Elliptic curve cryptography-based authentication with identity protection for smart grids

Elliptic curve cryptography-based authentication with identity protection for smart grids

L. Zhang, Shanyu Tang, and H. Luo

Abstract

In a smart grid, the power service provider enables the expected power generation amount to be measured according to current power consumption, thus stabilizing the power system. However, the data transmitted over smart grids are not protected, and then suffer from several types of security threats and attacks. Thus, a robust and efficient authentication proto- col should be provided to strength the security of smart grid networks. As the Supervisory Control and Data Acquisition system provides the security protection between the control center and substations in most smart grid environments, we focus on how to secure the communications between the substations and smart appliances. Existing security approaches fail to address the performance-security balance. In this study, we suggest a mitigation authentication protocol based on Elliptic Curve Cryptography with privacy protection by using a tamper-resistant device at the smart appliance side to achieve a delicate balance between performance and security of smart grids. The proposed protocol provides some attractive features such as identity protection, mutual authentication and key agreement. Finally, we demonstrate the completeness of the proposed protocol using the Gong- Needham- Yahalom logic.

Introduction

Compared with traditional power networks, smart grid networks can avoid excess electricity generation by adjusting the amount of electricity based on the customer's real-time requirements. In general, the smart grid network can be divided into three levels: control center, sub- stations and smart appliances [1]. In a smart grid network, smart appliances communicate with substations by using smart meters. The smart meters send user's requirements to the sub- stations, and then the substations transmit the requirements to the control center. Next, according to the received requirements, the control center can allocate adequate power supplies to customers. The Supervisory Control and Data Acquisition system is used to protect the communications between the control center and the substations [2], but the security problems between other two levels remain unsolved. Although the security mechanisms between substations and smart appliances have been researched in recent years, existing security protocols are not robust enough to resist several types of attacks. Therefore, a determined effort should be made to address the security issues associated with the communications between the substations and the smart appliances [3].

As smart meters are used to transmit the real-time electricity demands from customers, the data transmission process could easily suffer from several types of security threats and attacks. To protect the transmitted data, an efficient authentication scheme should be provided. Compared with the authentication protocols designed for other scenarios such as VoIP and Ad Hoc networks, it is more challenging to provide a suitable authentication protocol for smart grids due to its complicated architecture and diverse security requirements. On one hand, the authentication protocols should secure

against various types of possible attacks and provide several security features to satisfy the secure requirements of smart grids. For example, the user privacy should be fully considered especially the user's identity protection, to prevent the adversary from obtaining the information about user's daily patterns, which may not be important in other application environments. On the other hand, smart grid communications are more sensitive to transmission latency, and so existing security approaches with intensive computation are impractical in smart grid networks.

Recently, several authentication protocols have been proposed [4–19] to protect the data transmission between communication entities. In an attempt to prevent the adversary from obtaining the daily habit of the customer through analyzing the electricity usage pattern, T.W. Chim et al. [4] designed an authentication protocol by using a tamper-resistant device at the smart appliance and a pseudo identity for the smart grid network to protect the privacy of the customer. However the proposed protocol was suffered from impersonation attacks. Since only substations could authenticate smart appliances, the adversary could easily impersonate the substations to cheat the smart appliances. Besides, their protocol failed to provide a key agreement function capable of protecting the communication between substations and smart appliances. Furthermore, since a timestamp was used in the signing module of their protocol, the clock synchronization problem could not be avoided. In order to reduce the computational cost, Mostafa et al. [5] proposed a message authentication mechanism by using the Computational Diffie-Hellman assumption for smart grids. In their protocol, mutual authentication and key agreement were realized by using Diffie-Hellman exchange protocol between the smart meters distributed at different hierarchical networks of the smart grid system, and the subsequent messages could be

authenticated by using a shared session key established previously and the hash-based authentication code technique. However, the computational costs of both protocols were still very high due to the usage of expansive exponential operations. In the same year, Qing et al. [6] designed a multicast authentication protocol for smart grids by using one- time signature to reduce the storage cost and the signature size. Because the one-time signature-based multicast authentication could provide short authentication delay and low computation cost, their protocol achieved a good performance. However their work only focused on designing a light-weight authentication protocol, remained the key agreement issue unsolved.

In order to strengthen the security of smart grid communications, Soohyun Oh et al. [7] suggested a mutual authentication and key establishment mechanism based on public key certificates for smart grid. In their protocol, the data concentration unit's public key certificate and pre-shared long-term key were used to realize the mutual authentication between the data concentration unit and the intelligent devices. But the problem of distributing the shared long- term key limited this protocol's scalability and applicability. Biometric technique such as fingerprint was also adopted to achieve strong authentication for smart grids [10]. But these protocols are very complex due to the use of biometrics. In 2013, Binod Vaidya et al. proposed an authentication and authorization mechanism for smart grid networks [13]. They realized multi-factor authentication and attribute-based authorization in a smart grid environment by using public key certificates, zero-knowledge and access control technologies. But the heavy computational load could not be avoided since the implement of the public key certificates management and public key cryptography calculation. In the same year, Nicanfar et al. presented a password authenticated group key agreement protocol for

smart grid [15]. Although the proposed protocol provided forward and backward secrecy and enhanced the security of communications among the devices, the usage of expansive exponential operations decreased the practical application of the protocol. To reduce the computational cost, a password authenticated key exchange based on Elliptic Curve Cryptography (ECC) was proposed [17]. Com- pared with previous studies, this protocol was more efficient due to the usage of ECC, but a primitive password should be preloaded between an appliance and the Home Area Network controller, which made this solution hard to scale and might arouse an intractable problem of password table maintenance. Recently, Li et al. proposed fault-diagnosable authentication architecture for advanced metering infrastructure in smart grid [19]. Since this work only focused on authentication, key negotiation was not considered in the proposed authentication mechanism.

According to above analysis, protocol [4] was suffered from impersonate attacks and proto- cols [5, 19] were vulnerable to eavesdropping since these protocols could not provide key agreement to protect the further communications. Moreover, protocol [17] faced some attacks associated with password. Although some of these protocols achieved good performance, they could not provide security at an acceptable level. Furthermore, other protocols such as [13, 15] were secure against several attacks, but the use of expansive exponential operations, the signature generation, and the verification lead to high computational overhead and communication delay. Therefore, these protocols are not suitable for smart grid. In general, the existing authentication protocols for smart grids mentioned above are insecure against some cryptographic attacks or impractical due to high computational costs. In addition, all the protocols discussed above could not provide privacy protection which is very important in smart

grids. Based on these motivations, we proposed a robust and efficient authenticate protocol based on Elliptic Curve Cryptography (ECC) with identity protection for smart grids by using tamper-resistant attractive security properties. As ECC can achieve the same level security with a smaller key size, it offers better performance compared with other public key cryptosystems such as RSA or D-H. Thus, we adopted ECC to realize a mitigation authentication device at the smart appliance without involving time-consuming operations.

Compared with other security approaches, public key cryptosystems can resist most of possible attacks and provide more security properties to achieve a good balance between performance and security. By using ECC, the proposed protocol can achieve the authenticated key agreement with privacy protection at a lower computational cost. Furthermore, according to the characteristics of the smart grid, the control center can be considered fully trustable since it is managed by the government administrators; the substations that have higher computational power are difficult to be compromised than smart appliances; the smart appliances with limited power are more vulnerable to various attacks, and it can be combined with a tamper-resist device to protect the stored information. Taking advantage of above features, in the proposed protocol, a tamper-resist device was used to store secret information to help providing privacy protection through the authentication process. In addition, the control center and the substations can cooperate to complete the initialization process of the authenticated key agreement protocol.

In the proposed protocol, the smart meters are used to transmit the real-time electricity demands from customers intelligently. In order to protect the transmitted data, mutual

authentication and a shared key should be provide to protect the further communication between the substation and the smart appliances. In the proposed protocol, the smart meters could control when the authentication protocol begins and which appliances need to be authenticated. Furthermore, the shared key updating could be realized by restarting the authentication pro- cess and the smart meter could also control the period of key updating during the communication. Therefore, the smart meter could manage the smart devices intelligently during the authentication process. In this paper, our study focused on the design of the authentication protocol with privacy protection, so the intelligent management of smart meters is beyond the scope of our work.

Burrows-Abadi-Needham (BAN) Logic [20] is the first belief logic widely used to formally analyze the completeness of a cryptographic protocol, but it has some limitations [21]. Gong- Needham-Yahalom (GNY) logic [22] is one of the famous extensions to overcome the inherent limitations of BAN; and it has successfully disclosed redundancies or found defects in several protocols. Today, GNY has been used to demonstrate the completeness of several protocols successfully [23]. Therefore, we used the GNY logic to evaluate the security of the proposed protocol in this study.

The rest of this paper is organized as follows. Section 2 briefly describes the Elliptic Curve Cryptosystem. Our newly designed authentication protocol is detailed in Section 3. In Section 4, the completeness of the proposed protocol is proved through Gong-Needham-Yahalom logic. The performance of the proposed protocol is evaluated in Section 5, and the paper is concluded in Section 6.

Preliminaries

In this section we briefly introduce the basic concepts of the elliptic curve cryptosystem and the corresponding problems associated with it. We also explain the reason for adopting the elliptic curve cryptography.

ECC has been formally applied to public key cryptosystems since 1986. In an elliptic curve cryptosystem, the elliptic curve equation is defined as the form $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod{p}$ over a prime finite field F_p, where $p > 3$, $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \pmod{p}$. Given an integer $t \in F_p^*$ and a point $P \in E_p(a,b)$, the scalar multiplication tP over $E_p(a,b)$ can be defined as $tP = P + P + \ldots + P$(t times) [24]. And the corresponding problems associated with ECC are shown as follows:

Definition 1. Given two points P and Q over $E_p(a,b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $t \in 2\ F_p^*$ such that $Q = tP$.

Definition 2. Given three points P, sP and tP over $E_p(a,b)$ for s; $t \in 2\ F_p^*$, the computational Diffie-Hellman problem (CDHP) is to find the point stP over $E_p(a,b)$.

Definition 3. Given two points P and $Q = sP + tP$ over $E_p(a,b)$ for s; $t \in 2\ F_p^*$, the elliptic curve factorization problem (ECFP) is to find two points sP and tP over $E_p(a,b)$.

We assume that the three problems above are intractable. That is, there is no polynomial time algorithm that can solve these problems with non-negligible probability.

Next, we explain why we adopted ECC to design the authentication protocol for smart grid networks.

1) More complex: Since ECC can be implemented in different ways rather than a single encryption algorithm; it is more complex than RSA. Moreover, the elliptic curve discrete logarithm problem is more difficult to break than the factorization and discrete logarithm problem. Although many researchers have tried to attack ECC, it is still infeasible to break ECC with existing computational resources. Therefore, the security strength of ECC is much stronger than other public key cryptosystems such as RSA or Diffie-Hellman (D-H).

Table 1. Comparison of the key length between RSA and ECC on the same security level.

Key length of ECC (bits)	Key length of an RSA (bits)	Key length ratio
160	1024	1:6
256	3072	1:12
384	7680	1:20
512	15,360	1:12

2) Smaller key size: as shown in Table 1, compared with RSA, ECC offers equivalent security with smaller key sizes which implies lower power, bandwidth, and computational requirements. These advantages are very important when public-key cryptography is implemented for low power environments.

3) Computational efficiency: ECC is much more efficient than RSA and D-H public proto- cols in terms of computation, since implementing scalar multiplication

in software and hard- ware is much more feasible than performing multiplications or exponentiations in them.

According to above attractive properties of ECC, we chose it to design the proposed robust and efficient authentication protocol for smart grids.

Our Proposed Authentication Scheme

This section details our newly designed authentication protocol based on elliptic curve cryptography for smart grids. Considering the efficiency, ECC version for El-Gamal has been adopted for asymmetric encryption in the proposed protocol where the cycle group used in El-Gamal is taken from elliptic-curve. For the details, please see [24]. There were two phases in the pro- posed protocol: initialization phase and authentication phase. The procedure of our protocol is described in detail as follows:

Initialization phase

In this phase, several security parameters used for authentication and key agreement are calculated by the control center and the substations.

1) First, an elliptic curve equation $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod p$ over a prime finite field F_p is selected by the control center. Here $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0 \pmod p$. Next the control center chooses a base point P over $E_p(a, b)$ and writes P to the tamper-resistant device of U_i as well as the substations.

2) The control center allocates an identity ID_i for each smart appliance U_i and

preloads ID_i into the memory of the corresponding tamper-resistant devices. Then the identity ID_i of smart appliance U_i is written in an *ID* table by the control center. Next, the control center submits the identity table to the substation over a secure channel and assigns an identity SID_j for each sub- station S_j. The substation S_j stores the identity SID_j in its memory securely. Finally, a one-way hash function $h(\cdot)$: $\{0,1\}^* \rightarrow \{0,1\}^k$ is selected by the control center. And the substations as well as the tamper-resistant devices store the hash function in their memories.

3) The substation chooses a random integer $s \in_R Z_p^*$ as a secret key for symmetric encryption/ decryption. And then it generates a random integer $sk < n$ as a private key and computes its corresponding public key $pk = skP$, where n is the order of the base point P. The computed public/ private key pair (pk, sk) is used for asymmetric encryption/decryption. Then the substation calculates $C_1 = E_s(ID_i)$ and $C_2 = SID_jP$ for every smart appliance U_i. The system key s and the public/private key pair (pk, sk) are kept secret by the substation. Furthermore, the substation writes the public key pk and the pair secret (C_1, C_2) into each corresponding tamper-resistant device.

If a new smart appliance U_j wants to incorporate into the smart grid, the control center and the substation should cooperate to complete the initialization of the new appliance. First, the control center allocates a new identity ID_j for U_j and records it in the *ID* table. Then it sends the identity of the new smart appliance to the corresponding substation over a secure channel. Having received the message, the substation records the identity in its *ID* table and then computes a

secret (C_1, C_2) for the new smart appliance. Finally, the substation writes the point P, the one-way hash function, the identity ID_j, the public key pk and the pair secret (C_1, C_2) into the tamper-resistant device of U_j to achieve the initialization of the new smart appliance.

Authentication phase

During the authentication process, the substation and the smart appliance Ui perform the following four steps to realize mutual authentication and key agreement.

1) First, the tamper-resistant device of U_i selects an integer $r_1 \in_R Z_p^*$ randomly to compute $C_3 = e_{pk}(ID_i \| C_1 \| r_1)$, where $e_{pk}(\bullet)$ denotes the public key encryption function using the substation S_j's public key pk and $C_1 = E_s(ID_i)$ is a secret stored in the tamper-resistant device of U_i. Then, the smart appliance U_i sends $C_3 = e_{pk}(ID_i \| C_1 \| r_1)$ to the substation S_j.

2) In this step, the substation S_j obtains ID_i, C_1 and r_1 by decrypting the receiving message C_3 via its private key sk. Then, it checks whether ID_i is valid by matching it in the ID table. If not valid, the authentication process stops. Otherwise, the substation S_j uses the system key s to decrypt C_1 and then gets the ID_i. Next, it compares the value of ID_i in C_3 with that of ID_i in decrypted message C_1. If they are not equivalent, the substation terminates the authentication process; otherwise, the substation chooses two random integers $r_2 \in_R Z_p^*$ and $r_3 \in_R Z_p^*$ to calculate the shared session key $SK = h(r_1 \| r_2)$ and

authentication message $C_4 = E_{r_1}(SID_j \| r_2)$, where $E_{r1}(\bullet)$ denotes the secure symmetric encryption algorithm with the secret key r_1. Finally, the substation S_j submits the message (C_4, r_3) to U_i.

Here the random integer r_3 needs not be encrypted because it is used to check the freshness of the message only and is not connected with the final session key in any way. Even if the adversary obtained the random integer r_3, the shared key could not be compromised. Thus, the random integer r_3 is transmitted in plaintext, and this method has been widely used in authentication protocols to check the freshness of the message.

3) After receiving the message (C_4, r_3), the smart appliance U_i adopts r_1 to decrypt C_4 and then obtains r_2 and SID_j. Then it calculates SID_jP and checks whether the following equation holds $C_2 = SID_jP$. If the equation holds, the smart appliance U_i calculates the shared session key $SK' = h(r_1 \| r_2)$ and the authentication message $C_5 = h(SK' \| (r_3 + 1))$. And then U_i submits the authentication message C_5 to the substation S_j. Otherwise, the smart appliance U_i rejects the message and terminates the authentication process.

4) Upon receiving the message C_5, the substation S_j checks whether the value of the received C_5 equals to the value of the computed $h(SK \| (r_3 + 1))$. If true, the substation S_j sets SK as the shared session key with the smart appliance U_i; otherwise, it terminates the authentication process.

In the proposed protocol, if the substation D_n needs to be changed, it submits all

the shared keys between itself and corresponding smart appliance to the control center over a secure channel and then deletes the *ID* table and the shared keys from its memory. Next the control center transforms *ID* table including all identities of the smart appliance associated with substation D_n and all the session keys submitted from D_n to the new substation D_l over a secure channel. In addition, the control center also chooses a secure one-way hash function and transforms it to the substation D_l. After the substation D_l finishes the initialization procedure, it adopts the corresponding shared key to encrypt the secret information including the pair secret (C_1, C_2), the public key *pk* and the hash function. Then the substation D_l can transmit the secret information securely to the corresponding smart appliance. Consequently, the tamper-resistant devices can update the secret information securely. And the new session key between the new substation D_l and the smart appliance can be achieved by running the proposed key agreement protocol to realize the secure and easy change of the substation.

In the proposed protocol, instead of preloading the shared key, the secret (C_1, C_2) as "material" is stored in the tamper-resistant device of the smart appliance to help realize mutual authentication and key agreement. The session key is constructed by two high-entropy random integers chosen by the substation and the smart appliance freely, and the session key varies in each authentication and key agreement process, that is, the secret (C_1, C_2) is not connected with the final computed session key. Thus, even the secret (C_1, C_2) stored in the tamper-resistant device was compromised, the session key would not be leaked and the adversary could not obtain the information transmitted between the smart appliance and the substation encrypted by the session key. Under this case, if the secret (C_1, C_2) was compromised, the message relayed

between the smart appliance and the substation would not be exposed to the adversary. On the contrary, if the shared key was preloaded into a tamper-resistant device, the adversary could launch the capture attack to obtain the shared key, and then could use it to decrypt the message communicated between the smart appliance and the substation. In addition, the solution of preloading the shared key requires the substation storing the shared keys for each smart appliance. Once the substation was compromised by the adversary, all the shared keys would be revealed. Furthermore, the associated problems of shared key updating and maintaining make this security measure hard to scale up.

Security Analysis

Burrows-Abadi-Needham Logic [20] is the first belief logic which has been widely used to formally analyze the completeness of protocols. A great effort has been put into overcoming its limitations [21]. Gong-Needham-Yahalom (GNY) logic [22] is one of these extensions. And it has successfully disclosed redundancies or found defects in several protocols. Therefore, we adopted the GNY logic to evaluate the security of our proposed protocol.

In this section, some formulae and statements used in the GNY logic are introduced first; then the goals and the assumptions of the proposed protocol are set; finally the GNY logic is adopted to prove that the proposed protocol is valid and practical.

Formulae and statements

In the GNY logic, a formula is a name used to refer to a bit string, which has a

particular value in a run [22]. In order to describe the GNY logic, first let symbols *X* and *Y* range over formulae. Then, some formulae used in our authentication proof are introduced and the complete list of all logical postulates is described in [22].

1. (*X*, *Y*): conjunction of two formulae *X* and *Y*.

2. $\{X\}_K$ and $\{X\}_K^{-1}$: symmetrically encrypt and decrypt *X* with the key *K*.

3. $\{X\}_{+K}$ and $\{X\}_{-K}$: asymmetrically encrypt and decrypt *X* with the public key +*K* and the private key -*K*.

4. *h*(*X*): a one-way function of *X*.

5. $^*X$: *X* is not originated here.

3. $\{X\}_{+K}$ and $\{X\}_{-K}$: asymmetrically encrypt and decrypt *X* with the public key +*K* and the private key -*K*.

4. *h*(*X*): a one-way function of *X*.

5. $^*X$: *X* is not originated here.

A basic statement reflects some property of a formula. Let symbols *P* and *Q* be principals. The following are statements used in our authentication proof.

1. $P \lhd X$: *P* is told formula *X*.

2. $P \ni X$: *P* possesses formula *X*.

3. $P|\sim X$: *P* once conveyed formula *X*.

4. $P|\equiv \#(X)$: *P* believes that *X* is fresh.

5. $P|\equiv \phi(X)$: *P* believes that *X* is recognizable.

6. $P|\equiv P \xleftrightarrow{S} Q$: *P* believes that *S* is a suitable secret for *P* and *Q*.

7. $P|\Rightarrow X$: P has jurisdiction over X.

8. $P \lhd^{*} X$: P is told that a formula X which did not convey previously in the current run.

Protocol descriptions and goals

In this subsection, some notations are changed to fit the GNY logic and the proposed protocol are transformed into the form of $P \rightarrow Q$:(X). In addition, the server's private key is denoted as $-K$ and the corresponding public key is denoted as $+K$.

1. $U \rightarrow S : (\{ID_i \| \{ID_i\}_s \| c\}_{+K})$

2. $S \rightarrow U : (\{SID_j \| d\}_c, r)$

3. $U \rightarrow S : (h(h(c \| d) \| (r+1)))$

Next, our goals which consist of three aspects are described in detail.

(1) Message content authentication

Goal 1: S believes the message in the first run is recognizable.

$$S|\equiv \phi\{ID_i \| \{ID_i\}_s \| c\}_{+K}$$

Goal 2: U believes the message in the second run is recognizable.

$$U|\equiv \phi(\{SID_j \| d\}_c, r)$$

Goal 3: S believes the message in the third run is recognizable.

$$S|\equiv \phi(h(h(c \| d) \| (r+1)))$$

(2) Message origin authentication

Goal 4: U believes S conveyed the message in the second run.

$$U \mid\equiv S \mid\sim \{SID_j \| d\}_c$$

Goal 5: *S* believes *U* conveyed the message in the third run.

$$S \mid\equiv U \mid\sim h(h(c \| d) \| (r+1))$$

(3) Session key material establishment

Goal 6: *U* believes that *S* believes that *SK* is a secret shared between *U* and *S*.

$$U \mid\equiv S \mid\equiv U \xleftrightarrow{SK} S$$

Goal 7: *U* believes that *SK* is a secret shared between *U* and *S*.

$$U \mid\equiv U \xleftrightarrow{SK} S$$

Goal 8: *S* believes that *U* possesses *SK*.

$$S \mid\equiv U \ni SK$$

Goal 9: *S* believes that *U* believes that SK is a secret shared between *U* and *S*.

$$S \mid\equiv U \mid\equiv U \xleftrightarrow{SK} S$$

Assumption list

In this subsection, some assumptions are made as follows:

1. The secret key *s* is generated by *S* in the proposed protocol, so *S* possesses *s*. *S* also possesses the private key –*K* and the public key +*K*.

$$S \ni s, S \ni +K, S \ni -K$$

2. Since *S* keeps the identity table, *S* believes that ID_i is recognizable.

$$S \mid\equiv \phi(ID_i)$$

3. Since *U* stores $V_2 = SID_j P$ secretly and holds the base point *P*. Then *U* can check the SID_j and believes that SID_j is recognizable.

$$U \mid\equiv \phi(SID_j)$$

4. The random integer c is generated by U in the protocol, so U possesses c and believes that c is fresh. $U \ni c, U \mid\equiv \#(c)$

5. The random integer c is generated by U as part of the temporal session key in the current run. So, we assume that U believes c is a suitable secret for himself and S.

$$U \mid\equiv U \overset{c}{\longleftrightarrow} S$$

6. The random integer r and d are generated by S in the protocol, so S possesses r and d, and believes that r is recognizable and d is fresh.

$$S \ni r,\ S \mid\equiv \phi(r),\ S \ni d, S \mid\equiv \#(d)$$

7. The SK generated by S is a temporal session key in the current run. So we assume that S believes that SK is a suitable secret between itself and U.

$$S \mid\equiv S \overset{SK}{\longleftrightarrow} U$$

8. U believes that the server S is an authority on generating a suitable session key material SK shared between U and S.

$$U \mid\equiv S \mid\Rightarrow U \overset{SK}{\longleftrightarrow} S$$

Authentication proof using GNY logic

In this subsection, we adopt the GNY logic to analyze our protocol. A complete list of all logical postulates and the index in the list is provided [22], such as (T1, P1), to show how to achieve the goals.

(1) The first run:

$$\frac{S \mid\equiv \phi(ID_i), S \ni s}{S \mid\equiv \phi\{ID_i\}_s, S \mid\equiv \phi(ID_i \| \{ID_i\}_s \| c)} \qquad (R1, R2)$$

If *S* believes that ID_i is recognizable and *S* possesses the key *s*, then *S* is entitled to believe that the encryption of ID_i with the key *s* is recognisable and then the formula $\{ID_i \| \{ID_i\}_s \| c\}$ is also recognizable.

$$\frac{S \mid\equiv \phi(ID_i \| \{ID_i\}_s \| c), S \ni +K}{S \mid\equiv \phi\{ID_i \| \{ID_i\}_s \| c\}_{+K}} \qquad (R3)$$

If *S* believes $(ID_i \| \{ID_i\}_s \| c)$ is recognizable and *S* possesses a public key +*K*, then it believes that the encryption $\{ID_i \| \{ID_i\}_s \| c\}_{+K}$ is recognizable. Therefore, in the proposed protocol, the server *S* can recognize the message $\{ID_i \| \{ID_i\}_s \| c\}_{+K}$ in the first run. (Goal 1)

(2) The second run:

$$\frac{U \mid\equiv \phi(SID_j), U \ni c}{U \mid\equiv \phi(SID_j \| d), U \mid\equiv \phi\{SID_j \| d\}_c} \qquad (R1, R2)$$

If *U* believes that SID_j is recognizable, then *U* is entitled to believe that the formula $(SID_j \| d)$ of which SID_j is a component, is recognizable. Since *U* possesses *c*, it also believes that the encryption $\{SID_j \| d\}_c$ is recognizable.

$$\frac{S \mid\equiv \phi\{SID_j \| d\}_c}{S \mid\equiv \phi(\{SID_j \| d\}_c, r)} \qquad (R1)$$

If *S* believes $\{SID_j \| d\}_c$ is recognizable, then it is entitled to believe that $(\{SID_j \| d\}_c, r)$, of which $\{SID_j \| d\}_c$ is a component, is recognizable. So, we can conclude that in the proposed protocol, *U* can recognize the message $(\{SID_j \| d\}_c, r)$ in the second run. (Goal 2)

$$U < *\{SID_j \| d\}_c, U \ni c, \quad \frac{U \mid\equiv U \overset{c}{\longleftrightarrow} S, U \mid\equiv \phi(SID_j \| d), U \mid\equiv \#(c)}{U \mid\equiv S \mid\sim \{SID_j \| d\}_c, U \mid\equiv S \ni c} \qquad (I1)$$

If the following five conditions hold: 1) *U* receives the formula $(SID_j \| d)$ encrypted with the key *c* and marked with a not-originated-here mark; 2) *U* possesses *c*; 3) *U* believes that *c* is a suitable secret for itself and *S*; 4) *U* believes that the formula $(SID_j \| d)$ is recognizable; and 5) *U* believes that *c* is fresh. Then *U* is entitled to believe that 1) *S* once conveyed $(SID_j \| d)$ encrypted with *c* and 2) *U* believes that the *S* possesses *c*. (Goal 4)

According to the GNY logic, we assume that $U \mid\equiv S \mid\Rightarrow S \mid\equiv *$, that is, *U* believes that *S* is honest and competent, and then we can deduce the following statement:

$$U \mid\equiv S \mid\Rightarrow S \mid\equiv *, U \mid\equiv S \mid\sim (\{SID_j \| d\}_c, r)$$

$$\frac{\sim> S \mid\equiv U \overset{SK}{\longleftrightarrow} S), U \mid\equiv \#(\{SID_j \| d\}_c, r)}{U \mid\equiv S \mid\equiv U \overset{SK}{\longleftrightarrow} S} \qquad (J2)$$

If *U* believes that *S* is honest and competent; and *U* receives a message $(\{SID_j \| d\}_c, r) \sim> S \mid\equiv U \overset{SK}{\longleftrightarrow} S)$, which it believes *S* conveyed, then *U* ought to believe that *S* really believes $U \overset{SK}{\longleftrightarrow} S$. Therefore, *U* believes that *S* believes that *SK* is a suitable secret between *U* and *S*. (Goal 6)

$$\frac{U \mid\equiv S \mid\Rightarrow U \overset{SK}{\longleftrightarrow} S, U \mid\equiv S \mid\equiv U \overset{SK}{\longleftrightarrow} S}{U \mid\equiv U \overset{SK}{\longleftrightarrow} S} \qquad (J1)$$

If *U* believes that *S* is an authority on the statement $U \overset{SK}{\longleftrightarrow} S$ and *S* believe in $U \overset{SK}{\longleftrightarrow} S$, then *U* ought to believe in $U \overset{SK}{\longleftrightarrow} S$ as well. So, *U* believes that *SK* is a suitable secret between *U* and *S*. (Goal 7)

(3) The third flow:

$$\frac{S < \{ID_i \| \{ID_i\}_s \| c\}_{+K}, S \ni -K}{S < (ID_i \| \{ID_i\}_s \| c), S < c} \qquad (T3, T4)$$

If S is told a formula $(ID_i \| \{ID_i\}_s \| c)$ encrypted with the public key $+K$ and it possesses the corresponding private key $-K$, then it is considered to have been told the decrypted contents of that encrypted formula. And it has also been told c as the formula's components.

$$\frac{S \lhd c, S \ni d, S \ni r}{S \ni c, S \ni (c \| d), S \ni h(c \| d), S \ni (r+1)} \qquad (P1, P2, P4)$$

If S is told c, it is capable of possessing c. And if S also possesses d, it is capable of possessing $(c \| d)$ and $h(c \| d)$. For the same reason, if S possesses r then it possesses $(r+1)$.

$$\frac{S \ni h(c \| d), S \ni (r+1)}{S \ni (h(c \| d) \| (r+1))} \qquad (P2)$$

If S possesses $h(c \| d)$ and $(r+1)$, then it possesses $(h(c \| d) \| (r+1))$ as well.

$$\frac{S \mid\equiv \phi(r)}{S \mid\equiv \phi(h(c \| d) \| (r+1))} \qquad (R1)$$

If S believes that r is recognizable, then S believes that $(r+1)$ is recognizable and $(h(c \oplus d) \| (r+1))$, of which $(r+1)$ is a component, is also recognizable.

$$\frac{S \mid\equiv \phi(h(c \| d) \| (r+1)), S \ni (h(c \| d) \| (r+1))}{S \mid\equiv \phi h(h(c \| d) \| (r+1))} \qquad (R5)$$

If S believes that $(h(c \| d) \| (r+1))$ is recognizable and it also possesses $(h(c \| d) \| (r+1))$, and then it is entitled to believe that $h(h(c \| d) \| (r+1))$ is recognizable. So, we can say that S believes that the message $h(h(c \| d) \| (r+1))$ in the third run is recognizable. (Goal 3)

$$\frac{S \mid\equiv \#(d), S \ni (c \| d)}{S \mid\equiv \#(c \| d), S \mid\equiv \#(h(c \| d))} \qquad (F1, F10)$$

If S believes d is fresh then it is entitled to believe that $h(c \| d)$ is fresh. And then if S also possesses $(c \| d)$, it is entitled to believe that $h(c \| d)$ is fresh.

$$S < *h((r+1), < SK >),$$

$$\frac{S \ni ((r+1), SK), S \equiv S \xleftrightarrow{SK} U, S \equiv \#(SK)}{S \equiv U \sim ((r+1), < SK >), S \equiv U \sim h((r+1), < SK >)} \quad (I3)$$

If all of the following conditions hold: 1) *S* receives a formula consisting of a one way function of (*r*+1) and *SK* marked with a not-originated-here mark; 2) *S* possesses (*r*+1) and *SK*; 3) *S* believes *SK* is a suitable secret for itself and *U*; 4) *S* believes that *SK* is fresh. Then *S* is entitled to believe that *U* once conveyed ((*r*+1), *SK*) and $h(h(c \| d) \| (r+1))$ .Therefore, we can say that *S* believes that the message $h(h(c \| d) \| (r+1))$ in the third run of the proposed protocol is conveyed from *U*. (Goal 5)

$$\frac{S \equiv U \sim ((r+1), SK), S \equiv \#(SK)}{S \equiv U \sim SK, S \equiv U \ni SK} \quad (I6, I7)$$

If *S* believes that *U* once conveyed the formula ((*r*+1), *SK*), then it is entitled to believe that *U* once conveyed *SK*. And if *S* also believes that *SK* is fresh, then it is entitled to believe that *U* possesses *SK*. Therefore, *S* believes that *SK* is possessed by *U*. (Goal 8)

According to the GNY logic, we assume that $U \equiv S \Rightarrow S \equiv *$, that is, *S* believes that *U* is honest and competent, and then we can deduce the following statement:

$$S \equiv U \Rightarrow U \equiv *, S \equiv U \sim (h(SK \| (r+1))$$

$$\frac{\sim > U \equiv U \xleftrightarrow{SK} S), S \equiv \#(SK \| (r+1))}{S \equiv U \equiv U \xleftrightarrow{SK} S} \quad (J2)$$

If *S* believes that *U* is honest and competent, and *S* receives a message $h(SK \| (r+1)) \sim > U \equiv U \xleftrightarrow{SK} S$ which it believes is conveyed by *U*, then *S* ought to believe that *U* really believes $U \xleftrightarrow{SK} S$. So, we can conclude that in the proposed protocol, *S* believes that *SK* is a suitable secret between *U* and *S*. (Goal 9)

Complexity Analysis

In this section, we first summarize the functionalities of the proposed protocol, and then evaluate the computational cost of the protocol.

As an attractive feature, our protocol provides identity protection including the identities of the smart appliance and the substation. In the proposed protocol, the adversary cannot obtain the real identities of the smart appliance and the substation since the identities are transmitted in ciphertext. So even if the adversary compromises the secret (C_1, C_2) stored in the tamper- resistant device and intercepts all the messages transmitted between the smart appliance and the substation, she/he cannot obtain the real identities of the smart appliance and the substation. In addition, the proposed protocol also provides mutual authentication and key agreement to protect the communications between the smart appliance and the substation. Next, we compare the computational cost of the proposed protocol with other related protocols. Some notations are defined as follows:

1. T_m: the time for executing a modular exponentiation operation.
2. T_e: the time for executing a scalar multiplication operation of elliptic curve.
3. T_h: the time for executing a one-way hash function.
4. T_{se}: the time for executing a symmetric key encryption operation.
5. T_{sd}: the time for executing a symmetric key decryption operation.
6. T_{ae}: the time for executing an asymmetric key encryption operation.
7. T_{ad}: the time for executing an asymmetric key decryption operation.
8. T_{hmac}: the time for executing a Hash-based Message Authentication Code

(HMAC) operation.

Table 2. Computational costs comparison between our protocol and others.

	Our protocol	Chim et al.'s protocol [4]	Mostafa et al.'s protocol [5]
Smart appliance	$T_e+T_{ae}+T_{sd}+T_h$	$2T_{ae}+T_{hmac}$	-----
Substation	$T_e+T_{ad}+2T_{se}+T_{sd}+T_h$	T_{hmac}	-----
Control center	-----	$2T_{ad}$	-----
HAN	-----	-----	$2T_m+T_{ae}+T_{ad}+T_h+T_{hmac}$
BAN	-----	-----	$2T_m+T_{ae}+T_{ad}+T_h$
Total	$T_{ae}+T_{ad}+2T_h+2T_e+2T_{se}+2T_{sd}$	$2T_{ae}+2T_{ad}+2T_{hmac}$	$2T_{ae}+2T_{ad}+2T_h+4T_m+T_{hmac}$

HAN: home area network; BAN: building area network

As shown in Table 2, in the proposed protocol, the computational cost at the substation S_j side is T_e+T_{se} during the initialization phase. One scalar multiplication operation T_e is used to compute the secret $C_2 = SID_jP$. And one symmetric key encryption operation T_{se} is used to generate another secret $C_1 = E_s(ID_i)$ through using the system key s. In the authentication phase, the computational cost at the substation S_j side is $T_{ad} + T_h + T_{sd} + T_{se}$, and the computational cost at the smart appliance U_i side is $T_{ae} + T_{sd} + T_e + T_h$. The smart appliance U_i takes one asymmetric key encryption operation via the substation S_j's public key pk to generate $C3 = e_{pk}(Id_i \| C_1 \| r_1)$; takes one symmetric key decryption operation to get SID_j and r_2; takes one scalar multiplication operation to compute SID_jP; and takes a one-way hash function operation to calculate $C_5 = h(SK' \| (r_3 + 1))$. The substation S_j takes one asymmetric key decryption operation

to get the smart appliance U_i's identity ID_i, the random integer r_1 and the authentication message C_1; takes a one-way hash function operation to obtain $h(SK \| (r_3 + 1))$; and takes one sym- metric key decryption operation and one symmetric key encryption operation. So, the total computational cost of the proposed protocol is $2T_e+T_{ae}+T_{ad} + 2T_{sd} + 2T_{se} + 2T_h$. The theoretical analysis and experimental results [25] show that the modular exponentiation operation T_m and the asymmetric key encryption/decryption operations T_{ae}/T_{ad} are much higher than that of the symmetric key encryption/decryption operations T_{se}/T_{sd} and the scalar multiplication operation of elliptic curve T_e. In addition, compared with the asymmetric key encryption/decryption operations T_{ae}/T_{ad} and the modular exponentiation operation T_m, the computational cost of hash function operation T_h could be ignored. Close analysis of the data in Table 2, shows that our proposed protocol is more efficient than and Mostafa et al.'s protocol [5], because it eliminates the expansive modular exponentiation operations and reduces the numbers of asymmetric key encryption/decryption operations. In addition, compared with Chim et al.'s protocol [4], our protocol reduces the computational cost at the smart appliance side. Although Chim et al.'s protocol possesses better performance at the substation side in comparison with the pro- posed protocol, their protocol cannot support mutual authentication and fails to provide a key agreement.

Then, we discuss the communication and storage overhead by comparing our proposed protocol with other protocols. Since Mostafa et al.'s protocol do not use tamper-resistant device, we only compared storage overhead with Chim et al.'s protocol at the smart appliance side. In our protocol, the smart appliance

needs to store a hash function and the secure information (C_1, C_2, pk, P), where C_1, C_2, and P are 1024 bits, and pk is 128 bits. The total storage overhead needed at the tamper-resistant devices in our protocol is 3200 bits. In Chim et al.'s protocol, the tamper-resistant needs to store the public key Pub_{CC}, the secret key S_r, a pair private and public key, the identity of smart appliance RID_i and HMAC function. Where Pub_{CC} is 1024 bits, S_r is 128 bits, RID_i is 32 bits and a pair key is 2048 bits. Therefore, the total overhead at the tamper-resistant devices side in Chim et al.'s protocol is larger than 3232 bits. As shown in Table 3, Compared with Chim et al.'s protocol, our proposed protocol reduced the storage overhead at the tamper-resistant side.

Table 3. Communication costs and storage overhead comparison between our protocol and others.

	Our protocol	Chim et al.'s protocol [4]	Mostafa et al.'s protocol [5]
Storage overhead (tamper-resistance devise side)	3200 bits	3232 bits	-----
Communication cost	608 bits	4448 bits	3744 bits

We hereby present the communication overhead of the proposed protocol. In our experiments, the user's *ID* was 32 bits, the timestamp was 32 bits, the random number was 64 bits, the signature was 160 bits, and a modular exponentiation was 512 bits. In addition, the output of a 256-bit AES was based on the input of the plaintext. We assume that RSA was adopted as public key encryption/decryption algorithm in protocols [4, 5]. The communication cost comparisons between our protocol and others are shown in Table 3. In our proposed protocol, the average

communication cost was 608 bits. Compared with the protocols in [4, 5], the proposed protocol scaled down the communication cost significantly.

Conclusion

An efficient authentication protocol with identity protection for smart grids has been proposed in this paper. In the proposed protocol, based on elliptic curve cryptography the substations and smart appliances realized mutual authentication and key agreement via a tamper-resistant device. In addition, the identities of the smart appliance and the substation are transmitted in ciphertext in the proposed protocol. So the adversary cannot obtain the real identities of the smart appliance and the substation. Furthermore, the completeness of the proposed protocol is demonstrated by Gong, Needham, and Yahalom (GNY) logic. And performance analysis shows that our proposed protocol increases efficiency in comparison with other related protocols. Therefore, the proposed protocol is more suitable for the smart grids.

Acknowledgments

The authors are indebted to the staff at the secure communication institute at China University of Geosciences.

Author Contributions

Conceived and designed the experiments: LZ ST. Performed the experiments: HL. Analyzed the data: LZ HL. Contributed reagents/materials/analysis tools: LZ HL. Wrote the paper: LZ.

References

1. Northcote-Green J, Wilson R. Control and Automation of Electrical Power Distribution Systems. Boca Raton, Florida: CRC press, 2006.
2. ARC Advisory Group, SCADA Systems for Smart Grid, Available: http://www.arcweb.com/Research/ Studies/Pages/SCADA-Power.aspx.
3. Salem AA. Electricity agents in smart grid markets. Computers in Industry. 2013; 64(3):235–241. doi: 10.1016/j.compind.2012.10.009
4. Chim TW, Yiu SM, Hui LCK, Li VOK. PASS: Privacy-preserving Authentication Scheme for Smart Grid Network. Proceedings of Cyber and Physical Security and Privacy. 2011; 196–201. doi: 10.1109/ SmartGridComm.2011.6102316
5. Mostafa M, Fadlullah ZM, Kato N, Lu R, Shen X. A Light-weight Message Authentication Scheme for Smart Grid Communications. IEEE Transaction on Smart Grid. 2011; 2(4): 675–685. doi: 10.1109/ TSG.2011.2160661
6. Li QH, Cao GH. Multicast Authentication in the Smart Grid with One-Time Signature. IEEE Transaction on Smart Grid. 2012; 2(4) 686–696. doi: 10.1109/TSG.2011.2138172
7. Oh S, Kwak J. Mutual Authentication and Key establishment mechanism using DCU certificate in Smart Grid. Applied Mathematics & Information Sciences. 2012; 6(1S): 257S–264S.

8. Nam J, Choo KKR, Han S, Kim M, Paik J, Won D. Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation. Plos one, 2015; 10(4): 1–21. doi: 10.1371/journal.pone.0116709

9. He D, Kumar N, Chilamkurti N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Information Sciences. 2015; 321: 263–277. doi: 10.1016/j.ins.2015.02.010

10. Gao QH. Biometric Authentication in Smart Grid. Proceedings of Energy and Sustainability Conference. 2012; pp.1–5. doi: 10.1109/IESC.2012.6217197

11. He D, Zeadally S. Authentication protocol forambient assisted living system. IEEE Communications Magazine, 2015; 53(1):71–77. doi: 10.1109/MCOM.2015.7010518

12. Wang CQ, Zhang X, Zheng ZM. Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme. Plos one, 2016; 11(12):1–25. doi: 10.1371/journal.pone.0149173

13. Vaidya B, Makrakis D, Mouftah HT. Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Networks. IEEE Network. 2013; 5–11. doi: 10.1109/MNET.2013.6423185

14. Liu H, Ning HS, Zhang Y, Guizani M. Battery Status-aware Authentication Scheme for V2G Networks in Smart Grid. IEEE Transactions on Smart Grid. 2013; (4)(1):99–110. doi: 10.1109/TSG.2012.2224387

15. Nicanfar H, Leung VCM. Password-authenticated cluster-based group key agreement for smart grid communication. Security and Communication Networks. 2014; 7(1): 221–233. doi: 10.1002/sec.726

16. Zhang L, Tang S, Jiang Y, Ma Z. Robust and Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Smart Grids. 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 201; 2089– 2093. doi: 10.1109/GreenCom-iThings-CPSCom.2013.392

17. Nicanfar H, Leung VCM. Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System. IEEE Transaction on Smart Grid. 2013; 4(1): 253–264. doi: 10.1109/TSG.2012.2226252

18. He D, Kumar N, Lee JH. An efficient and privacy-preserving data aggregation scheme for the smart grid against internal attackers. Wireless Networks. 2016; 22(2): 491–502. doi: 10.1007/s11276-015-0983-3

19. Li D, Aung Z, Williams JR, Sanchez A. Efficient and fault-diagnosable authentication architecture for AMI in smart grid. Security and Communication Networks. 2015; 8(4):598–616, doi: 10.1002/sec.1006

20. Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transaction on Computer Systems. 1990; (8): 18–36.

21. Nessett DM. A critique of the Burrows, Abadi, and Needham logic. ACM SIGOPS Operating Systems Review. 1990; 24(2):35–38. doi: 10.1145/382258.382789

22. Li G, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. Proceedings of IEEE Computer Society Symp. Research in Security and Privacy. 1990; 234–248. doi: 10.1109/RISP.1990.

23. Fan CI, Lin YH. Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics. IEEE Transactions on Information Forensics and Security. 2009; 4(4):933–945. doi: 10.1109/TIFS.2009.2031942

24. Darrel H, Alfred M, Scott Vanstone. Guide to elliptic curve cryptography. 2004; Springer-Verlag, Berlin.

25. Kilinc HH, Yanik T. A Survey of SIP Authentication and Key Agreement Schemes. IEEE Communications Surveys& Tutorials. 2013; 1–19. doi: 10.1109/SURV.2013.091513.00050