid where electric power is delivered to the end users via substations (Figure 1), the power generation and distribution processes are centralized by the system, which assumes the role of mapping and visualizing the routine operations while controlling these processes to meet the power supply/demand schedule and its storage.

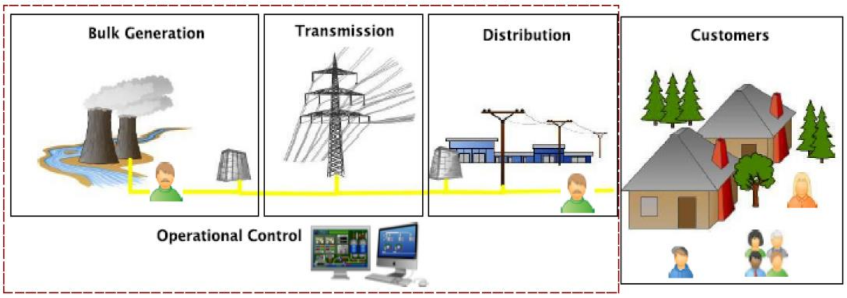

Figure 1. A typical power grid structure.

However, following the rapid development of information technology (IT), such a grid architecture transformed in a way that can provide a more efficient and effective means of power management by integrating with Internet Protocol (IP)-based technologies. The network convergence based on these technologies [11] allows the grid to interwork with an external network(s) by adopting the Transmission Control Protocol (TCP)/IP for a more efficient power management and provision of flexible but efficient service operations.

For the last decade, the development in the hardware, software, and communication technologies led to more advanced and sophisticated information and communications technology (ICT) which were the major factor of widespread mobile smart devices, software applications, or communication architectures [12,13].

The next-generation (21st century) power grid being called the smart grid (Figure 2) enables a smarter, interactive, and dynamic grid management and services based on the ubiquitous computing and advanced ICT technology to respond to the era of the fourth industrial revolution. One of the major advantages of the smart grid is that its bi-directional communication capability can not only improve the power management or operating process but also be utilized for establishing an Internet of things (IoT) system for the users' residences.

The conceptual smart grid model developed by the United States (US) National Institute of Standards and Technology (NIST) defined a smart grid as a complex infrastructure based on a set of seven chief domains [14], namely bulk generation, energy distribution, power transmission, operation and control, market, service providers, and customers and individual domains, composed of heterogeneous elements (e.g., organizations, buildings, individuals, and systems, including system resources and other entities). Also, the backhaul network is essential for achieving smooth but efficient communications between customers and utility companies when advanced power management systems such as advanced metering infrastructure (AMI) are to be embedded into the smart grid [15,16].

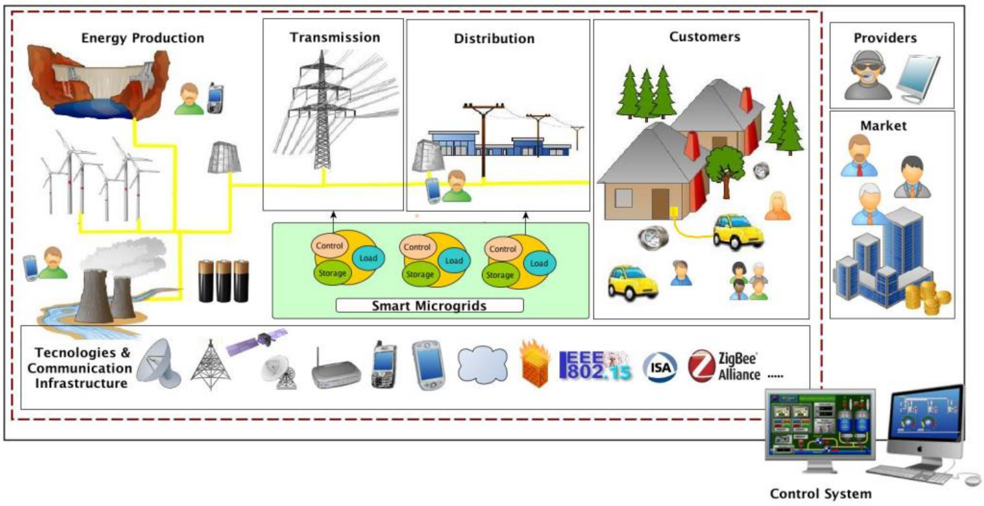

Figure 2. The architecture of a smart grid.

The problem pertaining to breach of privacy is one of the major issues when people are using a service which requires the user to be authenticated. A series of privacy protection schemes were introduced to let users remain anonymous by allowing only encrypted information or minimum user information to be disclosed to the system administrators; however, the security levels and the means of protection provided by those schemes vary and can be inadequate sometimes. The blind signature [17] or the homomorphic encryption [18] scheme is mainly used [19]. To simply describe them, for instance, the former is a scheme where the first party (Party 1) attaches his signature to the message generated by the second party (Party 2) without having any knowledge about the content of the message. Then, the third party (Party 3) can receive the message but the identity of the message sender (Party 2) will remain secure as his/her signature will not be authenticated. Meanwhile, in the latter scheme, a specific mathematical or a computational manipulation is applied to the message or the text to create a ciphertext so that only the authorized party with the right decryption key will be able to decipher the encrypted message. The smart meters usually adopt the latter scheme to encrypt and transmit their requirements to their central control system (utility company administrator) along with a specific encryption function to let the system to decrypt the contents of the requirement with an appropriate decryption key. These schemes were originally developed for the electronic voting systems to conceal the voters' information in the application layer but did not consider the possibility leaking the information from the lower layers (i.e., link layer or network layer) of the protocol stack. It is quite possible that the repeated use of the same IP address overtime may provide access to the identities of the communicating parties or a means for hackers to analyze the traffic [20].

Nonetheless, it is also true that such benefits may be provided at the cost of breaching privacy. That is, a large volume of generated data and its high granularity in which more information is contained would allow any third party with malicious intent to grasp the lifestyles of the customers. Also, there were some claims in some countries that the use of smart meters further endangered the security/privacy of the customers [21]. The balance between achieving an efficient and effective smart metering and guaranteeing the adequate level of personal information protection is always the focus of such a controversy. Using the terminology from Reference [22], the solutions that aim to protect the privacy should guarantee the customers a suitable level of anonymity together with a temporary unlinkability which disconnects them from the metering infrastructure (i.e., disabling power usage reading, etc.). However, the question here is whether the unlinkability can or should be fully achieved even when customers are required to settle their bills at some time or another. The same question can be addressed to unobservability, which refers to the condition where one's power usage cannot be observed by others. Although it is possible to keep the record of the total aggregated amount of one's power usage at the substation level, it still needs to be delivered to the main system for the smart metering system to be fully functional [22,23].

2.1. Anonymous Authentication and Anonymous Signature Schemes

The term "anonymous authentication" refers to a cryptographic technology that allows the person or entity requesting authentication to authenticate him or herself as a legitimate entity while remaining anonymous. Commonly, simple aliases designed to preserve anonymity cannot be used for this type of authentication as the user trail can be traced easily; thus, using them cannot be considered an anonymous authentication scheme. A group signature, anonymous letter of credit, and more were introduced for the purpose of anonymous authentication in a number of research works. The group signature is an electronic signature scheme which the signer can verify him/herself as a member of a particular group without having to reveal his/her identity, thus enabling the authenticator to determine that the person concerned is actually a member without being able to identify him/her. Also, the group signature scheme often involves a credible third-party organization referred to as an "opener", e.g., the police or an internet-related authority. The opener is authorized to identify a signer from the group signature and can track the identity of any user who displays inappropriate behavior (or commits illegal acts) while using anonymous services. The group signature scheme is currently considered the most practical for real-world applications such as web application services as it offers traceable anonymity. In general, the group signature scheme offers anonymity, traceability, and linkability.

Figure 3 shows a schematic representation of the group signature scheme, whose members are normally distinguished as the group manager who sets the parameters, the opener who is authorized to trace a specific signature in a group, the signer, and the authenticator. Each signer in the same group has his/her own private signature key, whereas the authenticator can verify the signatures with an open group key. Also, information that can be used to identify a signer is encrypted in the signature value so that only the opener can trace the identity of a group signer with his open group key.

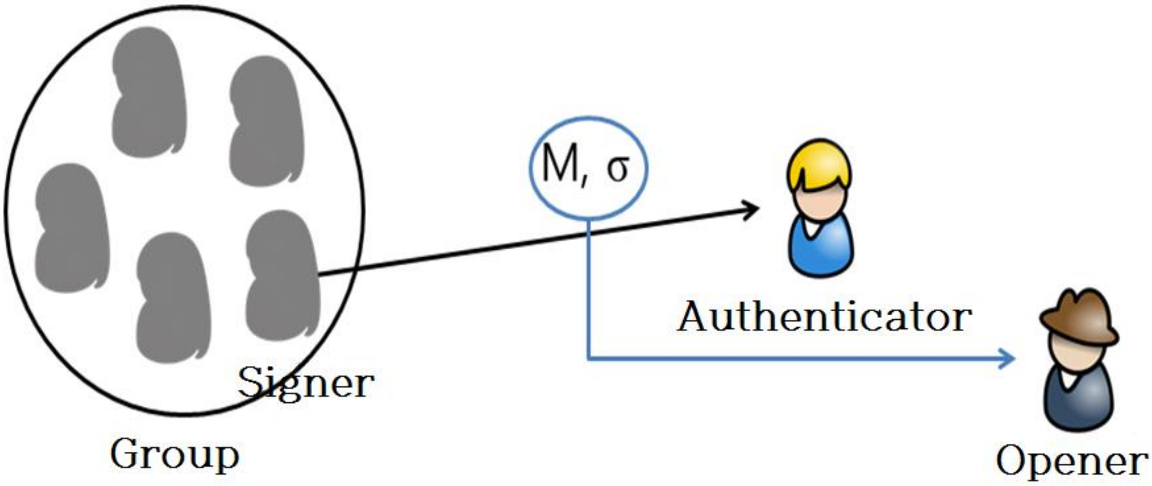

Figure 3. Diagram of the group signature scheme.

Figure 4 represents a group signature scheme that provides linkability, which was studied with a view of applying it to a variety of applications. Linkability is a basis for determining uniformity in a number of signatures so as to determine whether the signatures were written by the same person. Although the linker may detect uniformity in the signatures, he/she is not able to identify the signer.

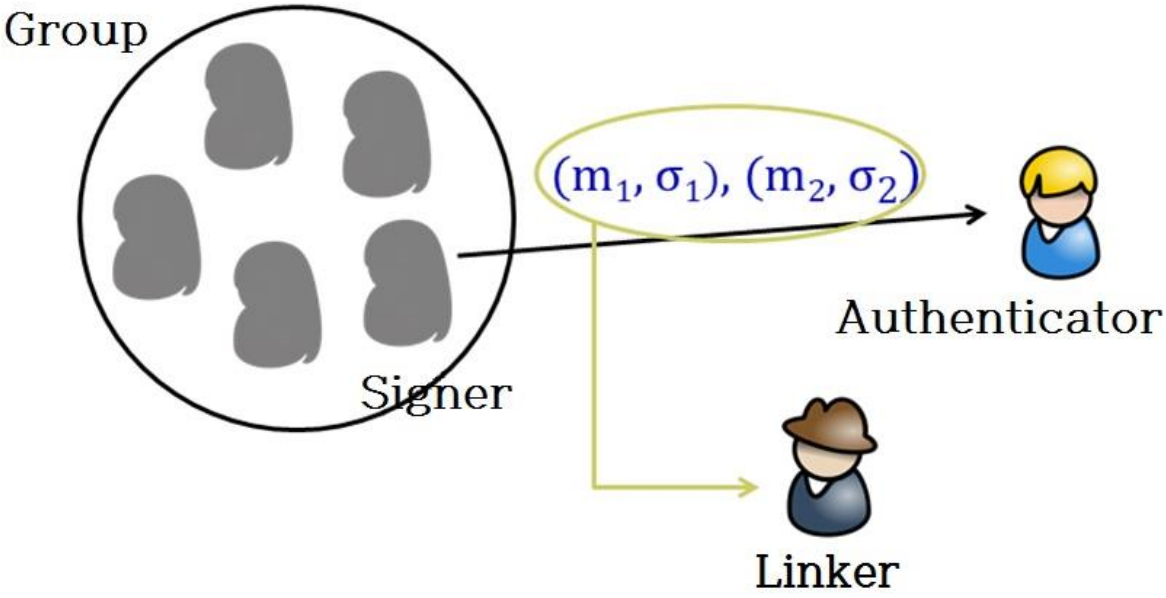

Figure 4. Diagram of group signature scheme with linkability.

In the smart grid environment, service providers can enhance the quality of their services by performing big data analyses of users' data, such as their real-time power usage patterns, etc., and then processing them into meaningful information. Thus, the level of privacy protection can be increased by offering anonymity through group signatures, while the service providers are able to provide flexible services by linking with the data of an anonymous user (signer). Jeong-Yeon Hwang et al. introduced a group signature scheme that provides local linkability [6]; however, in this study, the linker refers to an organization or institution that has a linking key generated by the group manager so that, in general, it becomes the service provider. The linker has the authority to check the link status for all signature values.

Figure 5 shows a group signature scheme offering limited linkability. Unlike existing group signature schemes where the opener is a credible third-party organization, the linker in this scheme is the service provider itself or the organization or institution designated by the service provider, with could result in privacy violations of the service users. For example, let us assume that an anonymous user in the smart grid environment uses a power usage analysis service along with an IoT service. In this case, the service provider will be able to link the power usage information of person A (who just entered his/her signature with the group signature key) with the information about his/her IoT service use. At this time, the service provider does not know the identity of A but it is able to determine whether the user currently using these two services is one and the same, potentially leading to an undesirable breach of privacy. As such, while studies related to existing group signature schemes focused on managing the system for the designated linker so as to be able to test the linkability of all signature values, this study aims to secure a fundamental technology capable of preventing unnecessary information exposures by developing a group signature scheme that allows the designated linker to test the linkability only for those signatures desired by the signer. Thus, in the example shown above, an anonymous signer A can transfer the power usage values to the linker for the linkability test, using a group signature key while transmitting the IoT usage information separately with the same key for the same test. Thus, this scheme can provide a more secure method of preventing privacy breaches by minimizing the level of personal information exposure.

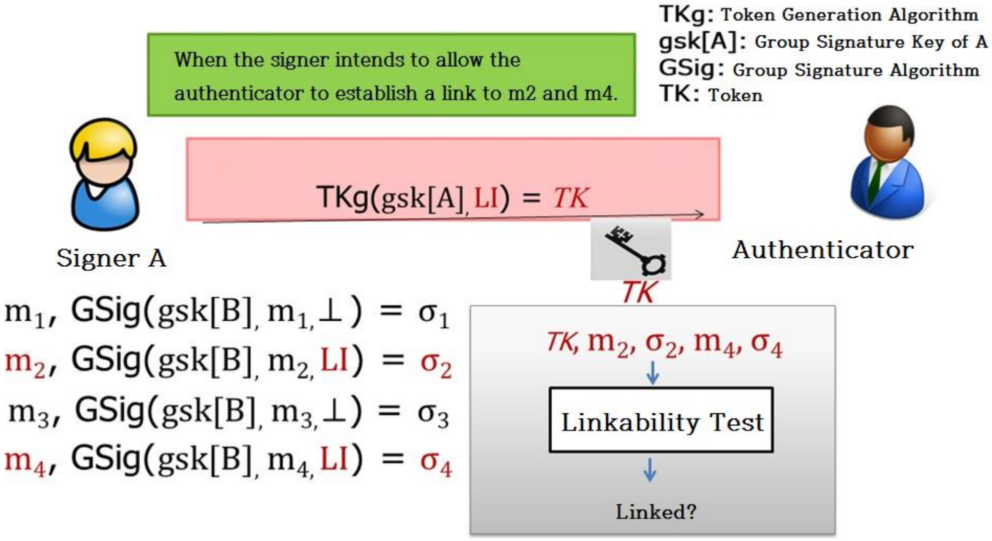
TKg: Token Generation Algorithm
gsk[A]: Group Signature Key of A
GSig: Group Signature Algorithm
TK: Token
When the signer intends to allow the authenticator to establish a link to m2 and m4.
TKg(gsk[A], LI) = TK
Signer A
Authenticator
TK
m1, GSig(gsk[B], m1, ⊥) = σ1
m2, GSig(gsk[B], m2, LI) = σ2
m3, GSig(gsk[B], m3, ⊥) = σ3
m4, GSig(gsk[B], m4, LI) = σ4
TK, m2, σ2, m4, σ4
Linkability Test
Linked?

Figure 5. Diagram of group signature scheme with limited linkability.

3. Anonymous Signature with Signer-Controlled Opening Capability

The anonymous signature scheme allows authentication of the signer without revealing his/her identity, whereas the group signature scheme is a method of verifying that the signer is a member of a certain group, also without exposing the signer's identity. Nevertheless, it is possible for an opener to identify an anonymous signer based on the information of the signer, which is neither desirable nor favorable for the signer who wishes his/her signature to be authenticated but does not want to reveal his/her actual identity. Thus, this section discusses a solution whereby the signer obtains a (security) token upon entering his/her signature so that the opener is not able to find the information of the signer without permission.

3.1. Application

The proposed anonymous signature scheme prevents the opener from identifying the signer without his/her permission so that the opener has to obtain a token specifically issued for the signature that the signer wishes to be identified. For example, this scheme can be applied to an anonymous donation system. The identities of the donors are hidden to ensure that the fundraiser cannot know who donated the funds. However, if the donors wish to apply for an income tax deduction, all they have to do is issue a token to the relevant tax administration to prove their donations through signature authentication. Currently, many countries operate an anonymous reporting system against corruption among civil servants, but the problem is that the filed reports and the identity of a whistle-blower or an accuser can be leaked while processing the report, thus endangering that person or making the system useless. The proposed anonymous signature scheme can prevent such an incident by offering a more secure protection mechanism that makes it almost impossible for an intruder or a report handler to find the identity of the person filing the report. If the reporting system requires the accuser to be identified, and if he/she agrees to disclose his/her identity for a final confirmation or compensation, all he/she has to do is issue a token allowing the relevant authority to confirm the true identity.

3.2. Formal Model

The proposed method has the following four algorithms:

GKg(1^{λ}, 1^{n}): This is the algorithm where the group manager puts the security parameter λ and the number of anonymous signers n to create the signer's signing key gsk_i, the opener's opening key ok, and the public parameters gpk for the system.

GSig(gpk, i, gsk_i, M): This is the algorithm where the anonymous signer uses the group public key gpk, the signer's index i, the signer's signing key gsk_i, and the message M to create the anonymous signature σ, and the token TK_M that permits disclosure.

GVf(gpk, i, gsk_i, M): This is the algorithm where the verifier puts the group public key gpk, the message M, and the anonymous signature σ to verify the signature.

Open(gpk, ok, M, σ, TK_M): This is the algorithm where the opener puts the group public key gpk, the opener's opening key ok, the message M, the anonymous signature σ, and the token TK_M to check the signer's identification.

3.3. Security Notion

The four security concepts based on the definition of a general security model [12,13] for the group signature schemes proposed by Mihir Bellare et al. are introduced in the proposed group signature scheme.

- Full anonymity: The identity of a signer should not be accessed unless a token is issued by the signer. Then, the opener, upon receiving the token, is allowed to trace the signer's identity.
- Correctness: A correct signature and a token issued in the proper way should be used for verification when identifying the signer.
- Unforgeability of signature: A valid anonymous signature can only be written by the signer him/herself to attach it to a specific message.
- Unforgeability of token: A valid token can be created and issued to allow the opener to access a specific message or a signature.

3.4. Proposed Scheme

GKg$(1^\lambda, 1^n)$

- Define two hash functions: H_1: $\{0, 1\}^* \rightarrow G$, H_2: $\{0, 1\}^* \rightarrow Z_p$.
- Select a parameter of the bilinear group (p, G, G_T, e, g).
- Select a random element u, v, $h \in G\backslash\{1\}$, a random integer ξ_1, ξ_2, ξ_3, $\gamma \in Z_p$, and calculate $g_1 = u^{\xi1}h^{\xi3}$, $g_2 = v^{\xi2}h^{\xi3}$, $\omega \leftarrow g^\lambda$.
- Select a random $x_i \in Z_p$ for each signer i ($1\leq i \leq n$), then calculate $A_i \leftarrow g^{1/(\gamma+xi)}$.
- Print out the group public key $gpk \leftarrow (p, G, G_T, e, g, g_z, u, v, h, g_1, g_2, \omega, H_1, H_2)$, the opener's opening key $ok \leftarrow (\xi_1, \xi_2, \xi_3, e(A_i, g)_{1\leq i\leq n})$, and each signer's signing key $gsk_{i(1\leq i\leq n)} \leftarrow (A_i, x_i)_{1\leq i\leq n}$.

GSig(gpk, i, gsk_i, M)

- Select a random integer α, β, ρ, η, $\mu \in Z_p$.
- Calculate $(T_1, T_2, T_3, T_4) \leftarrow (u^\alpha, v^\beta, h^{\alpha+\beta}, {g_1}^\alpha {g_2}^\beta A_i g^\eta)$ and $(T_5, T_6) \leftarrow (g^\rho, e(g^\mu, H_1(M))^\rho)$.
- Select a random integer $r_\alpha, r_\beta, r_\rho, r_\eta, r_x, r_{\alpha x}, r_{\beta x}, r_{\rho x}, r_{\eta x} \in Z_p$.
- Calculate $R_1 \leftarrow u^{r\alpha}$; $R_2 \leftarrow v^{r\beta}$; $R_3 \leftarrow h^{r\alpha+r\beta}$ $R_4 \leftarrow e(T_4, g)^{rx}\, e(g_1, \omega)^{-r\alpha}\, e(g_1, g)^{-r\alpha x}\, e(g_2, \omega)^{-r\beta}\, e(g_2, g)^{-r\beta x}\, e(g, \omega)^{-r\eta}\, e(g, g)^{-r\eta x}$ $R_5 \leftarrow g^{r\rho}$; $R_6 \leftarrow e(g^{\mu}, H_1(M))^{r\rho} e(g, g)^{-r\eta}$ $R_7 \leftarrow {T_1}^{rx} u^{-r\alpha x}$; $R_8 \leftarrow {T_2}^{rx} u^{-r\beta x}$; $R_9 \leftarrow \mathrm{T_5}^{\mathrm{rx}}\mathrm{u}^{-\mathrm{r\rho x}}$ $R_{10} \leftarrow {T_6}^{rx} e(g^\mu, H_1(M))^{r\rho x} e(g, g)^{-r\eta x}$ $c \leftarrow H_2(M, T_1, \ldots, T_6, R_1, \ldots, R_{10})$ $s_\alpha \leftarrow r_\alpha + c\alpha$; $s_\beta \leftarrow r_\beta + c\beta$; $s_\rho \leftarrow r_\rho + c\rho$ $s_\eta \leftarrow r_\eta + c\eta$; $s_x \leftarrow r_x + cx_i$; $\leftarrow s_{\alpha x} \leftarrow r_{\alpha x} + c\alpha x_i$ $s_{\beta x} \leftarrow r_{\beta x} + c\beta x_i$; $s_{\rho x} \leftarrow r_{\rho x} + c\rho x_i$; $s_{\eta x} \leftarrow r_{\eta x} + c\eta x_i$.
- Print out a signature $\sigma \leftarrow (g^{\mathrm{\mu}}, T_1, \ldots, T_6, c, s_\alpha, s_\beta, s_\rho, s_\eta, s_x, s_{\alpha x}, s_{\beta x}, s_{\rho x}, s_{\eta x})$.
- In addition, calculate and print out the opening-allowed token $TK_M = H_1(M)^\mu$.

GVf(gpk, M, σ)

- Calculate $R_1{}' \leftarrow u^{s\alpha}{T_1}^{-c}$; $R_2{}' \leftarrow v^{s\beta}{T_2}^{-c}$; $R_3{}' \leftarrow h^{s\alpha+s\beta}{T_3}^{-c}$ $R_4{}' \leftarrow e(T_4, g)^{sx}\, e(g_1, \omega)^{-s\alpha}\, e(g_1, g)^{-s\alpha x}\, e(g_2, \omega)^{-s\beta} \cdot e(g_2, g)^{-s\beta x}\, e(g, \omega)^{-s\eta}\, e(g, g)^{-s\eta x}\, (e(g, g)/e(T_4, \omega))^{-c}$ $R_5{}' \leftarrow g^{s\rho}{T_5}^{-c}$; $R_6{}' \leftarrow e(g^{\mathrm{\mu}}, H_1(M))^{s\rho} e(g, g)^{-s\eta}\, {T_6}^{-c}$ $R_7{}' \leftarrow {T_1}^{sx} u^{-s\alpha x}$; $R_8{}' \leftarrow {T_2}^{sx} v^{-s\beta x}$; $R_9{}' \leftarrow {T_5}^{sx} g^{-s\rho x}$ $R_{10}{}' \leftarrow {T_6}^{sx} e(g^\mu, H_1(M))^{-s\rho x}\, e(g, g)^{s\eta x}$.
- Print out "valid" if the equation $c \leftarrow H_2(M, T_1, \ldots, T_6, R_1{}', \ldots, R_{10}{}')$ is completed, or "invalid" if the equation is not completed.

Open$(gpk, ok, M, \sigma, TK_M)$

- Verify the signature's validity first using the GVf algorithm. Print out $\perp$ when invalid.
- Verify the token's validity using $e(g^\mu, H_1(M)) = e(g, TK_M)$. Print out $\perp$ when invalid.
- Identify the signer i, who satisfies the equation below when the signature and the token are valid.

$$e(T_4/({T_1}^{\xi1}{T_2}^{\xi2}{T_3}^{\xi3}), g)\cdot(T_6/\mathrm{e}(T_5,TK_M)) = e(A_i, g).$$

- Print out i if there is an i that satisfies the equation. Print out $\perp$ if not.

Based on the assumption that the correctness of the proposed scheme is adequate while the decisional bilinear Diffie–Hellman problem and the decisional linear problem are difficult to solve, full anonymity can be achieved with a random oracle model. Also, the unforgeability of a signature (token) can be dealt with using the same model by assuming that the q-strong (computational) Diffie–Hellman problem is difficult to solve. The details of proof were omitted as they deviate from the research purpose.

In the following section, an anonymous signature scheme is proposed whereby a signer allows the opener to trace his/her identity by accessing his/her information or message to which he/she gave permission by issuing a token. The proposed scheme is expected to raise the level of privacy protection for the signer and can be used in a variety of systems, such as anonymous donation or corruption reporting systems.

4. Group Signature with Signer-Controlled Opening Capability: Separate Token Generator

Group signature schemes are considered a high-security cryptographic signature authentication system for protection of the signer′s privacy. The authenticator or the verifier of a signature is provided with a limited amount of information or authority when he/she verifies the signer′s affiliation with a certain group without knowing the latter′s true identity. Nevertheless, it is still possible for the opener to trace the identity when the situation makes it necessary to deal with malicious accesses. However, concerns about breaches of the signer′s privacy through the exposure of his/her personal information still remain. This chapter deals with such a problem by allowing the signer to issue a token with which the opener can access only those messages or items of information, including the signer′s identity, whose disclosure is approved.

4.1. Formal Model

The proposed anonymous signature method is composed of the following four algorithms:

KGen(1^{λ}): This is an algorithm where a trusted third party puts a security parameter λ to create public parameters for the running system *gpk*, an issuing key for the key issuer *ik*, and an opening key for the opener *ok*.

ISS/Join: This is an interactive algorithm between users and issuers that functions as an issuer issues gsk_i to a user in response to a user request.

GSig(gpk, i, gsk_i, M): This is an algorithm where an anonymous signer creates a signature σ using a group public key *gpk*, an index of the signer *i*, a signing key of the signer *i*, gsk_i, and a message *M*.

TKGen(gpk, i, gsk_i, M): This is an algorithm where an anonymous signer creates an opening-permission token TK_M using a group public key *gpk*, and an index of a signer *i*.

GVf(gpk, i, gsk_i, M): This is an algorithm where a signature verifier performs a verification of an anonymous signature using a group public key *gpk*, a message *M*, and an anonymous signature σ.

Open(gpk, ok, M, σ, TK_M): This is an algorithm where an opener checks the identity of an anonymous signer from an anonymous signature using an opening key of an opener *ok*, a message *M*, an anonymous signature σ, and a token TK_M.

4.2. Security Notion

Mihir Bellare et al. defined the general security model of a group signature method [12,13]. This paper suggests the following four security notions based on Bellare′s definition:

Correctness: The proper signature and proper token are always valid when verifying, and the opener with the right signature and the right token can always check the identification from the signature.

Full anonymity: The identity on the anonymous signature must remain inaccessible until the anonymous signer issues a token. When a token is issued, the identity must be inaccessible except by the opener with the token.

Signature unforgeability: Only the proper signer can create a valid anonymous signature for a specific message.

Token unforgeability: Only the proper signer can create a valid token for a specific signature.

4.3. Proposed Scheme

GKg$(1^\lambda, 1^n)$

- Define the two hash functions: H_1: $\{0, 1\}^* \rightarrow G$, H_2: $\{0, 1\}^* \rightarrow Z_p$.
- Select a parameter of the bilinear group (p, G, G_T, e, g, g_z).
- Select a random element $u, v, h \in G\backslash\{1\}$, a random integer $\xi_1, \xi_2, \xi_3, \gamma \in Z_p$, and calculate $g_1 = u^{\xi 1} h^{\xi 3}$, $g_2 = v^{\xi 2} h^{\xi 3}$, $\omega \leftarrow g^\lambda$.
- Print out the group public key $gpk \leftarrow (p, G, G_T, e, g, g_z, u, v, h, g_1, g_2, \omega, H_1, H_2)$, and issue key λ, the opener's opening key $ok \leftarrow (\xi_1, \xi_2, \xi_3, e(A_i, g)_{1 \le i \le n})$.

ISS/Join

- User i selects random $y_i \in Z_p$ and calculates $S_i \leftarrow {g_z}^{yi}$.
- User i sends S_i to the issuer.
- Issuer selects random $x_i \in Z_p$ and calculates $A_i \leftarrow (g{g_z}^{yi})^{1/(\gamma + xi)}$.
- Issuer sends A_i, x_i to user i.
- User i obtains the signing key $gsk_i = (A_i, x_i, y_i)$.

GSig(gpk, i, gsk_i, M)

- Select a random integer $\alpha, \beta, \rho, \eta \in Z_p$.
- Calculate $(T_1, T_2, T_3, T_4) \leftarrow (u^\alpha, v^\beta, h^{\alpha+\beta}, {g_1}^\alpha {g_2}^\beta A_i g^\eta)$ and $(T_5, T_6, T_7) \leftarrow (g^\rho, e(T_5, g)^{yi}, e(T_5, H_1(M))^{yi} e(g, g)^{-\eta})$.
- Select a random integer $r_\alpha, r_\beta, r_y, r_\eta, r_x, r_{\alpha x}, r_{\beta x}, r_{\eta x} \in Z_p$.
- Calculate $R_1 \leftarrow u^{r\alpha}$; $R_2 \leftarrow v^{r\beta}$; $R_3 \leftarrow h^{r\alpha + r\beta}$ $R_4 \leftarrow e(T_4, g)^{rx}\, e(g_1, \omega)^{-r\alpha}\, e(g_1, g)^{-r\alpha x}\, e(g_2, \omega)^{-r\beta} \cdot e(g_2, g)^{-r\beta x}\, e(g, \omega)^{-r\eta}\, e(g, g)^{-r\eta x}\, e(g_z, g)^{-ry}$ $R_5 \leftarrow e(T_5, g)^{ry}$; $R_6 \leftarrow e(T_5, H_1(M))^{ry} e(g, g)^{-r\eta}$ $R_7 \leftarrow {T_1}^{rx} u^{-r\alpha x}$; $R_8 \leftarrow {T_2}^{rx} u^{-r\beta x}$; $R_9 \leftarrow {T_6}^{rx} e(T_5, g)^{-ryx}$ $R_{10} \leftarrow {T_7}^{rx} e(T_5, H_1(M))^{ryx} e(g, g)^{-r\eta x}$ $c \leftarrow H_2(M, T_1, \ldots, T_7, R_1, \ldots, R_{10})$ $s_\alpha \leftarrow r_\alpha + c\alpha$; $s_\beta \leftarrow r_\beta + c\beta$; $s_y \leftarrow r_y + cy$ $s_\eta \leftarrow r_\eta + c\eta$; $s_x \leftarrow r_x + cx_i$; $s_{\alpha x} \leftarrow r_{\alpha x} + c\alpha x_i$ $s_{\beta x} \leftarrow r_{\beta x} + c\beta x_i$; $s_{\rho x} \leftarrow r_{\rho x} + c\rho x_i$; $s_{\eta x} \leftarrow r_{\eta x} + c\eta x_i$.
- Print out $\sigma \leftarrow (T_1, \ldots, T_7, c, s_\alpha, s_\beta, s_y, s_\eta, s_x, s_{\alpha x}, s_{\beta x}, s_{\rho x}, s_{\eta x})$.

TKGen(gpk, i, gsk_i, M)

- Print out $TK_M = H_1(M)^{yi}$.

GVf(gpk, M, σ)

- Calculate $R_1{}' \leftarrow u^{s\alpha} {T_1}^{-c}$; $R_2{}' \leftarrow v^{s\beta} {T_2}^{-c}$; $R_3{}' \leftarrow h^{s\alpha + s\beta} {T_3}^{-c}$ $R_4{}' \leftarrow e(T_4, g)^{sx}\, e(g_1, \omega)^{-s\alpha}\, e(g_1, g)^{-s\alpha x}\, e(g_2, \omega)^{-s\beta}\, e(g_2, g)^{-s\beta x} \cdot e(g, \omega)^{-s\eta}\, e(g, g)^{-s\eta x}\, e(g_z, g)^{-sy}\, (e(g, g)/e(T_4, \omega))^{-c}$ $R_5{}' \leftarrow e(T_5, g)^{sy} {T_6}^{-c}$; $R_6{}' \leftarrow e(T_5, H_1(M))^{sy} e(g, g)^{-s\eta}\, {T_7}^{-c}$ $R_7{}' \leftarrow {T_1}^{sx} u^{-s\alpha x}$; $R_8{}' \leftarrow {T_2}^{sx} u^{-s\beta x}$; $R_9{}' \leftarrow {T_6}^{sx} e(T_5, g)^{-syx}$ $R_{10}{}' \leftarrow {T_7}^{sx} e(T_5, H_1(M))^{syx} e(g, g)^{-s\eta x}$.
- Print out "valid" if the equation $c \leftarrow H_2(M, T_1, \ldots, T_7, R_1{}', \ldots, R_{10}{}')$ is completed, or "invalid" if the equation is not completed.

Open$(gpk, ok, M, \sigma, TK_M)$

- Verify the signature's validity first using the **GVf** algorithm. Print out $\perp$ if invalid.
- Find out the signer i, who satisfies the equation below, when the signature and the token are valid.

$$e(T_4/({T_1}^{\xi 1} {T_2}^{\xi 2} {T_3}^{\xi 3}), g) \cdot (T_7/\mathrm{e}(T_5, TK_M)) = e(A_i, g).$$

- Print out i if there is an i that satisfies the equation. Print out $\perp$ if not.

Determining correctness in an anonymous signature scheme is not that difficult in the proposed scheme when compared to proving the level of full anonymity. Nevertheless, it can be proven with a random oracle model when an assumption is made that the decisional bilinear Diffie–Hellman problem is not easy to solve. The unforgeability of a signature can be proven with the same model as above when it is assumed that the q-strong Diffie–Hellman problem is not easy to prove. The problem of the unforgeability of a token can be solved in a similar way, but the assumption should be made that the computational Diffie–Hellman problem is not easy to solve. The details of proof were omitted as they deviate from the research purpose.

This chapter provides a solution to signers' concerns about the exposure of their identities in the anonymous signature schemes. The issues pertaining to the excessive authority of the openers were covered by another study in which an admitter was added to the scheme to limit the power of the openers. However, as the possibility of successfully tracing the signer's identity still remained, this study proposed a method by which the signer issues a token him/herself without the intervention of the admitter. It is expected that, if the proposed method is applied to the existing anonymous signature schemes, their level of security will be improved significantly, thus alleviating the users' concerns.

5. Efficiency Comparison

A comparison of theoretical computational costs involved in the algorithms for the generation and verification of the group signatures is shown in Table 1. The group signature scheme in Reference [24] is a sort of a pairing-based group signature scheme which does not offer linkability, and is used for the comparison as a reference scheme. On the other hand, the group signature scheme in Reference [6] offers linkability by allowing the pre-defined linker to check the linkability of all the relevant signatures. Reference [25] introduced a scheme where the signer can control the linkability. When generating the random elements, the respective coefficients (integers) of variables G1, G2, and Zp indicate the individual number of generated random elements (i.e., 2 G1 + 1 G2 + 2 Zp indicates that two random elements were generated for G1, one random element for G2, and two random for Zp). Also, in the calculation formula, P represents the pairing operation; MG1 (or MG2) is the scalar multiplication operation for the group G1 (or G2); EGT is the exponentiation operation in the group GT. As such, the expression 6 P + 9 MG1 + 1 MG2 + 6 EGT implies that six pairings and nine scalar multiplications for G1, one scalar multiplication for G2, and six exponentiations for GT were performed by the algorithm which mainly focuses on the pairing tasks (Table 2), where the pairing operations were performed approximately six times more than the scalar multiplications.

Table 1. The computational costs of the group signatures calculated with the algorithms used by the major group signature schemes.

	Cost	**[24]**	**[6]**	**[25]**	**Our Scheme 1**	**Our Scheme 2**
Parameter generation	Elements	2 G1 + 1 G2 + 3 Zp	6 G1 + 1 G2 + 5 Zp	3 G1 + 2 G2 + 3 Zp	3 G1 + 5 Zp	3 G1 + 4 Zp
	Computation	2 M_{G1} + 1 M_{G2}	4 M_{G1} + 3 M_{G2}	2 M_{G1} + 1 M_{G2}	5 M_{G1}	5 M_{G1}
Key generation	Elements	1 Zp	3 Zp	2 Zp	1 Zp	2 Zp
	Computation	1 M_{G1}	3 M_{G1}	2 M_{G1}	1 M_{G1}	2 M_{G1}
Signature generation	Elements	7 Zp	9 Zp	9 Zp	14 Zp	12 Zp
	Computation	3 P + 9 M_{G1} + 3 E_{GT}	7 P + 16 M_{G1} + 7 E_{GT}	5 P + 9 M_{G1} + 6 E_{GT} + 2 M_{G2}	11 P + 22 M_{G1} + 10 E_{GT}	17 P + 16 M_{G1} + 16 E_{GT}
Verification	Computation	5 P + 8 M_{G1} + 4 E_{GT}	7 P + 16 M_{G1} + 4 E_{GT}	7 P + 9 M_{G1} + 7 E_{GT}	13 P + 16 M_{G1} + 12 E_{GT}	16 P + 14 M_{G1} + 15 E_{GT}

Table 2. Performance comparison.

	[24]	[6]	[25]	Our Scheme 1	Our Scheme 2
Parameter generation	0.0306 s	0.0645 s	0.0443 s	0.0151 s	0.0146 s
Key generation	0.0020 s	0.0057 s	0.0038 s	0.0018 s	0.0037 s
Signature generation	0.0498 s	0.1051 s	0.0997 s	0.1579 s	0.2153 s
Verification	0.0653 s	0.0933 s	0.0910 s	0.1653 s	0.1959 s

The operation of each group signature scheme (Table 2) was simulated with the computer (Intel Sandy Bridge i3 2330M 2.2-GHz processor, 4 GB random-access memory (RAM), Ubuntu 12.04), whereas the operations (pairing) were performed using the Python Pairing-Based Cryptography (PYPBC) Library, adopting the d224 curve, specifically. The resulting values are the averages of 100 simulations conducted for the individual schemes. The time required for the proposed scheme to generate and verify the signature was similar to that of References [6,24,25] and the same level of similarity was found in the computational costs. This means that the function "signer-controlled opening capability" being added to the computation process did not actually affect the computational costs much. Meanwhile, the proposed algorithm in this study was developed in a way that it can be adopted in previous research [26–32] pertaining to smart grids.

6. Conclusions

The group signature scheme is an electronic signature scheme with which a signer can prove that he/she is a member of a certain group without revealing his/her own identity, and which allows the authenticator to make a judgment on whether the signature is written by the same person or not, but which does not allow the authenticator to know the identity of the signer. A number of previous studies flexibly applied group signature schemes to various applications.

Meanwhile, the proposed algorithm in this study was developed in a way that it can be adopted in previous research [26–32] pertaining to smart grids.

Thus, two anonymous signature schemes in a smart grid environment were proposed in this study: a scheme where the anonymous signer issues a token to let the opener identify him/her only for the designated signature, and another scheme which requires the signer's consent for identification. In the former, the signer generates the token along with his/her signature using a short-term secret key, whereas, in the latter, the token is generated using a long-term secret key only when the signer agrees to disclose his/her identity after entering the signature. Although there is a possibility of compromising the security a little when the latter scheme is adopted, the burden of the signer having to issue and keep the token all the time can be lightened, improving the convenience of the scheme.

Author Contributions: Conceptualization, S.E. and J.-H.H. Data curation, S.E. and J.-H.H. Formal analysis, S.E. Methodology, J.-H.H. Project administration, J.-H.H. Resources, S.E. and J.-H.H. Visualization, S.E. and J.-H.H. Writing—original draft, S.E. and J.-H.H. Writing—review and editing, J.-H.H.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2017R1C1B5077157).

Acknowledgments: The first draft of this paper was presented at The International Conference on Big data, IoT, and Cloud Computing (BIC 2017) [31,33], 22–24 August 2017, Republic of Korea.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Huh, J.H. *Smart Grid Test Bed Using OPNET and Power Line Communication*; IGI Global: Hershey, PA, USA, 2017; pp. 64–89.

2. Freitas, W.; Vieira, J.C.; Morelato, A.; Xu, W. Influence of Excitation System Control Modes on the Allowable Penetration Level of Distributed Synchronous Generators. *IEEE Trans. Energy Convers.* **2005**, *20*, 474–480. [CrossRef]
3. Dandeno, P.L.; Karas, A.N.; McClymont, K.R.; Watson, W. Effect of High-Speed Rectifier Excitation Systems on Generator Stability Limits. *IEEE Trans. Power Appar. Syst.* **1968**, *PAS-87*, 190–201. [CrossRef]
4. Wang, D.; Mao, C.; Lu, J. Coordinated Control of EPT and Generator Excitation System for Multidouble-Circuit Transmission-Lines System. *IEEE Trans. Power Deliv.* **2008**, *23*, 371–379. [CrossRef]
5. Park, S.; Huh, J.H. Effect of Cooperation on Manufacturing IT Project Development and Test Bed for Successful Industry 4.0 Project: Safety Management for Security. *Processes* **2018**, *6*, 88. [CrossRef]
6. Hwang, J.Y.; Chen, L.; Cho, H.S.; Nyang, D. Short dynamic group signature scheme supporting controllable linkability. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1109–1124. [CrossRef]
7. Chaum, D.; van Heyst, E. Group Signatures. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, 8–11 April 1991; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
8. Hwang, J.Y.; Eom, S.; Chang, K.; Lee, P.J.; Nyang, D. Anonymity-Based Authenticated Key Agreement with Full Binding Property. In Proceedings of the International Workshop on Information Security Applications, Jeju Island, Korea, 16–18 August 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 177–191.
9. Sakai, Y.; Emura, K.; Hanaoka, G.; Kawai, Y.; Matsuda, T.; Omote, K. Group Signatures with Message-Dependent Opening. In Proceedings of the International Conference on Pairing-Based Cryptography, Cologne, Germany, 16–18 May 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 270–294.
10. Ohara, K.; Sakai, Y.; Emura, K.; Hanaoka, G. A group signature scheme with unbounded message-dependent opening. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013; pp. 517–522.
11. McClanahan, R. SCADA and IP: Is Network Convergence Really Here? *IEEE Ind. Appl. Mag.* **2003**, *9*, 29–36. [CrossRef]
12. Fan, J.; Borlase, S. The Evolution of Distribution. *IEEE Power Energy Mag.* **2009**, *7*, 63–68.
13. Farhangi, H. The Path of the Smart Grid. *IEEE Power Energy Mag.* **2010**, *8*, 18–28. [CrossRef]
14. NIST. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*; NIST Special Publication: Gaithersburg, MD, USA, 2012.
15. Mark, J. New Electricity Grids May Be Smart, but Not so Private—The Denver Post. 18 May 2010. Available online: http://www.denverpost.com/business/ci_15106430 (accessed on 9 September 2018).
16. Siddiqui, F.; Zeadally, S.; Alcaraz, C.; Galvao, S. Smart grid privacy: Issues and solutions. In Proceedings of the 2012 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 July–2 August 2012.
17. Cheung, J.; Chim, T.; Yiu, S.; Li, V. Credential-based privacypreserving power request scheme for smart grid network. In Proceedings of the IEEE Global Telecommunications Conference, Kathmandu, Nepal, 5–9 December 2011; pp. 1–5.
18. Marmol, F.; Sorge, C.; Ugus, O.; Perez, G. Do not snoop my habits: Preserving privacy in the smart grid. *IEEE Commun. Mag.* **2012**, *50*, 166–172. [CrossRef]
19. Zeadally, S.; Pathan, A.; Alcaraz, C.; Badra, M. Towards privacy protection in smart grid. *Wirel. Pers. Commun.* **2013**, *73*, 23–50. [CrossRef]
20. Badra, M.; Zeadally, S. Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 321–329. [CrossRef]
21. Hoenkamp, R.; Huitema, G.B.; de Moor-van Vugt, A.J. The neglected consumer: The case of the smart meter rollout in the Netherlands. *Renew. Energy Law Policy Rev.* **2011**, *2*, 269–282. [CrossRef]
22. Ptzmann, A.; Hansen, M. A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Available online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (accessed on 9 September 2018).
23. Tudor, V.; Almgren, M.; Papatriantafilou, M. Analysis of the impact of data granularity on privacy for the smart grid. In Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society, Berlin, Germany, 4–8 November 2013.

24. Boneh, D.; Boyen, X.; Shacham, H. Short group signature. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 15–19 August 2004; Springer: Berlin/Heidelberg, Germany, 2004.
25. Eom, S.; Huh, J.H. Group signature with restrictive linkability: Minimizing privacy exposure in ubiquitous environment. *J. Ambient Intell. Humaniz. Comput.* **2018**, *1*, 1–11. [CrossRef]
26. Yu, C.M.; Chen, C.Y.; Kuo, S.Y.; Chao, H.C. Privacy-Preserving Power Request in Smart Grid Networks. *IEEE Syst. J.* **2014**, *8*, 441–449. [CrossRef]
27. Ciabattoni, L.; Comodi, G.; Ferracuti, F.; Fonti, A.; Giantomassi, A.; Longhi, S. Multi-apartment residential microgrid monitoring system based on kernel canonical variate analysis. *Neurocomputing* **2015**, *170*, 306–317. [CrossRef]
28. Ancillotti, E.; Bruno, R.; Conti, M. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun.* **2013**, *36*, 1665–1697. [CrossRef]
29. Kim, S.K.; Huh, J.H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
30. Lee, H.G.; Huh, J.H. A Cost-Effective Redundant Digital Excitation Control System and Test Bed Experiment for Safe Power Supply for Process Industry 4.0. *Processes* **2018**, *6*, 85. [CrossRef]
31. Eom, S.; Huh, J.H. Anonymous Signature with Signer-Controlled Opening Capability. In *Advances in Computer Science and Ubiquitous Computing*; Springer: Singapore, 2017; pp. 878–882.
32. Bellare, M.; Micciancio, D.; Warinschi, B. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Warsaw, Poland, 4–8 May 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 614–629.
33. Eom, S.; Huh, J.H. *Group Signature with Signer-Controlled Opening Capability: Separate Token Generator, In Advances in Computer Science and Ubiquitous Computing*; Springer: Singapore, 2017; pp. 883–887.