Identity-based Deniable Authenticated Encryption for E-voting Systems

Chunhua Jin[1], Guanhua Chen[1*], Jianyang Zhao[1], Shangbing Gao[1], Changhui Yu[1]
[1] Faculty of Computer & Software Engineering, Huaiyin Institute of Technology
Huaian, 233003 - China
[e-mail: xajch0206@163.com]
*Corresponding author: Guanhua Chen

Received December 4, 2017; revised April 3, 2018; revised September 28, 2018; accepted November 13, 2018; published June 30, 2019

Abstract

Deniable authentication (DA) is a protocol in which a receiver can generate an authenticator that is probabilistically indistinguishable from a sender. DA can be applied in many scenarios that require user privacy protection. To enhance the security of DA, in this paper, we construct a new deniable authenticated encryption (DAE) scheme that realizes deniable authentication and confidentiality in a logical single step. Compared with existing approaches, our approach provides proof of security and is efficient in terms of performance analysis. Our scheme is in an identity-based environment; thus, it avoids the public key certificate-based public key infrastructure (PKI). Moreover, we provide an example that shows that our protocol is applicable for e-voting systems.

Keywords: DAE, identity-based cryptography, random oracle model

http://doi.org/10.3837/tiis.2019.06.029 **ISSN : 1976-7277**

1. Introduction

Network communication has become an indispensable part of our daily lives. The security of network communication is a problem we have to consider. To achieve secure communication over the network, two basic security needs have to be considered: message confidentiality and message authentication. Message confidentiality typically means that a sender encrypts the message to be transmitted using the session key through symmetric cryptography; then, the session key is encrypted employing a receiver's public key; finally, the resulting ciphertext is sent with the encrypted symmetric key (ESK) to the receiver. The receiver decrypts ESK using his secret key, and then decrypts the resulting ciphertext using the session key. Message authentication is generally realized through digital signatures; however, the digital signature scheme is a non-repudiation scheme, and any independent third party can certify its validity, which is undesirable for applications where privacy is needed (such as e-voting systems). Therefore, deniable authentication was developed to protect the privacy of users.

Deniable authentication protocol (DAP) is designed to achieve two properties: (1) for a given message, only the prescribed receiver can determine its source; and (2) for any third party, the specified receiver is not capable of determining the provenience of a prescribed message. As such, DAPs are useful in many application scenarios that require privacy protection, such as electronic voting systems, e-tendering systems, and internet negotiations[1].

1.1 Related Work

Dwork et al.[2] developed the first DAP, which achieves concurrent zero-knowledge by pushing all use of timing into a constant round preprocessing phase. In 2013, Chen and Chou[3] proposed an ECC-based DAP. Their protocol, which is very efficient, used the Fiat–Shamir heuristic to realize full deniability. In 2014, Li et al.[4] constructed an identity-based (IB) DAP in an ad hoc network. Their protocol provides provable security in the random oracle model (ROM). Gambs et al.[5] designed a distance bounding scheme which defines and models prover anonymity. The anonymity can insure that the server is not capable of distinguishing prover manner from rancorous verifier manner. Shi et al.[6] constructed a quantum DAP without entanglement. Their protocol has greater qubit efficiency and consumes fewer quantum resources. In terms of security, their design meets all known security requirements of DAP. Dimitriou and Al-Ibrahim[7] designed a deniable-LBS (location-based services) scheme. This scheme can protect user location privacy even if its location is leaked to any third-party. Mandal et al.[8] designed an IBDAP without pairings. Their scheme admits provable security in ROM under the ECCDH (elliptic curve computational Diffie–Hellman) problem and is applicable for mobile devices with limited resources. Hong and Wang[9] proposed a DA scheme without pairings. Their scheme provides provable security in the standard model and achieves a low computational cost by implementing a precomputation technique. In 2017, Zeng et al.[10] constructed an encryption scheme with multi-receiver which achieved CCA2 security to support deniable ring authentication. This protocol achieves full deniability, requires only two communication rounds, and can be applied in LBS to protect vehicle privacy. Later, Zeng et al.[11] designed a DA with a ring signature that can hide sources. Their construction is based on the projective hash function, and the encryption scheme is not required to achieve CCA security. Recently, Li et al.[12] proposed two heterogeneous DA protocols that allow the sender and the receiver to be in different environments.

However, when we carefully examine the protocols listed above, we find that the messages are all transmitted in plaintext, and thus carry the risk of revealing the entities' private information. For confidentiality, messages should be kept secret. Harn and Ren[13] designed a fully deniable authentication protocol that is supported by the current PGP and S/MIME to offer deniability and message authentication. Lu et al.[14] proposed a DAP. Their protocol provides proof of security in the ROM and achieves their alleged security requirements. Later, to resist receiver spoofing attacks, Yoon et al.[15] designed an improved DAP. They claimed that their construction meets all security requirements. Nevertheless, Li and Takagi[16] clear that Yoon et al.'s scheme has a security breach, where the receiver is capable of proving the provenience of a prescribed message to any independent third-party. Subsequently, based on their proposed signcryption, Hwang and Sung[17] designed a DAP that achieves confidentiality, sender anonymity and protection. Harn et al.[18] proposed a 1-out-of-∞ DAP that can achieve full deniability. Later, Hwang et al.[19] constructed a non-interactive (NIA) DAP that supports both fair protection and anonymity. Li et al.[20] designed a DAE scheme. They provide an example of how to apply their proposed DAE scheme to e-mail systems.

Nevertheless, the above protocols must simplify the key management procedure, as they are all in a PKI environment. To eliminate various disadvantages brought by PKI, identity-based DAE (IBDAE) was proposed[21,22,23]. Wu et al.[21] proposed the first IBDAE protocol. They provide the proof of security of their scheme in the ROM. Later, Li et al.[22] presented an IBDAE protocol using a hybrid signcryption mechanism. They provide proof of security in the ROM and had better performance by comprehensive performance evaluation. Jin and Zhao[23] designed an IBDAE scheme. Their scheme shows high efficiency in the light of comprehensive performance evaluation. Recently, many related protocols[24,25,26,27] have been presented. Jin et al.[24] proposed a DAE scheme, and their construction is applicable for e-voting systems. Unger and Goldberg[25] proposed three deniable authenticated key exchange protocols. These three protocols can support forward secrecy against future quantum adversaries. Ahene et al.[26] proposed a DAE scheme in a certificateless setting. They provide concrete instantiation in e-voting systems. Jin and Zhao[27] devised an efficient ciphertext length (CL) aggregate DA protocol. Their protocol adopts aggregate verification, which expedites authenticator verification.

1.2 Motivation and Contribution

Signature-then-encryption schemes have disadvantages in terms of computational and communication costs. To solve these problems, Zheng[28] presented the concept of signcryption (SC). Nevertheless, the SC scheme is a non-repudiation scheme, which is undesirable, especially for some confidential occasions. In this paper, our goal is to design a scheme that satisfies the deniability. Motivated by the aforementioned studies, in this paper, we construct a novel IBDAE scheme that provides confidentiality and deniable authentication in one logical step. Our construction provides proof of security in the ROM under the DBDH and BDH assumptions and shows high efficiency in terms of performance analysis. Moreover, we provide an example that involves integrating our scheme into e-voting systems.

1.3 Organization of the Paper

Section 2 depicts preliminary work. We define the security model for IBDAE in Section 3, and the IBDAE scheme is designed in Section 4. In Section 5, we analyze the IBDAE scheme and discuss formal security in the ROM. Section 6 presents the results of the performance tests of our design. A secure e-voting system is constructed in Section 7, and the conclusions are

provided in Section 8.

2. Preliminaries

This section discusses the basics of bilinear pairings.

Let G_1 and G_2 be a cycle additive group and a cycle multiplication group, respectively. G_1 is generated by P. G_1 and G_2 have the same prime order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$, with the properties as below:

- Bilinearity: For all $P, Q \in G_1, a, b \in Z_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$;
- Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;
- Computability: There exists an efficient algorithm for computing $e(P, Q)$ for all P, $Q \in G_1$.

The admissible maps of this type are the modified Weil pairing and the Tate pairing (Refs.[29,30] provide more information). The security of this scheme lies in the difficulty of the below problems.

Definition 2.1 According to the aforementioned basic definition of bilinear pairings, the DBDH problem in (G_1, G_2, e) is to determine whether $h = e(P, P)^{abc}$ given (P, aP, bP, cP) and an element $h \in G_2$.

Definition 2.2 According to the aforementioned basic definition of bilinear pairings, the BDH problem in (G_1, G_2, e) is to calculate $h = e(P, P)^{abc}$ given (P, aP, bP, cP).

3. Formal Model for the IBDAE Protocol

This section presents the framework and the security concepts.

3.1 Framework

Four algorithms of the presented protocol is described as below.

Setup: Upon inputting a security parameter *k*, a public key generator (PKG) produces the public system parameters params and a master private key *s*. For simplicity, the following algorithms do not include params.

Extract: Upon inputting *ID* (an identity) and *s*, PKG calculates S_{ID} (the corresponding private key) and outputs it securely to its owner.

DAE: Upon inputting a sender's private key S_{ID_s}, a message *m*, and a receiver's identity ID_r, the sender calculates DAE(m, S_{ID_s}, ID_r) to obtain the ciphertext σ.

DAD: Upon inputting a sender's identity ID_s, the ciphertext σ, and a receiver's private key S_{ID_r}, the receiver calculates DAD(σ, S_{ID_r}, ID_s), obtaining either the message *m* or $\perp$ when σ is an invalid ciphertext.

For consistency, if σ =DAE(m, S_{ID_s}, ID_r), then m=DAD (σ, S_{ID_r}, ID_s) must also be true.

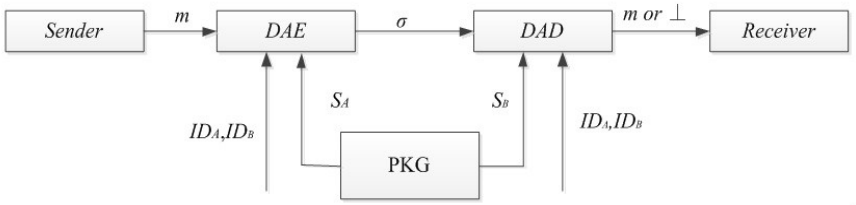

Fig. 1. Communication process in our scheme

Fig. 1 presents the communication process in which the sender generates the ciphertext σ for message m using his/her identity ID_s , private key S_{ID_s} , and the receiver's identity ID_r . The receiver decrypts σ using his/her identity ID_r with the corresponding private key S_{ID_r} and the sender's identity ID_s , resulting in either m or $\perp$. Note that S_{ID_s} and S_{ID_r} are from the PKG.

3.2 Security Concepts

Our construction must achieve the desirable security requirements below:

- Confidentiality: any independent third party other than the entities involved cannot acquire any valuable advice related to the plaintext of a ciphertext;
- Deniable authentication: the receiver creates a deniable transcript that is probabilistically indistinguishable from the sender.

For confidentiality, the standard security concept used in our construction is the indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2). For deniable authentication, the security concept used in our construction is the deniable authentication against adaptive chosen message attacks (DA-IBDAE-CMA) proposed in[4]. It is assumed that the following games (Definition 3.1 and Definition 3.2) are played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Definition 3.1 *An IBDAE scheme is IND-IBDAE-CCA2 secure when no adversary has a non-negligible advantage in the game below.*

Setup: $\mathcal{C}$ *executes Setup algorithm to create param and then transmit it to* $\mathcal{A}$.

Phase 1: $\mathcal{A}$ *adaptively executes queries; any request may count on the responses to former queries.*

- *Extract:* $\mathcal{A}$ *elects an identity* ID . $\mathcal{C}$ *executes the Extract algorithm and transmits the corresponding private key* S_{ID} *to* $\mathcal{A}$.
- *DAE:* $\mathcal{A}$ *elects a message m and two identities* ID_i, ID_j . $\mathcal{C}$ *first obtains the sender's private key* S_{ID_i} *by implementing the Extract algorithm. Then, it transmits the result of DAE(* m, S_{ID_i}, ID_j *) to* $\mathcal{A}$.
- *DAD:* $\mathcal{A}$ *elects two identities* ID_i *and* ID_j *, and a ciphertext* σ . $\mathcal{C}$ *first obtains the sender's private key* S_{ID_j} *by executing the Extract algorithm. Then, it transmits the result of DAD(* σ, ID_i, S_{ID_j} *) to* $\mathcal{A}$ *(if* σ *is invalid, the result is* $\perp$ *).*

Challenge: $\mathcal{A}$ determines when Phase 1 is over. Then, $\mathcal{A}$ outputs two challenged identities, ID_A and ID_B, and two equal-length messages, m_0 and m_1. It cannot request the private key of identities ID_A or ID_B in Phase 1. $\mathcal{C}$ elects a bit $b \in \{0,1\}$, calculates $\sigma = DAE(m_b, S_{ID_A}, ID_B)$ and transmits σ to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ requests queries as in Phase 1. In this phase, it cannot execute an *Extract* query on identities ID_A or ID_B nor can it execute a DAD query on (σ, ID_A, S_{ID_B}) to possess the message *m* for σ.

Guess: $\mathcal{A}$ outputs a guess b' and wins the game if $b = b'$.

The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |2P[b' = b] - 1|$, where $P[b' = b]$ denotes the probability that $b' = b$.

Definition 3.2 *An IBDAE scheme is DA-IBDAE-CMA secure when no adversary has a non-negligible advantage in the game below.*

Setup: The procedure is the same as Setup in Definition 3.1.

Attack: $\mathcal{A}$ adaptively executes queries (*any query counts on the responses to former queries*). *The allowed types of queries, such as Extract, DAE and DAD, are the same as those in Definition 3.1.*

Forgery: $\mathcal{A}$ exports a pair identities ID_A and ID_B and a ciphertext σ, which never emerge in any Extract query in the Attack phase. $\mathcal{A}$ wins the game if the result of DAD(σ^*, ID_A, S_{ID_B}) is not $\perp$.

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

In the previous definition, the adversary is unallowed to perform an Extract query on identity ID_B, which is essential for realizing deniability. The sender and the receiver can create an indistinguishable transcript.

4. A New IBDAE Protocol

This section presents our construction.

Setup: Define G_1,G_2, *e*, *k*, and *q* as in Section 2. Let *n*, *l* be security parameters, H_1, H_2, and H_3 be three hash functions, i.e., H_1: $\{0,1\}^* \rightarrow G_1$, H_2:$G_2 \rightarrow Z_q$, and H_3: $\{0,1\}^n \times Z_q \rightarrow \{0,1\}^l$, and *E* and D be symmetric encryption and decryption algorithms, respectively. PKG elects $s \in Z_q^*$ and calculates P_{pub}=sP. PKG publishes system parameters $(G_1, G_2, n, l, e, P, q, P_{pub}, H_1, H_2, H_3, E, D)$ but secretly retains *s*. The plaintexts must have a fixed bitlength of *n* where $n + l < k \approx \log_2^q$.

Extract: On input an identity *ID*, the PKG calculates the user's public key Q_{ID}=$H_1(ID) \in G_1$ and the corresponding private key S_{ID}=sQ_{ID}, which is sent to the owner securely.

DAE: Upon inputting a message *m*, a sender's private key S_{ID_s}, and a receiver's identity ID_r, the sender performs the following work.

- Select $x \in Z_q^*$.
- Calculate $\tau = e(P_{pub}, Q_{ID_r})^x$.
- Calculate $k_2 = H_2(\tau)$.
- Calculate $r = E_{k_2}(m \| H_3(m, k_2))$.
- Calculate $S = xP_{pub} - rS_{ID_s}$.
- Calculate $V = e(S, Q_{ID_r})$.
- Output $\sigma = (r, V)$.

DAD: Upon inputting a sender's identity ID_s, a ciphertext σ, and a receiver's private key S_{ID_r}, the receiver performs the procedure below.

- Calculate $\tau = Ve(Q_{ID_s}, S_{ID_r})^r$.
- Calculate $k_2 = H_2(\tau)$.
- Calculate $m' = D_{k_2}(r)$.
- Take m as the first n bits of m' if and only if $(m, H_3(m, k_2))$ are the first $n + l$ bits of m'.

5. Analysis of the Protocol

This section analyzes the presented protocol's consistency and security.

5.1 Consistency

We can certify the consistency of our construction by the equations below.

$$\begin{aligned} V &= e(S, Q_{ID_r}) \\ &= e(xP_{pub} - rS_{ID_s}, Q_{ID_r}) \\ &= e(xP_{pub}, Q_{ID_r}) e(-rS_{ID_s}, Q_{ID_r}) \\ &= e(P_{pub}, Q_{ID_r})^x e(S_{ID_s}, Q_{ID_r})^{-r} \\ &= \tau e(S_{ID_s}, Q_{ID_r})^{-r} \\ &= \tau e(Q_{ID_s}, S_{ID_r})^{-r} \\ &= V \end{aligned}$$

5.2 Security

We also certify that our design possesses deniability. A receiver with private key S_{ID_r} creates a ciphertext that is probabilistically indistinguishable from a ciphertext created by a sender possessing S_{ID_s}. To imitate the ciphertext, the receiver can perform the following steps.

- Select $\overline{x} \in Z_q^*$ randomly.
- Compute $\overline{\tau} = e(P_{pub}, Q_{ID_r})^{\overline{x}}$.
- Compute $\overline{k_2} = H_2(\overline{\tau})$.
- Calculate $\overline{r} = E_{\overline{k_2}}(\overline{m} \| H_3(\overline{m}, \overline{k_2}))$.
- Compute $\overline{V} = \overline{\tau} e(Q_{ID_s}, S_{ID_r})^{-\overline{r}}$.
- Output is $\overline{\sigma} = (\overline{r}, \overline{V})$.

The generated ciphertext $\overline{\sigma} = (\overline{r}, \overline{V})$ is indistinguishable from $\sigma = (r, V)$ produced by the sender in Section 4. The sender randomly chooses a ciphertext $\sigma' = (r', V')$ from the sender's valid set of ciphertexts that are intended for the receiver. The probability $P_r[\overline{\sigma} = \sigma']$ is $1/(q-1)$ because $\overline{\sigma}$ is chosen from $\overline{x} \in Z_q^*$. Likewise, the probability that $P_r[\sigma = \sigma']$ is the same value, $1/(q-1)$, because σ is chosen from $x \in Z_q^*$, i.e., they have the same probability distribution.

Next, we show that our design is provably secure. The two theorems below indicate that the design is secure with regard to both IND-IBDAE-CCA2 and DA-IBDAE-CMA.

Theorem 5.1 *In the ROM, if $\mathcal{A}$ wins the game in Definition 3.1, with an advantage of ε within a time t by at most requesting q_{H_i} queries to oracle $H_i (i = 1, 2, 3)$, q_K KE queries, q_E DAE queries, and q_D DAD queries, then $\mathcal{C}$ can settle the DBDH problem within a time of $O(t + (2q_{H_3}^2 + q_D)T_e)$ with an advantage of*

$$Adv(\mathcal{C}^{DBDH(G_1,P)}) > \frac{2(\varepsilon - q_D / 2^{k-1})}{q_{H_1}^4},$$

In which T_e represents the calculation time of the bilinear pairing.

Proof. $\mathcal{C}$ acquires (P, aP, bP, cP) of the DBDH problem and attempts to determine whether $h = e(P,P)^{abc}$. $\mathcal{C}$ is $\mathcal{A}$'s challenger in the IND-IBDAE-CCA2 game. $\mathcal{C}$ consults $\mathcal{A}$ for a response to H_1, H_2, and H_3 which are randomly produced. $\mathcal{C}$ maintains three lists, L_1, L_2, and L_3, to save the response. $\mathcal{A}$ will request $H_1(ID)$ before ID is employed.

Setup: $\mathcal{C}$ runs *Setup* algorithm and sends $P_{pub} = cP$ to $\mathcal{A}$. Note that $\mathcal{C}$ knows nothing about c, which serves as PKG's master private key.

Phase 1: $\mathcal{A}$ adaptively executes queries.

- H_1 queries: $\mathcal{C}$ randomly selects two index values $i, j \in \{1, ..., q_{H_1}\}$. $\mathcal{A}$ requests H_1 queries on identities it chooses. For query H_1, at the i-th, $\mathcal{C}$ returns $H_1(ID_i)$ as aP; $\mathcal{C}$ returns $H_1(ID_j)$ as bP at the j-th. For queries $H_1(ID_\alpha)$ with $\alpha \neq i, j$, $\mathcal{C}$ selects d_α from Z_q^*, stores (ID_α,d_α) in list L_1, and returns $H_1(ID_\alpha) = d_\alpha P$.
- H_2 queries: For query $H_2(g_e)$, $\mathcal{C}$ checks whether the value of H_2 is in the list. If so, it returns the same answer to $\mathcal{A}$; if not, $\mathcal{C}$ randomly picks a value $k_2 \in Z_q^*$ as a response and stores (g_e,

k_2) in L_2.

- H_3 queries: For query $H_3(m, k_2)$, $\mathcal{C}$ checks if the value of H_3 is in the list. If so, it transmits the same answer to $\mathcal{A}$. If not, $\mathcal{C}$ returns value $u \in Z_q^*$ as a response and stores (m, k_2, u) in list L_3.
- KE queries: When $\mathcal{A}$ submits an identity to $\mathcal{C}$, if ID_α=ID_i or ID_α = ID_j, $\mathcal{C}$ fails. If $ID_\alpha \neq ID_i, ID_j$, the list L_1 must have (ID_α, d_α) for some d_α (indicating that $\mathcal{C}$ previously answered $H_1(ID_\alpha)$=$d_\alpha P$). The private key of ID_α is $d_\alpha P_{pub}$= $d_\alpha cP$. The failure probability in KE queries is at most $2 / q_{H_1}$.
- DAE queries: $\mathcal{A}$ can perform DAE queries on m, ID_α and ID_β.
  (1). If $ID_\alpha \neq ID_i, ID_j$, $\mathcal{C}$ first calculates the private key S_{ID_α} by executing KE query algorithm; then, it performs the DAE($m, S_{ID_\alpha}, ID_\beta$) algorithm to answer the query.
  (2). If ID_α= ID_i or ID_α = ID_j, but $ID_\beta \neq ID_i, ID_j$, $\mathcal{C}$ runs a simulation as follows. It obtains the private key S_{ID_β} using the key extraction algorithm. Then, it selects the random elements $(r, V) \in Z_q^* \times G_2$ and computes $\tau = Ve(Q_{ID_s}, S_{ID_r})^r$. The simulation depends on whether list L_2 has a tuple of the form (τ, ·).
  When L_2 contains an entry (τ, k_2) and L_3 has an item (m, k_2, u), when the first n bits of $D_{k_2}(r)$ can be distinguished from m, $\mathcal{C}$ selects another (r, V) and repeats the procedure. When L_3 contains no entry for (m, k_2, u), $\mathcal{C}$ takes $u = [D_{k_2}(r)]_{n+1\ldots n+l}$ (in which $[x]_{i\ldots j}$ symbolises the bit string between the i-th and j-th leftmost bits of x) and stores (m, k_2, u) in list L_3.
  When no entry (τ, ·) exists in list L_2, $\mathcal{C}$ chooses a random $k_2 \in Z_q^*$. It also selects a random $u \in \{0,1\}^l$ to ensure that (m, ·, u) is not in list L_3. Then, it calculates $m' = m \| u$. When no item (m, k_2, u') with $u' \neq u$ is in list L_3, $\mathcal{C}$ stores (τ, k_2) and (m, k_2, u) in lists L_2 and L_3, respectively. Otherwise, $\mathcal{C}$ provides other alternative data (r, V) and repeats the procedure.
  $\mathcal{C}$ updates lists L_2 and L_3 after it searches alternative data (r, V), and it returns (r, V) as the ciphertext. The procedure is repeated at most $2qH_3$. After each attempt, only one pairing is computed.
  (3). When ID_α = ID_i, ID_β = ID_j or ID_β = ID_i, ID_α = ID_j, $\mathcal{C}$ randomly selects x from Z_q^* and computes τ = $e(P_{pub}, Q_B)^x$ and k_2 = $H_2(\tau)$ such that no (τ, k_2) exists in list L_2. Then, $\mathcal{C}$ verifies whether list L_3 contains an item for (m, τ, u). If not, $\mathcal{C}$ stores (m, τ, u) in list L_3 and (τ, k_2) in list L_2. Then, $\mathcal{C}$ computes $r = E_{k_2}(m \| u)$, selects $V \in G_2$ and transmits σ=(r, V) to $\mathcal{A}$. $\mathcal{A}$ would not know that σ is an invalid ciphertext, but it requests the decryption of σ.
- DAD queries: $\mathcal{A}$ generates a ciphertext σ for ID_α and ID_β. When $ID_\beta \neq ID_i, ID_j$, $\mathcal{C}$ can obtain S_{ID_β} by running the KE algorithm and then running DAD($\sigma, ID_\alpha, S_{ID_\beta}$). Otherwise, $\mathcal{C}$ fails. The failure probability is at the utmost $q_D / 2^k$.

After the first stage, $\mathcal{A}$ selects two identities it wishes to challenge. The challenged identities are (ID_i, ID_j) with a probability of at least $2/q_{H_1}$. $\mathcal{C}$ fails if $\mathcal{A}$ requests the private key of ID_i or ID_j in first stage because it is unable to answer the question. $\mathcal{C}$ also fails if $\mathcal{A}$ does not pick these two identities as the target identities.

Then, $\mathcal{A}$ creates two messages, m_0 and m_1. $\mathcal{C}$ chooses a random bit $b \in \{0,1\}$ and encrypts m_b. It chooses $r \in Z_q^*$ and $V \in G_2$ and computes $\tau = Vh^r$ (where h is $\mathcal{C}$'s candidate for the DBDH problem) to receive $k_2 = H_2(\tau)$ (according to H_2 simulation algorithm) and $u_b = H_3(m_b, k_2)$ (according to H_3 simulation algorithm). Then, it verifies whether L_3 already contains the entry (m_b, k_2, u_b). If not, it stores (m_b, k_2, u_b) in list L_3; otherwise, it selects another (r,V) and repeats the procedure. After looking up admissible element (r,V), $\mathcal{C}$ sends the ciphertext $\sigma = (r,V)$ to $\mathcal{A}$.

$\mathcal{A}$ then executes the second stage queries as in the first stage. When the simulation is over, it creates a bit b' as $\sigma = DAE(m_{b'}, S_{ID_i}, ID_j)$ from the standpoint of $\mathcal{A}$. If $b = b'$, $\mathcal{C}$ answers 1 because $\mathcal{A}$ has produced a valid σ using its knowledge of h. Otherwise, $\mathcal{C}$ responds 0.

Now we consider $\mathcal{C}$'s probability of success. $\mathcal{C}$ does not successful if $\mathcal{A}$ requests the private key of ID_i or ID_j in the first stage. There are $\binom{q_{H_1}}{2}$ options to pick (ID_i, ID_j). Of these identities, at least one will never have made a KE query from $\mathcal{A}$. $\mathcal{A}$ will not query Keygen(ID_i) and Keygen(ID_j) with a probability greater than $2/q_{H_1}$. Further, $\mathcal{A}$ elects challenge identities (ID_i, ID_j) with a exactly probability $2/q_{H_1}$, and $\mathcal{C}$ settles its DBDH problem if $\mathcal{A}$ wins the IND-IBDAE-CCA game.

In the end, because $p_1 = \Pr[b' = b \mid \sigma = DAE(m_b, S_{ID_i}, ID_j)] = \frac{\varepsilon + 1}{2} - \frac{q_D}{2^k}$

$$p_0 = \Pr[b' = i \mid h \in G_2] = 1/2 \text{ for i=0,1}$$

we have

$$Adv(\mathcal{C}) = \left| \Pr_{a,b,c \in \mathbb{Z}_q}[1 \leftarrow \mathcal{C}(aP, bP, cP, e(P,P)^{abc})] - \Pr_{a,b,c \in \mathbb{Z}_q, h \in G_2}[1 \leftarrow \mathcal{C}(aP, bP, cP, h)] \right|$$

$$= \frac{|p_1 - p_0|}{(2/q_{H_1})^2} = \frac{\varepsilon - q_D/2^{k-1}}{2(2/q_{H_1})^2} > \frac{2(\varepsilon - q_D/2^{k-1})}{q_{H_1}^4}.$$

Note that the denominator is $q_{H_1}^4$ rather than $q_{H_1}^2$ because $\mathcal{A}$ determines the challenged identities after the first stage.

Theorem 5.2 In the ROM, if $\mathcal{A}$ wins the game of Definition 3.2 with an advantage of $\varepsilon \geq 5(q_E + 1)(q_E + q_{H_3})q_{H_1}/(2^k - 1)$ within time *t* and by at most requesting q_{H_i} queries to $H_i (i = 1,2,3)$, q_K KE queries, q_E DAE queries, and q_D DAD queries, then $\mathcal{C}$ settles the BDH problem in an expected time of $t' \leq 60343 q_{H_3} q_{H_1} 2^k t / \varepsilon(2^k - 1)$.

Proof. To wield the forking algorithm[31], we have to prove how our design is applicable for the signature scheme described in[31]. In DAE imitate steps, the sender's private key fails (implying that the master private key fails). In this case, a method is needed to settle the BDH problem.

First, observe that the DAE of our design meets the requested three-phase honest-verifier zero-knowledge identification protocol, in which $\sigma_1 = k_2 = H_2(e(P_{pub}, Q_B)^x)$ is the commitment, $h = H_3(m, k_2)$ is the hash value, and σ_2=V is the answer.

Second, we give a concrete imitate step and show a method of settling the BDH problem. Upon inputting (P, aP, bP, cP) of the BDH problem, $\mathcal{C}$ is needed to calculate $e(P,P)^{abc}$. $\mathcal{C}$ executes $\mathcal{A}$ as a subroutine. $\mathcal{A}$ consults $\mathcal{C}$ to answer H_1, H_2, and H_3 and $\mathcal{C}$ holds lists L_1, L_2, and L_3 to save the randomly generated responses. The H_1, H_2, H_3, DAE and DAD queries are requested in the way they are in the proof of Theorem 1.

Forgery: $\mathcal{A}$ outputs a triple (σ^*, ID_i, ID_j), where $\sigma^* = (r^*, V^*)$. We coalesce the identities $ID_\theta = \{ID_i, ID_j\}$ and the message m^* into (ID_θ, m^*) so that we can hide the IB aspect of the DA-IBDAE-CMA attacks and imitate an identity-less adaptive-CMA existential forgery.

If $\mathcal{A}$ is an attacker with adequate efficiency in the above interaction, we can create a Las Vegas machine $\mathcal{A}'$ that returns two forgeries $((ID_\theta, m^*), r^*, V^*)$ and $((ID_\theta, m^*), \bar{r}^*, \bar{V}^*)$ with $r^* \neq \bar{r}^*$ and the same commitment x. To settle the BDH problem based on the machine $\mathcal{A}'$ derived from $\mathcal{A}$, we construct a machine $\mathcal{C}'$ as follows.

- $\mathcal{C}'$ executes $\mathcal{A}'$ to acquire two distinct forgeries $((ID_\theta, m^*), r^*, V^*)$ and $((ID_\theta, m^*), \bar{r}^*, \bar{V}^*)$.
- $\mathcal{C}'$ calculates $e(P,P)^{abc}$ as $(V^*/\bar{V}^*)^{-1/(\bar{r}^* - r^*)}$.

The machine $\mathcal{C}'$ is our reduction of the BDH problem. If the success probability of $\mathcal{A}'$ is $\varepsilon \geq 5(q_E + 1)(q_E + q_{H_3})q_{H_1} / (2^k - 1)$, while its running time is t, then $\mathcal{C}'$ can settle the BDH problem in an expected time $t' \leq 60343 q_{H_3} q_{H_1} 2^k t / \varepsilon(2^k - 1)$. Here, there is a change in the coefficient since the simulator has to bring forward two disparate identities.

6. A Secure E-voting Protocol

The construction is employed in an e-voting system (EVS). Here, we provide the example shown in **Fig. 2**. An electronic power corporate expects to select a general manager by having all employees vote. However, if the votes are sent as plaintext, the process would be insecure. Each employee is a voter who first runs $DAE(m, S_{ID_s}, Q_{ID_r})$ to gain the ciphertext. Then, the voter sends the ciphertext to the electronic power tally authority (TA). In this protocol, a PKG exists in the company in charge of registration. The PKG gives a secret key to each employee and to the TA. The employees can use their smart devices to transmit their ciphertexts to the TA. Finally, the TA runs $DAD(\sigma, Q_{ID_S}, S_{ID_r})$ to obtain each message m. While the TA can know that the ciphertexts were sent by valid staff because the protocol

owns the authentication, the TA cannot certify the sender's identity of the ciphertext to any trusted entity, as this design is deniable. Moreover, if the TA and a third party were to cooperate, the third party might suspect the truth of the ciphertext as provided by the TA because the TA can also generate valid ciphertexts. Thus, the third party cannot force an employee to select a particular candidate.

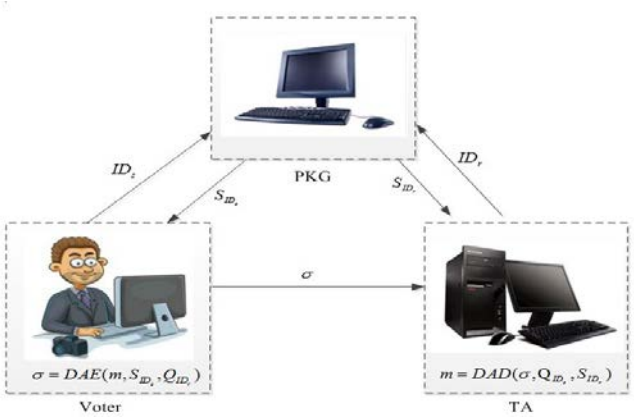

Fig. 2: A secure e-voting protocol

7. Performance

We will construct a detailed performance analysis of our design with the existing schemes[16,17,21,22] listed in Table 1. We employ the point add (PA) calculation and the point multiplication (PM) calculation in G_1, the bilinear pairing (BP) calculation, the modular exponentiation (ME) calculation and the multiplication (MT) calculation in a finite field, and a certificate verification (CV) calculation (which generally costs approximately the same as two ME computations). Note that the ME calculation in a finite field (FF) is equivalent to a PM calculation in the elliptic curve cryptosystem (ECC) (i.e., ME=PM), and the MT calculation in a FF is equal to the PA calculation in ECC (i.e., MT=PA). The XOR, hash function, and add calculation in a FF are omitted because their computation speeds are sufficiently fast to be negligible. Additionally, let $|G_1|$ =160 bits, $|m|$ = 160 bits, $|p|$ = 512 bits, $|cert|$ = 320 bits, $|q|$ = 160 bits, hash value = 160 bits, and $|G_2|$ =1024 bits. Here, the key size (KS) is made up of both public key and private key size. As shown in **Table 1**, regarding KS and CL, our approach is highly efficient. Additionally, the scheme in [16] is interactive and lacks proof of security. Our design is in the ID-based setting. As such, our design avoids problems related to PKI.

We conduct an experiment on the PBC library. As needed, we set the library's embedding degree to 2. The experiment is executed on an Intel Pentium(R) Dual-Core processor running at 2.69 GHz, with 2,048 MB of RAM (2,007.04 MB available). On this machine, a PA computation and a PM computation require 0.065 ms and 15.927 ms using an ECC with 160 bits of q, respectively. A BP computation and a ME computation require 26.68 ms and 3.126 ms, respectively. DAE and DAD consume 95.562 ms and 95.562 ms in [16], 79.7 ms and 63.773 ms in [17], 88.34 ms and 42.672 ms in [21], and 101.206 ms and 58.534 ms in[22]. In our scheme, DAE and DAD consume 101.206 ms and 42.607 ms, respectively. [16,17,21,22], the computational expense for DAE in our design is the same as that in [22] but slightly higher than those in [16,17,21] because it requires two pairings that belong to G_2. Our design has the lowest computational expense for DAD, although we have one pairing

computation. In terms of type, [16,17] are in the PKI setting, while [21,22] and our design are in an ID-based setting and avoid the problems in PKI. **Fig. 4** shows the CL for [16,17,21,22] and our scheme. Although our design must transmit V, which belongs to G_2, our protocol still has the smallest communication overhead.

Table 1. Performance comparison

Schemes	Computational cost		KS	CL	Interactive mode	Security proof	Type
	DAE	DAD					
Li[16]	4ME+1CV =6ME	4ME+1CV =6ME	672	832+$\|cert\|$ =1252	IA	No	PKI
Hwang[17]	3ME+1MT +1CV =5ME+1MT	2ME+1MT+ 1CV =4ME+1MT	672	992+ $\|cert\|$ =1312	NIA	Yes	PKI
Wu[21]	2BP+1ME +2PM	2BP+1PA+1 PM	320	1856	NIA	Yes	ID
Li[22]	2BP+1PA+ 3PM	1BP+2PM	320	1536	NIA	Yes	ID
Ours	2BP+3PM +1PA	1BP+1PM	320	1184	NIA	Yes	ID

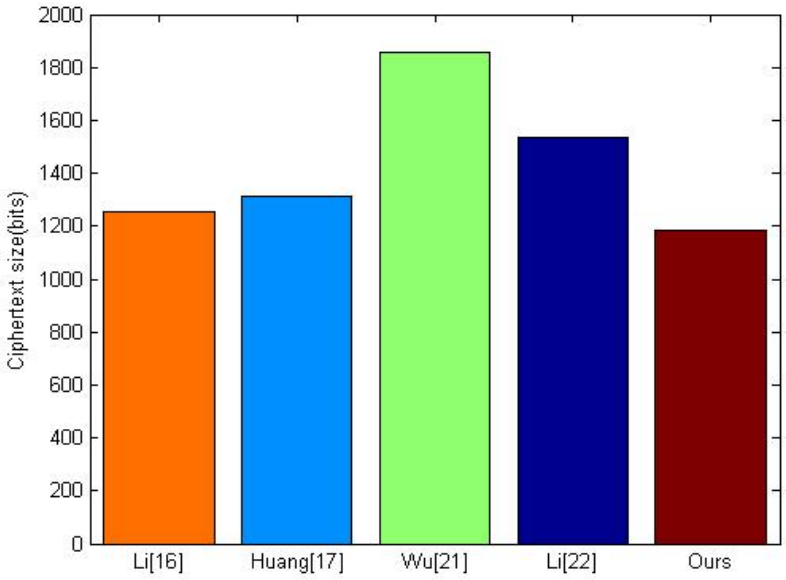

Fig. 3. Primary computational cost of DAE

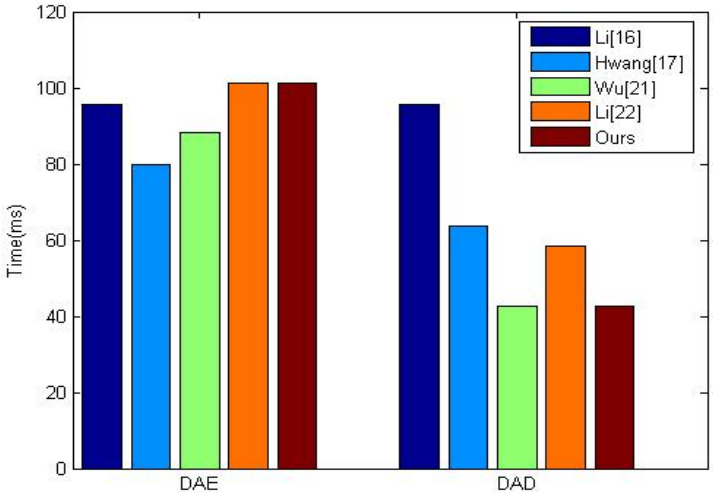

Fig. 4. Communication overhead of DAE

8. Conclusion

In this paper, we construct a novel non-interactive IBDAE scheme that realizes deniable authentication and confidentiality in a logical single step. Our construction provides proof of security and is efficient in terms of performance analysis. In addition, we provide an example to show how our construction can be used in e-voting systems. As such, our design is applicable to privacy protection scenarios.

Acknowledgements

This work is supported by the Natural Science Foundation of Huai'an (Grant No.HAB201837), the Electric Power Company Technology Project of Jiangsu Province (Grant No.J2017123), the Natural Science Foundation of Jiangsu Province (Grant No.BK20161302), the National Key R & D Program of China (No. 2018YFB1004904), the Huai'an Science and Technology Project (No. HAC201705, No.HAB201803), the Key Project of JiangSu Provincial Department of Education (No.18KJA520001), the Six Talent Peaks Project in Jiangsu Province (XYDXXJS-011), and the Jiangsu 333 Engineering Research Funding Project (BRA2016454)..

References

[1] Y. Aumann and M. Rabin, "Authentication, enhanced security and error correcting codes," *in Proc. of 20th Annual International Cryptology Conference, CRYPTO 1998*, pp. 299-303, August 23-27, 1998. Article (CrossRef Link).

[2] C. Dwork, M. Naor and A. Sahai, "Concurrent zero-knowledge," in *Proc. of the Thirtieth Annual ACM Symposium on the Theory of Computing Symposium on Theory of Computing (STOC'98)*, pp. 409-418, May 23-26, 1998. Article (CrossRef Link).

[3] Y. Chen and J. Chou, "ECC-Based Non-Interactive Deniable Authentication with Designated Verifier," *IACR Cryptology ePrint Archive*, pp. 783, 2013. Article (CrossRef Link).

[4] F. Li, P. Xiong and C. Jin, "Identity-Based Deniable Authentication for Ad Hoc Networks," *Computing*, vol. 96, no. 9, pp. 843-853, September, 2014. Article (CrossRef Link).
[5] S. Gambs, C. Onete and J. Robert, "Prover anonymous and deniable distance-bounding authentication," in *Proc. of the 9th ACM symposium on Information, computer and communications security*, pp. 501-506, June 4-6, 2014. Article (CrossRef Link).
[6] W. Shi, J. Zhang, Y. Zhou and Y. Yang, "A novel quantum deniable authentication protocol without entanglement," *Quantum Information Processing*, vol.14, no.6, pp. 2183-2193, January, 2015. Article (CrossRef Link).
[7] T. Dimitriou and N. Al-Ibrahim, "Denying Your Whereabouts: A Secure and Deniable Scheme for Location-Based Services," *in Proc. of Cryptology and Network Security- 15th International Conference*, pp. 713-718, November 14-16, 2016. Article (CrossRef Link).
[8] S. Mandal, S. Mohanty, and B. Majhi, "An ID-based Non-Interactive Deniable Authentication Protocol based on ECC," *in Proc. of the 2017 the 7th International Conference on Communication and Network Security*, pp. 48-52, November 24-26, 2017. Article (CrossRef Link).
[9] X. Hong and B. Wang, "A non-interactive deniable authentication scheme in the standard model," *Journal of Electrical and Electronic Engineering*, vol. 5, no. 2, pp. 80, December, 2017. Article (CrossRef Link).
[10] S. Zeng, Y. Chen, S. Tan and M. He, "Concurrently deniable ring authentication and its application to LBS in VANETs," *Peer-to-Peer Networking and Applications*, vol.10, no.4, pp. 844-856, January, 2017. Article (CrossRef Link).
[11] S. Zeng, Y. Mu, G. Yang and M. He, "Deniable Ring Authentication Based on Projective Hash Functions," *in proc. of Provable Security- 11th International Conference, ProvSec 2017*, pp. 127-143, October 23-25,2017. Article (CrossRef Link).
[12] F. Li, J. Hong and A. Omala, "Practical deniable authentication for pervasive computing environments," *Wireless Networks*, vol.24, no.1, pp. 139-149, January, 2018. Article (CrossRef Link).
[13] L. Harn and J. Ren, "Design of fully deniable authentication service for e-mail applications," *Communications Letters*, vol.12, no.3, pp. 219-221, January, 2008. Article (CrossRef Link).
[14] R. Lu, X. Lin, Z. Cao, L. Qin and X. Liang, " A simple deniable authentication protocol based on the Diffie-Hellman algorithm," *International Journal of Computer Mathematics*, vol.85, no.9, pp. 1315-1323, 2008. Article (CrossRef Link).
[15] E. Yoon, K. Yoo, S. Yeo and S. Lee, "Robust deniable authentication protocol," *Wireless personal communications*, vol. 55, no. 1, pp. 81-90, September, 2010. Article (CrossRef Link).
[16] F. Li and T. Takagi, "Cryptanalysis and Improvement of Robust Deniable Authentication Protocol," *Wireless personal communications*, vol. 69, no.4, pp. 1391-1398, January, 2013. Article (CrossRef Link).
[17] S. Hwang and Y. Sung, "Confidential deniable authentication using promised signcryption," *Journal of Systems and Software*, vol. 84, no. 10, pp. 1652-1659, January, 2011. Article (CrossRef Link).
[18] L. Harn, C. Lee, C. Lin, and C. Chang, "Fully deniable message authentication protocols preserving confidentiality," *The Computer Journal*, vol. 54, no. 10, pp. 1688-1699, January, 2011. Article (CrossRef Link).
[19] S. Hwang, Y. Sung and J. Chi, "Deniable Authentication Protocols with Confidentiality and Anonymous Fair Protections," *in Proc. of the International Computer Symposium ICS 2012*, pp. 41-51, December 12-14, 2013. Article (CrossRef Link).
[20] F. Li, D. Zhong and T. Takagi, "Efficient Deniably Authenticated Encryption and Its Application to E-Mail," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2477-2486, November, 2016. Article (CrossRef Link).
[21] W. Wu and F. Li, "An Efficient Identity-Based Deniable Authenticated Encryption Scheme," *KSII Transactions on Internet and Information Systems* (*TIIS*), vol. 9, no. 5, pp. 1904-1919, January, 2015. Article (CrossRef Link).

[22] F. Li, Z. Zheng and C. Jin, "Identity-based deniable authenticated encryption and its application to e-mail system," *Telecommunication Systems*, vol. 62, no. 4, pp. 625-639, May, 2016. Article (CrossRef Link).
[23] C. Jin and J. Zhao, "Efficient and Short Identity-Based Deniable Authenticated Encryption," in proc. of *International Conference on Cloud Computing and Security*, pp. 244-255, June 17-18, 2017. Article (CrossRef Link).
[24] C. Jin, G. Chen, C. Yu and J. Zhao, "Deniable authenticated encryption for e-mail applications," *International Journal of Computers and Applications*, pp.1-10, May, 2018. Article (CrossRef Link).
[25] N. Unger and I. Goldberg, "Improved Strongly Deniable Authenticated Key Exchanges for Secure Messaging," in *Proc. of Privacy Enhancing Technologies*, 2018, pp.21-66,July 24-27, 2018. Article (CrossRef Link).
[26] E. Ahene, C. Jin and F. Li, "Certificateless deniably authenticated encryption and its application to e-voting system," *Telecommunication Systems*, pp. 1-18, 2018. Article (CrossRef Link).
[27] C. Jin and J. Zhao, "Certificateless aggregate deniable authentication protocol for ad hoc networks," *International Journal of Electronic Security and Digital Forensics*, vol. 10, no. 2, pp. 168-187, 2018. Article (CrossRef Link).
[28] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost(encryption)," in *Proc. of Cryptology-CRYPTO'97,17th Annual International Cryptology Conference*, pp. 165-179, August 17-21, 1997. Article (CrossRef Link).
[29] J. Cha and J. Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Proc. of Public Key Cryptography- PKC 2003, sixth International Workshop on Theory and Practice in Public Key Cryptography*, pp. 18-30, January 6-8, 2003. Article (CrossRef Link).
[30] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. of Cryptology- CRYPTO 2001, 21st Annual International Cryptology Conference*, pp. 213-229, August 19-23, 2001. Article (CrossRef Link).
[31] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptography*, vol. 13, no. 3, pp. 61-396, 2003. Article (CrossRef Link).

Chunhua Jin received a B.S. degree from Northwestern Polytechnical University, Xi'an, P.R. China in 2007, an M.S. degree from Xidian University, Xi'an, P.R. China in 2011, and a Ph.D. degree in Cryptography from the University of Electronic Science and Technology of China, Chengdu, P.R. China in 2016. She is now a lecturer in the Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, P.R. China. Her recent research interests include cryptography and network security.

Guanhua Chen received a B.S. degree from Xi'an University of Technology, Xi'an, P.R. China in 2006. He is now a graduate student in the Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, P.R. China. His recent research interests include cryptography and network security.

Jianyang Zhao received an Ms.D. degree in power electronic engineering and a Ph.D. degree in test measurement techniques and instruments from the Nanjing University of Aeronautics and Astronautics. His current research interests are power quality monitoring and analysis, transient analysis, and power system equipment modeling and diagnoses.

Shangbing Gao received a BS degree in mathematics from the Northwestern Polytechnical University in 2003, a MS degree in applied mathematics from the Nanjing University of Information and Science and Technology in 2006, and a Ph.D. degree with the School of Computer Science and Technology, Nanjing University of Science and Technology (NUST). Since 2014, he has been an associate professor at Huaiyin Institute of Technology, China. His current research interests include pattern recognition and computer vision

Changhui Yu received a B.S. degree from Liaoning Normal University, Dalian, P.R. China in 1996, and an M.S. degree from Southeast University, Nanjing, P.R. China in 2009. She is now a teacher in the Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, P.R. China. Her recent research interests include cryptography and network security.