




RESEARCH ARTICLE

An efficient heterogeneous signcryption for smart grid

Chunhua Jin ^{*}, Guanhua Chen ^{*}, Changhui Yu ^{*}, Jinsong Shan ^{*}, Jianyang Zhao ^{*}, Ying Jin ^{*}

Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, China

 These authors contributed equally to this work.

* xajch0206@163.com



Abstract

A smart grid, considered the next-generation type of power grid, combines a traditional power grid with information and communication technologies to effectively facilitate power generation and ensure transmission security and reliability in real-time. Only authorized consumers should be able to access the smart grid because the information gathered by smart meters includes users' private information. However, smart grid security is still a challenge. Motivated by this challenge, in this paper, we propose a heterogeneous signcryption (HSC) scheme for secure communication between smart meters and the utility. We demonstrate that this scheme is indistinguishable against adaptive chosen-ciphertext attacks (IND-CCA2), existentially unforgeable against adaptive chosen-message attacks (EUF-CMA) and ciphertext-anonymous against adaptive chosen ciphertext attacks (ANON-CCA2) under the computational Diffie-Hellman (CDH) problem in the random oracle model. Our scheme simultaneously achieves confidentiality, integrity, authentication, non-repudiation and ciphertext anonymity in a single logical step. It supports heterogeneous systems, allowing a meter in an identity-based cryptography (IBC) environment to transmit electrical usage data to a utility in a public key infrastructure (PKI) environment. Compared with other existing related schemes, our scheme has the lowest communication overhead and energy consumption for the smart grid. Based on these features, our scheme is highly suitable for secure power transmissions in a smart grid.

OPEN ACCESS

Citation: Jin C, Chen G, Yu C, Shan J, Zhao J, Jin Y (2018) An efficient heterogeneous signcryption for smart grid. PLoS ONE 13(12): e0208311. <https://doi.org/10.1371/journal.pone.0208311>

Editor: Mauro Villarini, Universita degli Studi della Tuscia, ITALY

Received: December 26, 2017

Accepted: November 8, 2018

Published: December 18, 2018

Copyright: © 2018 Jin et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: This work is supported by the Natural Science Foundation of Jiangsu Province (Grant No. BK20161302 to JZ), Electric Power Company Technology Project of Jiangsu Province (Grant No. J2017123 to JZ). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing interests: The authors have declared that no competing interests exist.

Introduction

Smart grid is envisioned as a next-generation power grid that aims to provide users with electricity in a more reliable and efficient manner [1–5]. The main feature of a traditional power grid is one-way electricity distribution from power plants to consumers. In contrast, a smart grid integrates advanced communication technologies into the traditional grid, allowing two-way energy and information flow. In addition, a smart grid provides consumers with tools to optimize their energy consumption.

Smart meters, which include processors and storage, are key components of a smart grid. Smart meters can communicate with household appliances as well as with facilities at the

utility. A smart grid equipped with smart meters can monitor electricity distribution and consumption information in real-time, provide subscribed users with power and fulfill advanced demands as well as manage power usage and outages [6] through a reliable communication network. A smart meter at each home collects electrical usage data from all the electric appliances at the home and transmits these data to the utility company. Thus, a smart grid can provide specific real-time power usage details through the communications between the smart meters and the utility. Then, the utility can change the price of power accordingly. Moreover, it also can adjust users' power usage using preset load controls to flatten peak demands and avoid potential blackouts. Customers can obtain information about their electricity usage from the smart meters, and thus reschedule their current electric power usage, transferring power usage from peak times to non-peak times to control their costs.

A smart grid provides large benefits for both consumers and the utility. However, its success heavily relies upon communications systems, and the vulnerabilities inherent to communications systems can clearly affect the smart grid, cause severe harm to the entire infrastructure, and damage the economy, the society and affect people's lives. Thus, communications security is a primary concern in smart grids [7–15]. In this paper, we concentrate primarily on sending power consumption information from smart meters to a utility in a secure manner. The basic considerations are as follows. 1) The power consumption data should be obtainable only by the smart meters and the utility. No other entities should be able to obtain the power consumption data because these data are sensitive. 2) The power consumption data must be authenticated. Without authentication, power consumption data are potentially fake. 3) The power consumption data must not have been altered during transmission. If the power consumption data have been modified, malicious operations have been detected. 4) After a smart meter has sent a consumer's data to the utility, it cannot retroactively deny its action. 5) The power usage data include no extractable information that can help a third party to identify either the meter or the utility.

It is difficult to propose a scheme that simultaneously meets all the abovementioned properties. Additionally, we must consider that the computational and communication resources of a smart meter are limited. However, the utility has strong computational and communication resources. Thus, the resources available to smart meters and to the utility are not equivalent. Thus, we propose a heterogeneous secure signcryption scheme that accords with such characteristics. The advantage of this heterogeneous scheme is that smart meters have no certificate management problem, but the utility can afford the overhead involved in certificate management.

To ensure secure communications from smart meters to the utility, in this paper, we design a secure HSC scheme. This scheme supports heterogeneous operations on the communication entities. There are three primary innovative points made in this paper.

- First, based on the fact that energy usage data must be well protected, we propose a secure HSC scheme to simultaneously achieve confidentiality, authentication, integrity, non-repudiation and ciphertext anonymity in a logical single step.
- Second, to analyze the security strength of our scheme, a provable security technique is employed to formally prove the proposed scheme's security. This scheme has the properties of IND-CCA2 [16] and EUF-CMA [16] under the CDH problem in the random oracle model. According to this performance analysis, we conclude that the proposed scheme is more efficient than any other existing HSC schemes [17–19].
- Third, we adopt the heterogeneous communication system. Specifically, we require that a smart meter working in an IBC system be able to send a message to a utility belonging to a

PKI system. This heterogeneous characteristic allows our scheme to be used for power information transmission in a smart grid because smart meters have no certificate management ability.

The remainder of the paper is arranged as follows. Related works are reviewed in Section 2. The system model, security requirements, design goal and bilinear pairings are introduced in Section 3. Then, the HSC scheme is designed in Section 4. We discuss its security and performance in Sections 5 and 6, respectively. Finally, Section 7 provides conclusions.

Related work

Signcryption [20] is a cryptographic primitive that can simultaneously fulfill the functions of a digital signature and public key encryption in a logical single step. Meanwhile, its cost is significantly lower, and its performance exceeds those of the traditional sign-then-encrypt approach. These advantages make signcryption particularly beneficial in environments with limited resources because the properties of confidentiality, authentication, integrity and non-repudiation can be achieved simultaneously at a lower cost. Some PKI-based signcryption schemes [16, 21–23] and some IBC-based signcryption [24–28] schemes have been proposed. But these signcryption schemes are homogeneous; in other words, both the sender and the receiver must be working in the same environment. This requirement of homogeneity is unsuitable for heterogeneous communications.

To employ signcryption in heterogeneous systems, efficient and secure signcryption schemes must be constructed that support heterogeneous communications. Sun and Li [17] presented two HSC schemes. The first HSC scheme permits a sender that belongs to a PKI to transmit a message to a receiver that belongs to an IBC, while the second HSC scheme permits a sender that belongs to an IBC to transmit a message to a receiver that belongs to a PKI. However, these two schemes are not secure from insider attacks because such signcryption schemes have no non-repudiation guarantees. The notion of insider security is stronger than that of outsider security [29], and has two requirements: (1) if the private key of a sender is revealed, an attacker cannot obtain the original message; and (2) if the private key of a receiver is revealed, an attacker cannot counterfeit a ciphertext.

Regarding insider security, Huang et al. [18] presented an HSC scheme that permits a sender who belongs to an IBC to transmit a message to a receiver that belongs to a PKI. This approach is very promising and has triggered considerable followup research [19, 30–32]. For example, Li and Xiong (hereafter called LX) [19] presented a heterogeneous online/off-line signcryption (HOOSC) scheme that splits the SC into two phases: an offline phase and an online phase. The offline phase has no knowledge of messages, and most of the complex computations are implemented in this phase. In contrast, the online phase has knowledge of messages and performs only simpler calculations. In 2013, Li et al. [30] presented two SC schemes that support heterogeneous communication. The first HSC permits a sender belonging to a PKI environment to send a message to a receiver belonging to an IBC environment, while the second HSC permits a sender belonging to an IBC environment to send a message to a receiver belonging to the PKI environment. Recently, Li et al. (hereafter termed LZJ) [31] constructed a heterogeneous ring signcryption (HRSC) scheme that works from sensors to servers. The proposed scheme can protect the privacy of the sensor nodes. It permits a sensor node belonging to an IBC environment to send a message to a server belonging to a PKI environment. In 2016, Li et al. (hereafter called LHJ) [32] constructed an HSC scheme intended for communications from wireless sensor networks (WSNs) to an Internet server. In [32], the WSNs belong to a certificateless cryptography environment while the server works in a PKI environment.

Motivation and contribution

The motivation of this paper is to design a secure heterogeneous signcryption for smart grid. In our scheme, we adopt heterogeneous system which allows smart meters belonging to an IBC environment to transmit electrical usage data to a utility belonging to a PKI environment. The heterogeneity makes our scheme be suited to smart grid. We show that the proposed heterogeneous signcryption is indistinguishable against adaptive chosen-ciphertext attacks (IND-CCA2), existentially unforgeable against adaptive chosen-message attacks (EUF-CMA) and ciphertext-anonymous against adaptive chosen ciphertext attacks (ANON-CCA2) under the computational Diffie-Hellman (CDH) problem in the random oracle model. Our scheme can attain the insider security for confidentiality, integrity, authentication, non-repudiation and ciphertext anonymity in a single logical step. For performance analysis, our scheme has the lowest communication overhead and energy consumption for the smart grid.

System model, security requirements and design goals

In this section, we describe the system model, security requirements and design goals.

System model

Our heterogeneous system model, which includes three entity types: a PKG (Private Key Generator), a smart meter and a utility. The PKG is responsible for smart meter registration; it allocates an identity and a corresponding private key to every smart meter. It is always assumed to be trustworthy and never compromised. The smart meter is responsible for collecting electrical usage data and sending the collected data to the utility. The utility is responsible for detecting, responding, adjusting, and storing the power data.

Security requirements

Security is important for smart grid communications. In our system model, we assume that both the PKG and the certificate authority (CA) are trustable. However, an adversary exists who may eavesdrop or intercept users' power data and the utility's management control messages. The adversary may also perform attacks that affect data integrity. Moreover, the smart meters cannot deny any data they have previously transmitted. Therefore, to protect the electrical usage data, a smart grid must satisfy the following security requirements.

- Confidentiality: Power usage information and management control messages should be kept secret to protect consumers' privacy and the utility's business information from anyone except the smart meters and the utility.
- Authentication: Only a valid smart meter should be able to send electrical usage data to the utility and receive the corresponding utility services.
- Integrity: The smart grid should be able to ensure that electrical usage data from smart meters and management messages from the utility have not been modified by unauthorized entities.
- Non-repudiation: Once a smart meter has sent electrical usage data to the utility, that action cannot be retroactively denied (i.e., the smart meter cannot deny having transmitted the previous electrical usage data).
- Scalability: Every smart meter sends its electronic data to the utility which realize one to one communication. We add a data collector in the sender to achieve multiple to one communication.

Design goals

Based on the system model described above and the security requirements, our design goal is to construct an efficient HSC scheme to ensure smart grid security. Specifically, we must achieve the following three objectives.

- Heterogeneous systems could participate in the constructed scheme. As noted above, smart meters have limited computing capacity and storage resources, while the utility has strong computing, energy, bandwidth and storage capacities. Therefore, the proposed scheme should match these characteristics.
- Our proposed scheme should achieve all the security requirements. We know that security is important for smart grids. If security is not ensured, the electricity usage data from the smart meters and the management messages from the utility could conceivably be forged and/or modified by an adversary. Therefore, our constructed scheme should achieve confidentiality, authentication, integrity and non-repudiation simultaneously.
- The proposed scheme should achieve effective communications. Because the power transmission between the smart meter and the utility must meet real-time requirements, our constructed scheme must satisfy the requirements for effective communication.

Preliminaries

In this section, the bilinear pairings and the CDH problem are outlined.

Let G_1 and G_T be a cyclic additive group and a cyclic multiplicative group. The generator of G_1 is P . G_1 and G_T have the same order q . A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_T$ with the following three properties:

1. Bilinear: On inputting $P, Q \in G_1, a, b \in \mathbb{Z}_q^*$, we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degeneracy: There exists a $P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.
3. Computability: On inputting $P, Q \in G_1$, an efficient algorithm exists to compute $\hat{e}(P, Q)$.

A bilinear pairing that satisfies the abovementioned properties is called an admissible bilinear pairing. The modified Weil pairing or Tate pairing are admissible maps of this type. For more details, readers can refer to [33].

On inputting a cyclic addition group G_1 , its prime order q and generator P , the CDH problem in G_1 involves computing abP given $(P, aP, bP) \in G_1$.

Definition 1. The (ϵ, t) -CDH assumption holds when no t -polynomial time adversary \mathcal{A} exists who has advantage of at least ϵ in solving the CDH problem.

An HSC scheme

In this section, we first provide the syntax and security notions for an HSC scheme that permits only a sender belonging to an IBC system to transmit a message to a receiver belonging to a PKI system. Here, we employ IP-HSC to denote the following SC, in which “I” denotes IBC and “P” denotes PKI. Then, we describe our proposed HSC scheme.

Syntax

A generic IP-HSC scheme comprises the following five algorithms.

Setup: On inputting a security parameter k , this algorithm, which executes on a PKG, outputs a master private key s as well as the system parameters $params$.

IBC-KE: On inputting the master key s and an identity ID of a user, this algorithm, which executes on a PKG, outputs a secret key S_{ID} . The PKG securely transmits the secret key to the corresponding user.

PKI-KG: This algorithm is executed by PKI users. The user selects a secret key x and calculates a corresponding public key y which is signed by its CA.

SC: On inputting a message m , a sender's secret key S_{ID_s} and a receiver's public key y_r , this algorithm (executed by the sender) returns a ciphertext σ .

USC: On inputting a ciphertext σ , the identity ID_s of a sender as well as the receiver's private key x_r , this algorithm (executed by the receiver) returns a message m when σ is valid or a symbol \perp when σ is not valid.

For consistency, the algorithm should satisfy the following requirement: if

$$\sigma = \text{Signcrypt}(m, S_{ID_s}, y_r)$$

then we have

$$m = \text{Usigncrypt}(\sigma, ID_s, x_r)$$

Security notions

Both confidentiality and unforgeability should be satisfied in a signcryption scheme. Here, we slightly amend the notions in [24–26, 34, 35] to adjust IP-HSC.

For confidentiality, the following game is enacted between a challenger \mathcal{C} and an adversary \mathcal{F} .

Initial: On inputting a security parameter k , \mathcal{C} executes the *Setup* algorithm and sends a master private key s as well as the system parameters $params$ to the adversary \mathcal{F} . Additionally, \mathcal{C} also runs the *PKI-KG* algorithm to generate the receiver's private key x_r and public key y_r . It transmits y_r to \mathcal{F} .

Phase 1: \mathcal{F} requests USC queries adaptively. For a USC query, \mathcal{F} chooses a ciphertext σ as well as the identity ID_s of a sender. \mathcal{C} runs $USC(\sigma, ID_s, x_r)$ and transmits the result to \mathcal{F} .

Challenge: \mathcal{F} determines when Phase 1 ends. \mathcal{F} produces two equal-length messages, m_0 and m_1 , as well as the challenge identity ID_s^* of a sender. \mathcal{C} first runs the *IBC-KE* algorithm to obtain the secret key $S_{ID_s^*}$. Then, \mathcal{C} picks a random bit $\beta \in \{0, 1\}$ and transmits $\sigma^* = SC(m_\beta, S_{ID_s^*}, y_r)$ to \mathcal{F} .

Phase 2: As in phase 1, \mathcal{F} again performs USC queries in an adaptive manner. Nevertheless, it cannot perform a USC query on (σ^*, ID_s^*, x_r) to obtain the corresponding message this time.

Guess: Therefore, \mathcal{F} generates a bit β' and wins the game if $\beta = \beta'$.

\mathcal{F} 's advantage is defined as $\text{Adv}(\mathcal{F}) = |2\text{Pr}[\beta' = \beta] - 1|$, where $\text{Pr}[\beta' = \beta]$ denotes the probability that $\beta' = \beta$.

Definition 2(Confidentiality). An IP-HSC scheme is (ϵ, t, q_u) -IND-CCA2 secure when no PPT (probabilistic polynomial time) adversary \mathcal{F} succeeds with an advantage of at least ϵ after at most q_u USC queries.

Notice that the aforementioned definition obtains the confidentiality's insider security because \mathcal{F} is aware of the master private key and all senders' private keys [29]. This corresponds to the insider security requirements that the signcryption scheme's forward security

must be ensured, and means that confidentiality is maintained even if the sender’s secret key is compromised.

For unforgeability, we consider the following game interacted between a challenger and an adversary \mathcal{F} .

Initial: On inputting a security parameter k , \mathcal{C} executes the *Setup* algorithm and transmits the system parameters to \mathcal{F} . Additionally, \mathcal{C} executes the *PKI-KG* algorithm to obtain the receiver’s private key x_r and public key y_r and transmits them to \mathcal{F} .

Attack: \mathcal{F} requests key extraction queries and signcryption queries adaptively. In a key extraction query, \mathcal{F} first chooses an identity ID and transmits it to \mathcal{C} . Then, \mathcal{C} executes the *IBC-KE* algorithm and transmits the corresponding secret key S_{ID_s} to \mathcal{F} . In a signcryption query, \mathcal{F} generates an identity ID_s of a sender as well as a message m . \mathcal{C} first runs *IBC-KE* algorithm to obtain the private key S_{ID_s} of the sender. Then, \mathcal{C} sends $\sigma = SC(m, S_{ID_s}, y_r)$ to \mathcal{F} .

Forgery: \mathcal{F} generates a challenge identity ID_s^* of a sender as well as a challenge ciphertext σ^* . It succeeds if the following conditions hold:

1. $USC(\sigma^*, ID_s^*, x_r) = m^*$.
2. \mathcal{F} has not requested a key extraction query on identity ID_s^* .
3. \mathcal{F} has not requested a signcryption query on (m^*, ID_s^*) .

The advantage of \mathcal{F} is defined as the probability that it wins.

Definition 3(Unforgeability) An IP-HSC scheme is (ϵ, t, q_k, q_s) -EUF-CMA secure, if no PPT (probabilistic polynomial time) adversary \mathcal{F} succeeds with an advantage of at least ϵ after at most q_k key extraction queries and q_s signcryption queries.

In the above definition, note that the adversary is aware of the receiver’s private key x_r . This corresponds to the insider security requirement for the unforgeability of a signcryption scheme [29].

Proposed IP-HSC scheme

In this section, we present an efficient IP-HSC scheme for secure smart grid communications that mainly comprises five algorithms: *Setup*, *IBC-KE*, *PKI-KG*, *SC* and *USC*. Then, we present the design of IP-HSC. We list the main notations of our scheme in Table 1.

Setup: On inputting a security parameter k , the PKG selects the bilinear map groups (G_1, G_2) of prime order q , a generator P for G_1 and a bilinear map $G_1 \times G_1 \rightarrow G_2$. It then chooses a master private key $s \in Z_q^*$, a master public key $P_{pub} = sP$, and the hash functions $H_1: \{0, 1\}^* \rightarrow G_1$, $H_2: \{0, 1\}^n \times G_1^3 \rightarrow G_1$, $H_3: G_1^3 \rightarrow \{0, 1\}^n$. Here, n denotes the size of a message to be signcrypted. The public parameters are $\{G_1, G_2, e, q, P, P_{pub}, n, H_1, H_2, H_3\}$.

IBC-KE: A sender belonging to an IBC transmits its identity ID_s to PKG. The PKG calculates $Q_{ID_s} = H_1(ID_s)$ and sends the private key $S_{ID_s} = sQ_{ID_s}$ to the sender.

PKI-KG: A receiver in a PKI selects a random value $x_r \in Z_q^*$ as its private key and computes $y_r = x_r P$ as the corresponding public key.

SC: On inputting a message m , the sender’s private key S_{ID_s} , and the receiver’s public key y_r , the sender executes the following procedures.

1. Choose $r \in Z_q^*$ randomly and compute $U = rP$.

Table 1. Notations.

Notations	Descriptions
k	A security parameter
G_1	A cyclic addition group
G_2	A cyclic multiplicative group
e	A bilinear map $e: G_1 \times G_1 \rightarrow G_2$
P	A generator of group G_1
q	The order of group G_1 and G_2
n	The size of a message to be signcrypted
s	A master private key of PKG
P_{pub}	A master public key of PKG
$H_i()$	A collision-resistant hash function ($i = 1, 2, 3$)
ID_s	An identity of a sender
Q_{ID_s}	A public key of a sender
S_{ID_s}	A private key of a sender with identity ID_s
x_r	A private key of a receiver
y_r	A public key of a receiver

<https://doi.org/10.1371/journal.pone.0208311.t001>

2. Compute $h_2 = H_2(m, U, ID_s, y_r)$.
3. Compute $V = S_{ID_s} + rh_2$.
4. Compute $W = m \parallel ID_s \oplus H_3(U, y_r, ry_r)$.
5. Output the ciphertext $\sigma = (U, V, W)$.

USC: On inputting a ciphertext σ , a sender’s public key Q_{ID_s} , and a receiver’s private key x_r , the receiver executes the following procedures.

1. Compute $T = x_r U$.
2. Compute $m \parallel ID_s = W \oplus H_3(U, y_r, T)$.
3. Compute $h_2 = H_2(m, U, ID_s, y_r)$.
4. Check whether $e(P, V) = e(P_{pub}, Q_{ID_s})e(U, h_2)$. If so, output the message m . Otherwise, reject and output a failure symbol \perp .

Our IP-HSC scheme is heterogeneous, which is different from HSC [24–26, 34, 35]. In our proposed scheme, the sender is in an IBC system while the receiver is in a PKI system. Therefore, the characteristics of heterogeneous systems are highly suitable for power usage data transmission in a smart grid. A smart meter belonging to the IBC system employs the SC algorithm to obtain a ciphertext and transmits it to a utility belonging to the PKI system. Notice that we use the IBC technique in smart meters, which have no certificate management problem; thus, the computational burden of the smart meters is decreased. We employ the PKI technique at the utility, which has no key escrow problem.

In our scheme, every smart meter sends its electronic data to the utility which realize one to one communication. In smart grid, there will be many smart meters to communicate with the utility. Therefore, in order to achieve scalability, we add a data collector in the sender, which collect data from lots of smart meters. The utility does not need to establish a single communication channel to each smart meter. Thus, we can achieve multiple to one communication. To

realize efficiency, the limited computation ability of smart meter does not perform many expensive calculation.

Security analysis

In this section, we analyze the confidentiality and unforgeability of our proposed IP-HSC scheme by following Theorem 1 and 2, respectively.

Theorem 1 (Confidentiality) In the random oracle model, if an adversary \mathcal{F} exists that can break the IND-CCA2 security of our proposed IP-HSC scheme with a nonnegligible advantage ϵ , running in a given time t and making at most q_u unsigncryption queries and q_{H_i} oracle H_i ($i = 1, 2, 3$) queries, then there exists a PPT algorithm \mathcal{C} that settles the CDH problem with an advantage

$$\epsilon' > \epsilon(1 - \frac{q_u}{2^k})$$

in a given time $t' < t + O(q_{H_3} + q_u)t_e$, where t_e is the time of a pairing operation.

Proof: It is assumed that we construct an algorithm \mathcal{C} that employs \mathcal{F} as a subroutine to settle the random instance (P, aP, bP) of the CDH problem.

Initial: \mathcal{C} randomly selects a master private key s and calculates a master public key $P_{pub} = sP$. \mathcal{C} also calculates a receiver's public key $y_r = aP$. Here a simulates the receiver's private key, and \mathcal{C} is not aware of the value of a .

Phase 1: \mathcal{C} acts as the challenger to \mathcal{F} in the confidentiality game defined in Section 4. Three lists are kept to simulate the hash oracles H_1, H_2, H_3 , respectively. Assume that H_1 queries are distinct. We also assume that \mathcal{F} will issue an $H_1(ID)$ query before employing ID in any other queries.

- H_1 queries: For an H_1 query on the identity ID_i , \mathcal{C} first examines whether H_1 's value is already in the list L_1 . If yes, the existing value is returned; otherwise, \mathcal{C} selects $t_i \in Z_p^*$ randomly, set t_iP as the value and inserts the tuple (ID_i, t_i) into the list L_1 .
- H_2 queries: For an H_2 query on (m, U, ID_s, y_r) , \mathcal{C} first determines whether H_2 's value is already in the list L_2 . If so, the existing value is returned; otherwise, \mathcal{C} picks a random value $e_i \in Z_p^*$, sets e_iP as the answer and inserts the tuple (m, U, ID_s, y_r, e_iP) into the list L_2 .
- H_3 queries: For an H_3 query on (U, y_r, T) , \mathcal{C} performs the following steps.
 1. If $e(aP, bP) = e(T, P)$, \mathcal{C} outputs T and stops. On this occasion, \mathcal{C} has settled the given CDH problem.
 2. If a tuple of the form $(U, y_r, *, h_{3,i})$ exists in list L_3 such that $e(U, y_r) = e(T, P)$, \mathcal{C} outputs $h_{3,i}$ and regenerates the symbol $*$ with T .
 3. If \mathcal{C} reaches the execution point, it selects $h_{3,i} \in \{0, 1\}^n$ randomly and gives it to \mathcal{F} . Then, \mathcal{C} saves the query and inserts the response into the list L_3 .

Unsigncryption queries: \mathcal{F} selects a sender's identity ID_s and a ciphertext $\sigma = (U, W)$. \mathcal{C} performs the following steps.

1. \mathcal{C} searches for a tuple of the form (U, y_r, T) for different T values, such that $e(U, y_r) = e(T, P)$. If such an entry exists, $h_{3,i}$'s correct value can be obtained, and \mathcal{C} employs this value $h_{3,i}$ to decrypt the ciphertext (i.e., $m = W \oplus h_3$). If no such entry exists in L_3 , \mathcal{C} randomly selects

$h_{3,i} \in \{0, 1\}^n$ and adds the tuple $(U, y_r, *, h_{3,i})$ to the list L_3 . Then, \mathcal{C} decrypts the ciphertext using the random value $h_{3,i}$.

- \mathcal{C} asks an H_2 query and obtains $h_{2,i} = H_2(m, U, ID_s, y_r)$. Then, it checks whether $e(P, V) = e(P_{pub}, Q_{ID_s})e(U, h_2)$. When the conditions hold, message m is returned to \mathcal{F} . Otherwise, \mathcal{C} rejects the ciphertext.

Challenge: \mathcal{F} produces two equal length plaintexts $(m_0 \text{ and } m_1)$ and a challenge identity ID_s^* of a sender. In response, \mathcal{C} first sets $U^* = bP$ and selects W^* from $\{0, 1\}^n$. Then, \mathcal{C} transfers the ciphertext $\sigma^* = (U^*, W^*)$ to \mathcal{F} .

Phase 2: \mathcal{F} adaptively performs an unsigncryption query again as in Phase 1. There is a restriction that \mathcal{F} cannot issue an unsigncryption query on (σ^*, ID_s^*, x_r) to obtain the corresponding plaintext. \mathcal{C} replies to \mathcal{F} 's queries following the same approach as in Phase 1.

Guess: \mathcal{F} generates a bit β' that is neglected by \mathcal{C} .

The simulation is perfect except that \mathcal{F} requests an H_3 query on the entry (u^*, y_r, aT^*) . If no such entry exists in the list L_3 , \mathcal{F} has no advantage. Nevertheless, if that happens, because of the first step in H_3 's simulation, \mathcal{C} will solve the CDH problem. Throughout this entire simulation, the failure probability for unsigncryption queries is at most $q_u/2^k$.

Theorem 2 (Unforgeability) Under the random oracle model, if an adversary \mathcal{F} exists that can break the EUF-CMA security of our proposed IP-HSC scheme, running in a given time t and making at most q_k key extraction queries, q_s signcryption queries, and q_{H_i} oracle H_i ($i = 1, 2, 3$) queries with a nonnegligible advantage ϵ , then there exists an algorithm \mathcal{C} that settles the CDH problem with an advantage

$$\epsilon' \geq \epsilon \frac{1}{e(q_k + 1)} \left(1 - \frac{q_s(q_s + q_{H_2})}{2^k}\right)$$

in a time of $O(t)$.

Proof: Assume that we construct an algorithm \mathcal{C} that employs \mathcal{F} as a subroutine to solve the random instance (P, aP, bP) of the CDH problem.

Initial: \mathcal{C} randomly selects a receiver's secret key x_r from Z_p^* and calculates the corresponding public key $y_r = x_r P$. Then, \mathcal{C} sends the receiver's key pair (x_r, y_r) and the system parameters $params$ with $P_{pub} = aP$ to \mathcal{F} . Notice that \mathcal{C} is not aware of the a value that simulates the PKG's master private key.

Attack: \mathcal{C} acts as the challenger to \mathcal{F} in the unforgeability game defined in Section 4. Three lists are kept to simulate the hash oracles $H_1, H_2,$ and H_3 . It is assumed that H_1 queries are distinct. We also assume that \mathcal{F} will re-query $H_1(ID)$ before utilizing ID in any other queries.

- H_1 queries: \mathcal{F} performs H_1 queries on identity ID_i , as in the proof technique by Coron [36]. \mathcal{C} spins a coin $T \in \{0, 1\}$ that takes a value of 0 with the probability of ξ and a value of 1 with the probability $1 - \xi$. If $T = 0$, then \mathcal{C} picks n_i from Z_q^* and defines $H_1(ID_i) = n_i P$. If $T = 1$, then \mathcal{C} outputs $H_1(ID_i) = n_i bP$. In these two cases, \mathcal{C} adds a triple (ID_i, n_i, T) to the list L_1 .
- H_2 queries: For an $H_2(m, U, ID_s, y_r)$ query, \mathcal{C} first examines whether the H_2 value is already in list L_2 for the entry (m, U, ID_s, y_r) . If so, it outputs the existing value; otherwise, \mathcal{C} outputs $h_{2,i}$ from G_1 as the answer. Then, \mathcal{C} inserts the tuple $(m, U, ID_s, y_r, h_{2,i})$ into list L_2 .
- H_3 queries: For an $H_3(U, y_r, T)$ query, \mathcal{C} first determines whether the H_3 value is already in list L_3 for the entry (U, y_r, T) . If so, it returns the existing value; otherwise, \mathcal{C} outputs a

random value $h_{3,i}$ from $\{0, 1\}^n$ as the answer. Then, \mathcal{C} inserts the tuple $(U, y_r, T, h_{3,i})$ into the list L_3 .

- *Key extraction queries:* When \mathcal{F} performs a key extraction query on an identity ID_i , \mathcal{C} obtains the corresponding triple (ID_i, n_i, T) from list L_1 . When $T = 1$, \mathcal{C} fails and stops because it cannot compute the private key. Otherwise, \mathcal{C} outputs the private key $n_i aP$.
- *Signcryption queries:* \mathcal{F} selects a message m and a sender's identity ID_s . In response, \mathcal{C} performs the following steps.
 1. Select $r, t \in Z_q^*$ randomly and compute $U = tP_{pub}, V = rP_{pub}$.
 2. Set $t^{-1}(rP - Q_{ID_s}) = H_2(m, U, ID_s, y_r)$ and add the tuple (m, U, ID_s, y_r) to the list L_2 .
 3. Define $h_3 = H_3(U, y_r, T)$ and insert the tuple (U, y_r, T) into the list L_3 .
 4. Compute $W = m \oplus h_3$.
 5. Return the ciphertext $\sigma = (U, W)$.

Eventually, \mathcal{F} outputs a challenge ciphertext $\sigma^* = (U^*, W^*)$ and a challenge identity ID_s^* of a sender. Then, \mathcal{C} retrieves the tuple (ID_s^*, n_i^*, T^*) from the list L_1 . If $T^* = 0$, \mathcal{C} fails and stops. Otherwise, it continues and list L_2 must contain an item $(m^*, U^*, ID_s^*, y_r^*, e_i^*)$ with an overwhelming probability. Because $h_2^* = H_2(m^*, U^*, ID_s^*, y_r^*)$ was defined as $e_i^*P \in G_1$, if \mathcal{F} succeeds in the game, \mathcal{C} realizes that $e(P, V^*) = e(P_{pub}, Q_{ID_s^*}^*)e(U^*, h_2^*)$ with $h_{2,i}^* = e_i^*P, Q_{ID_s^*}^* = n_i^*bP$ for $e_i^*, n_i^* \in Z_q^*$. Then, \mathcal{C} is aware of that $e(P, V^*) = e(aP, n_i^*bp)e(U^*, e_i^*P)$ and that $n_i^{*-1}(V^* - e_i^*U^*)$ is the solution of the CDH problem.

Now we evaluate the ρ value. \mathcal{C} 's successful probability in all key extraction queries is at most ρ^{q_k} . During the forgery phase, the probability that \mathcal{F} has not asked a key extraction query for an identity ID_s^* is $1 - \rho$. In addition, \mathcal{C} 's probability of success for all key extraction queries is $\rho^{q_k}(1 - \rho)$. The value is maximized at $\rho' = q_k/(q_k + 1)$. Utilizing this value, ρ' , we obtain

$$\left(\frac{q_k}{q_k + 1}\right)^{q_k} \left(1 - \frac{q_k}{q_k + 1}\right) = \frac{1}{\left(1 + \frac{1}{q_k}\right)^{q_k}} \frac{1}{q_k + 1}.$$

Additionally, utilizing the result $\lim_{\lambda \rightarrow 0} (1 + \lambda)^{1/\lambda} = e$, we have $\frac{1}{\left(1 + \frac{1}{q_k}\right)^{q_k}} \geq \frac{1}{e}$ for large q_k values. Hence, the probability that \mathcal{C} will succeed in key extraction queries is at most $\frac{1}{e^{(q_k+1)}}$, while the probability of \mathcal{C} failing at all signcryption queries is $q_s(q_s + q_{H_2})/2^k$ because a conflict exists on H_2 . Therefore, we obtain

$$\epsilon' \geq \epsilon \frac{1}{e^{(q_k + 1)}} \left(1 - \frac{q_s(q_s + q_{H_2})}{2^k}\right).$$

Performance evaluation

Table 2 shows the performance of the proposed scheme, which is evaluated based on comparing the major computational cost, security, and communication overhead of our scheme with those of existing schemes SL-II [17], HWY-I [18], HWY-II [18] and LX-II [19], which are representative HSC schemes. In these four schemes, the senders work in the IBC setting and the receivers work in the PKI setting. They are denoted by PM, E, PC, the point multiplication in G_1 , the exponentiation, and the pairing operation in G_2 . Since hash function operation and XOR operations are much cheaper than PM or PC, we ignore those two operations. We

Table 2. Performance comparison.

Schemes	Computational cost		Security				Communication overhead (bits)
	Signcrypt	Unsigncrypt	CCA2	CMA	ANON	IS	
SL-II [17]	1PC	1PC+1E	Yes	No	No	No	560
HWY-I [18]	3PM	2PM+2PC	Yes	Yes	No	Yes	1328
HWY-II [18]	2PM	4PM	Yes	Yes	No	Yes	1328
LX-II [19]	2PM+1E	2PC+1PM+1E	Yes	Yes	No	Yes	704
Ours	3PM	1PM+3PC	Yes	Yes	Yes	Yes	432

<https://doi.org/10.1371/journal.pone.0208311.t002>

assume that the sender in an IBC system has limited computation and storage capability but that the receiver in the PKI system has sufficient computation and storage resources. Therefore, we compare only the computational cost for signcryption. From Table 2, we can see that the computational cost of signcryption in these five schemes is considerable. In the “security” column, CCA2, CMA, and IS, denote IND-CCA2, EUF-CMA, and insider security, respectively. we can see that SL-II [17] does not meet CMA and IS security requirements. HWY-I [18], HWY-II [18], LX [19] and our scheme meet the requirements of insider security. In the “Communication overhead” column, our scheme is the shortest at 432 bits.

Here we give a quantitative analysis for SL-II [17], HWY-I [18], HWY-II [18], LX-II [19] and our scheme. We also only consider the smart meter part which has limited capacity. The experiment in [37] is adopted on MICA2 which is equipped with an ATmega128 8-bit processor clocked at 7.3728 MHz, 4 KB RAM and 128 KB ROM. According to [37], a PC needs 1.9s and an E needs 0.9s utilizing the supersingular curve $y^2 + y = x^3 + x$ with an embedding degree 4 and implementing η_T pairing: $E(F_{2^{271}}) \times E(F_{2^{271}}) \rightarrow F_{2^{4 \cdot 271}}$ at an 80-bit security level. From [38], a PM operation in the extension field $F_{2^{4 \cdot 271}}$ takes about 0.81s. As in [37, 38], we can see that the computational time on the meter of SL-II [17], HWY-I [18], HWY-II [18], LX-II [19] and our scheme are $1 \cdot 1.9 = 1.9s$, $3 \cdot 0.81 = 2.43s$, $2 \cdot 0.81 = 1.62s$, $2 \cdot 0.81 + 1 \cdot 0.9 = 2.52s$ and $3 \cdot 0.81 = 2.43s$, respectively. Fig 1 shows the relationship between the computational cost of smart meters and the related protocols. From Fig 1, we can see that the computational cost of our scheme is not the least, which is lower than LX-II [19], but higher than SL-II [17] and HWY-II [18].

According to [37, 39], let us suppose that the current draw in active mode is 8.0mA, the current draw in receiving mode is 10mA, the current draw in transmitting mode is 27mA, the power level of MICA2 is 3.0V, and the data rate is 12.4kbps. For energy consumption, as in [40, 41], a PC operation consumers $3.0 \cdot 8.0 \cdot 1.9 = 45.6mJ$, an E operation in G_2 consumers $3.0 \cdot 8.0 \cdot 0.9 = 21.6mJ$ and a PM consumers $3.0 \cdot 8.0 \cdot 0.81 = 19.44mJ$. Hence, the computational energy cost on the meter of SL-II [17], HWY-I [18], HWY-II [18], LX-II [19] and our scheme are $1.9 \cdot 45.6 = 86.64mJ$, $3 \cdot 0.81 \cdot 19.44 = 47.24mJ$, $2 \cdot 0.81 \cdot 19.44 = 31.49mJ$, $2 \cdot 0.81 \cdot 21.16 + 0.9 \cdot 19.44 = 51.78mJ$ and $3 \cdot 0.81 \cdot 19.44 = 47.24mJ$, respectively.

For the communication cost, let us suppose that $|ID| = 80bits$ as well as $|m| = 160bits$. Because we employ a subgroup G_1 of the 252-bit prime order, which is based on the supersingular curve $y^2 + y = x^3 + x$ over $F_{2^{271}}$, an element’s size in group G_1 is 542bits and can be reduced to 272bits (34 bytes) by means of standard compression technique [37] and an element’s size in group G_2 is 1084bits. Therefore, the meter in SL-II [17], HWY-I [18], HWY-II [18], LX-II [19] and the proposed scheme needs to transmit 560bits = 70bytes, 1328bits = 166bytes, 1328bits = 166bytes, 704bits = 88bytes and 432bits = 54bytes messages. From [37], we can see that the meter consumers $3 \cdot 27 \cdot 8/12400 = 0.052mJ$ to transmit one byte messages. Hence, the communication energy consumption of the meter in SL-II [17],

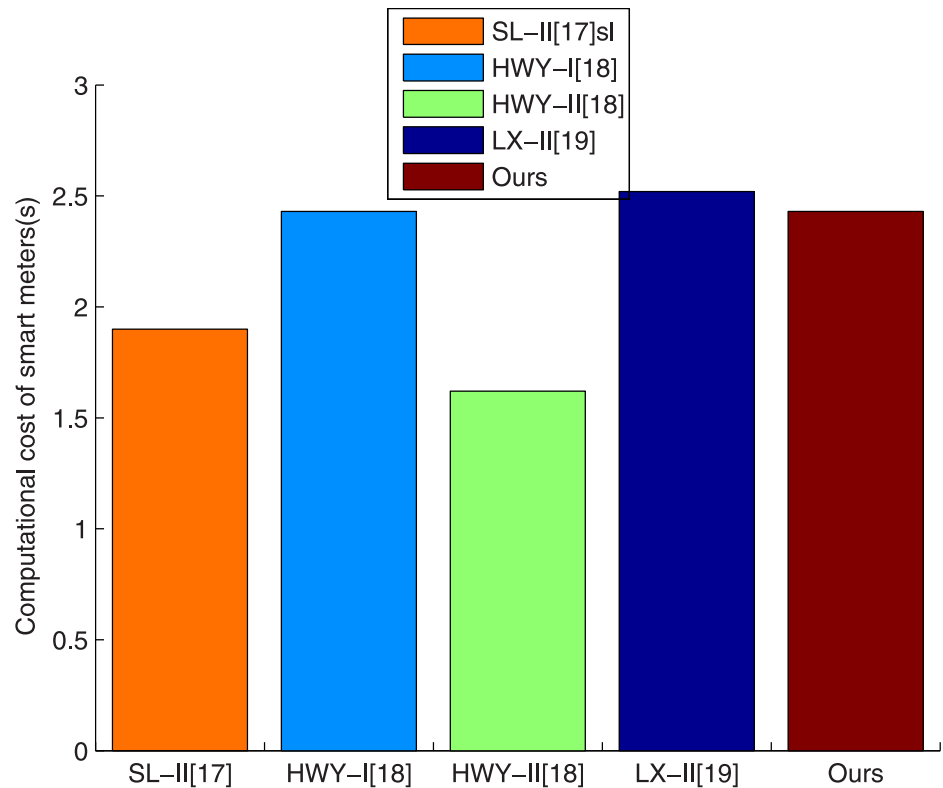


Fig 1. The computational cost of smart meters versus related protocols.

<https://doi.org/10.1371/journal.pone.0208311.g001>

HWY-I [18], HWY-II [18], LX-II [19] and our scheme are $0.025 * 70 = 1.75\text{mJ}$, $0.025 * 166 = 4.15\text{mJ}$, $0.025 * 166 = 4.15\text{mJ}$, $0.025 * 88 = 2.2\text{mJ}$, $0.025 * 54 = 1.35\text{mJ}$. Therefore, the total energy consumption of SL-II [17], HWY-I [18], HWY-II [18], LX-II [19] and our scheme are $86.84 + 1.75 = 88.39\text{mJ}$, $47.24 + 4.15 = 51.39\text{mJ}$, $31.49 + 4.15 = 35.64\text{mJ}$, $51.78 + 2.2 = 53.98\text{mJ}$ and $47.24 + 1.35 = 48.59\text{mJ}$.

The communication energy consumption at the meter is summarized in Fig 2, from which we can see that the proposed scheme requires the least energy consumption for communication among the five tested schemes. We can also see that the proposed scheme needs only 1.35mJ to transmit a message. This energy cost is highly suitable for practical use in a smart grid.

Conclusion

In this paper, we proposed an efficient HSC scheme for secure smart grid communications that allows a sender to belong to an IBC environment but to transmit a message to a receiver belonging to a PKI environment. The proposed scheme is proved to have IND-CCA2 as well as EUF-CMA properties under the CDH problem in the random oracle model, and it achieves confidentiality, integrity, authentication and non-repudiation simultaneously in a single logical step. Compared with existing HSC schemes that support a sender working in an IBC setting and a receiver working in a PKI setting, our scheme greatly enhances the communication efficiency, which meets the demand for real-time power usage data transmission in smart grid communications. A performance analysis is provided to demonstrate the efficiency improvement.

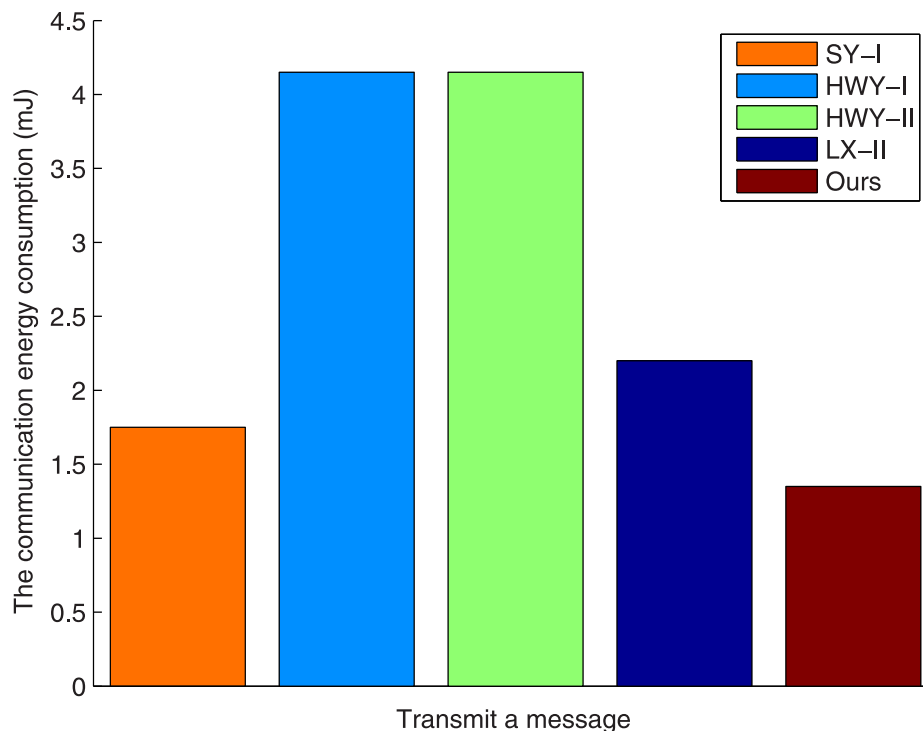


Fig 2. The communication energy consumption versus transmit a message.

<https://doi.org/10.1371/journal.pone.0208311.g002>

Supporting information

S1 Fig. The computational cost of smart meters versus related protocols.

(PDF)

S2 Fig. The communication energy consumption versus transmit a message.

(PDF)

S1 File. The minimal underlying data set.

(DOCX)

Acknowledgments

The authors thank the anonymous reviewers and the Editor for the constructive comments and generous feedback.

Author Contributions

Formal analysis: Guanhua Chen, Changhui Yu.

Investigation: Chunhua Jin.

Project administration: Jinsong Shan.

Supervision: Jianyang Zhao.

Validation: Changhui Yu, Ying Jin.

References

1. Ren K, Li Z, Qiu R. Guest editorial cyber, physical, and system security for smart grid. *IEEE Transactions on Smart Grid*. 2011; 2(4): 643–644. <https://doi.org/10.1109/TSG.2011.2175834>
2. Su W, Eichi H, Zeng W, Chow MY. A survey on the electrification of transportation in a smart grid environment. *IEEE Transactions on Industrial Informatics*. 2012; 8(1): 1–10 <https://doi.org/10.1109/TII.2011.2172454>
3. Liang H, Choi BJ, Zhuang W, Shen X. Towards optimal energy store-carry-and-deliver for PHEVs via V2G system. *Proc. INFOCOM*: 2012; 1674–1682.
4. Mets K, Ojea JA, Develder C. Combining power and communication network simulation for cost-effective smart grid analysis. *IEEE Communications Surveys & Tutorials*. 2014; 16(3): 1771–1796 <https://doi.org/10.1109/SURV.2014.021414.00116>
5. Erol-Kantarci M, Mouftah HT. Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues. *IEEE Transactions on Industrial Informatics*. 2012; 8(1): 1–10
6. Li F, Luo B, Liu P. Secure information aggregation for smart grids using homomorphic encryption. *Proc. Smart Grid Communications (SmartGridComm)*. 2010; 327–332
7. Lu R, Liang X, Li X, Lin X, Shen X. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*. 2012; 23(9): 1621–1631 <https://doi.org/10.1109/TPDS.2012.86>
8. Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*. 2014; 16(4): 1933–1954 <https://doi.org/10.1109/COMST.2014.2320093>
9. Liu T, Liu Y, Mao Y, Sun Y, Guan X, Gong W, Xiao S. A dynamic secret-based encryption scheme for smart grid wireless communication. *IEEE Transactions on Smart Grid*. 2014; 5(3): 1175–1182 <https://doi.org/10.1109/TSG.2013.2264537>
10. Hu B, Gharavi H. Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking. *IEEE Transactions on Smart Grid*. 2014; 5(2): 550–558 <https://doi.org/10.1109/TSG.2013.2277963>
11. Chim TW, Yiu SM, Li VO, Hui LC, Zhong J. PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Transactions on Dependable and Secure Computing*. 2015; 12(1): 85–97 <https://doi.org/10.1109/TDSC.2014.2313861>
12. Diao F, Zhang F, Cheng X. A privacy-preserving smart metering scheme using linkable anonymous credential. *IEEE Transactions on Smart Grid*. 2015; 6(1): 461–467 <https://doi.org/10.1109/TSG.2014.2358225>
13. He D, Kumar N, Lee JH. Privacy-preserving data aggregation scheme against internal attackers in smart grids. *Wireless Networks*. 2016; 22(2): 491–502 <https://doi.org/10.1007/s11276-015-0983-3>
14. Liu Y, Cheng C, Gu T, Jiang T, Li X. A Lightweight Authenticated Communication Scheme for Smart Grid. *IEEE Sensors Journal*. 2016; 16(3): 836–842 <https://doi.org/10.1109/JSEN.2015.2489258>
15. Saxena N, Choi BJ, Lu R. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*. 2015; 11(5): 907–921 <https://doi.org/10.1109/TIFS.2015.2512525>
16. Li CK, Yang G, Wong DS, Deng X, Chow SS. An efficient signcryption scheme with key privacy and its extension to ring signcryption. *Journal of Computer Security*. 2010; 18(3): 451–473 <https://doi.org/10.3233/JCS-2009-0374>
17. Sun Y, Li H. Heterogeneous signcryption with key privacy. *The Computer Journal*. 2010; 53(3): 557–566
18. Huang Q, Wong DS, Yang G. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction. *Science China Information Sciences*. 2011; 54(4): 525–536
19. Li F, Xiong P. Practical secure communication for integrating wireless sensor networks into the internet of things. *IEEE Sensors Journal*. 2013; 13(10): 3677–3684 <https://doi.org/10.1109/JSEN.2013.2262271>
20. Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)+ cost (signature)+ cost (encryption). *Proc. Annual International Cryptology Conference*. 1997; 165–179
21. Bao F, Deng RH. Asigncryption scheme with signature directly verifiable by public key. *Proc. Public Key Cryptography*. 1998; 55–59
22. Gamage C, Leiwo J, Zheng Y. Encrypted message authentication by firewalls. *Proc. Public Key Cryptography*. 1999; 69–81

23. Malone-Lee J, Mao W. Two birds one stone: signcryption using RSA. *Proc. RSA Conference*. 2003; 211–226
24. Boyen X. Multipurpose identity-based signcryption. *Proc. Annual International Cryptology Conference*. 2003; 383–399
25. Barreto PS, Libert B, McCullagh N, Quisquater JJ. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. *Proc. the Theory and Application of Cryptology and Information Security*. 2005; 515–532
26. Chen L, Malone-Lee J. Improved identity-based signcryption. *Proc. Public Key Cryptography*. 2005; 362–379
27. So HKH, Kwok SH, Lam EY, Lui KS. Zero-configuration identity-based signcryption scheme for smart grid. *Proc. Smart Grid Communications (SmartGridComm)*. 2010; 321–326
28. Jo HJ, Paik JH, Lee DH. Efficient privacy-preserving authentication in wireless mobile networks. *IEEE Transactions on Mobile Computing*. 2014; 13(7): 1469–1481 <https://doi.org/10.1109/TMC.2013.134>
29. An JH, Dodis Y, Rabin T. On the security of joint signature and encryption. *Proc. the Theory and Applications of Cryptographic Techniques*. 2002; 83–107
30. Li F, Zhang H, Takagi T. Efficient signcryption for heterogeneous systems. *IEEE Systems Journal*. 2013; 7(3): 420–429 <https://doi.org/10.1109/JSYST.2012.2221897>
31. Li F, Zheng Z, Jin C. Secure and efficient data transmission in the Internet of Things. *Telecommunication Systems*. 2016; 62(1): 111–122 <https://doi.org/10.1007/s11235-015-0065-y>
32. Li F, Han Y, Jin C. Practical Signcryption for Secure Communication of Wireless Sensor Networks. *Wireless Personal Communications*. 2016; 1–22
33. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. *Proc. Annual International Cryptology Conference*. 2003; 213–229
34. Libert B, Quisquater JJ. New identity based signcryption schemes from pairings. *IACR Cryptology ePrint Archive*. 2003, 23
35. Chow SS, Yiu SM, Hui LC, Chow KP. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. *Proc. Information Security and Cryptology*. 2003, 352–369
36. Coron JS. On the exact security of full domain hash. *Proc. Annual International Cryptology Conference*. 2000, 229–235
37. Shim KA, Lee YR, Park CM. EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad Hoc Networks*. 2000; 11(1): 182–189 <https://doi.org/10.1016/j.adhoc.2012.04.015>
38. Gura N, Patel A, Wander A, Eberle H, Shantz SC. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. *Proc. Cryptographic Hardware and Embedded Systems*. 2004; 119–132
39. Cao X, Kou W, Dang L, Zhao B. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. *Computer communications*. 2008; 31(4): 659–667 <https://doi.org/10.1016/j.comcom.2007.10.017>
40. Ma C, Xue K, Hong P. Distributed access control with adaptive privacy preserving property for wireless sensor networks. *Security and Communication Networks*. 2014; 7(4): 759–773 <https://doi.org/10.1002/sec.777>
41. Shim KA. S2DRP: secure implementations of distributed reprogramming protocol for wireless sensor networks. *Ad Hoc Networks*. 2014; 19: 1–8 <https://doi.org/10.1016/j.adhoc.2014.01.011>