Secure and Efficient Identity-based Batch Verification Signature Scheme for ADS-B System

Jing-xian Zhou[1, 2,*] Jian-hua Yan[3]
[1] Information Security Evaluation Center, Civil Aviation University of China
Tianjin 300300, P.R. China
[2] Information Technology Research Base of Civil Aviation Administration of China
Civil Aviation University of China, Tianjin 300300, P.R. China
[e-mail: yzzxtj@aliyun.com]
*Corresponding author: Jingxian Zhou
[3] School of Information and Electric Engineering, Ludong University, Yantai 264025, P.R. China

Received 28 June, 2018; revised October 18, 2018; revised Decebmer 19, 2018; revised Feburay 7, 2019; revised May 22, 2019; accepted July 18, 2019; published December 31, 2019

Abstract

As a foundation of next-generation air transportation systems, automatic dependent surveillance–broadcast (ADS-B) helps pilots and air traffic controllers create a safer and more efficient national airspace system. Owing to the open communication environment, it is easy to insert fake aircraft into the system via spoofing or the insertion of false messages. Efforts have thus been made in academic research and practice in the aviation industry to ensure the security of transmission of messages of the ADS-B system. An identity-based batch verification (IBV) scheme was recently proposed to enhance the security and efficiency of the ADS-B system, but current IBV schemes are often too resource intensive because of the application of complex hash-to-point operations or bilinear pairing operations. In this paper, we propose a lightweight IBV signature scheme for the ADS-B system that is robust against adaptive chosen message attacks in the random oracle model, and ensures the security of batch message verification and against the replaying attack. The proposed IBV scheme needs only a small and constant number of point multiplication and point addition computations instead of hash-to-point or pairing operations. Detailed performance analyses were conducted to show that the proposed IBV scheme has clear advantages over prevalent schemes in terms of computational cost and transmission overhead.

Keywords: ADS-B, identity-based signature, batch verification, efficient, pairing free.

This work is partially supported by the National Natural Science Foundation of China (Nos. 61601467, U1833107), the Natural Science Foundation of Shandong Provience (Nos. ZR201702180067), the Project of Civil aviation safety capacity (Nos. PESA2019074, PESA2018082), the science research foundation of CAUC (Nos. 2013QD24X).

1. Introduction

Civil aviation systems are continually being modernized through advanced technologies. Automatic dependent surveillance–broadcast (ADS-B) is one of the most important technologies in aviation systems. Aircraft can periodically broadcast information about themselves through ADS-B systems, such as location and identification information. Two types of information are broadcast. Information broadcasted by a subsystem to other aircraft and ground stations is called *ADS-B Out*, whereas that processed by the subsystem from the ADS-B of other aircraft is called *ADS-B In* [1]. Both subsystems combine to create situational awareness, which provides pilots with complete knowledge of the scenario and helps them make decisions. This makes air traffic management much easier.

ADS-B systems have been deployed widely across the globe, and are expected to replace radars and become the mainstay of air traffic management systems. In recent years, international organizations have made strenuous efforts to standardize ADS-B. ADS-B systems will be operational in most airspaces by 2020 to support next-generation air transportation systems. For instance, the Federal Aviation Administration requires that aircraft in the US be prepared for ADS-B by 2020 [2], and China's civil aviation plans to implement a fully operational ADS-B system on July 1, 2019 [3].

From the perspective of security, messages in the ADS-B system are transmitted through wireless channels without being encrypted [4]. Therefore, adversaries can mount a series of attacks by intercepting, modifying, injecting, and replaying a message at will. A large number of attacks against ADS-B systems have featured the use of low-cost and simple tools (e.g., aircraft spoofing attacks) in recent years [5]. These attacks can cause significant damage, such as hijacking an aircraft. Thus, it is important to address security risks in ADS-B systems to ensure aviation safety.

Message authenticity and integrity need to be solved for first in ADS-B applications. Message integrity means that the information has not been falsified and message authenticity means that the messages were broadcasted by the indicated aircraft. They can prevent adversaries from falsifying or implanting messages to attack the system—for example, through spoofing attacks and virtual trajectory modification attacks [6]. Several studies have been conducted on ensuring ADS-B messages' authenticity and integrity. Methods of implementing secure authentication in the ADS-B system can be roughly divided into non-cryptographic approaches [7], [8] and cryptographic approaches [9], [10]. In this paper, cryptographic approaches are considered in detail.

Although these approaches can address some security problems in ADS-B systems, the relevant schemes suffer from weaknesses. First, complex computation operations are used to guarantee security, such as the hash-to-point operation [10], bilinear pairing operation [6], and expensive certification management [10]. When signatures arrive frequently, the recipient does not have enough time to verify each received signature, especially where the verification of the signature scheme involves costly pairing operations. This can be avoided by using pairing to enhance efficiency. Second, in some studies on the IBV scheme, the security of the protocol itself has not been fully considered. For example, in the security problem in Yang's YKLY scheme [6], some signatures cannot pass signatures verification separately but can pass batch verification by themselves.

The main contributions of this study are as follows: First, an IBV signature scheme is proposed to guarantee the security of ADS-B messages, and it is shown to be provably secure. Second, compared with previously proposed schemes in the area, the computational cost of the

verification algorithm in the proposed signature scheme is reduced by half as it uses fewer point multiplication calculations.

The remainder of this paper is organized as follows: The status of research in the area is described in Section 2. Some preliminaries were introduced in Section 3. In Section 4, we explain the nomenclature used in this paper, and the proposed IBV signature scheme is described in detail in Section 5. The security analysis and calculation evaluation are given in Sections 6 and 7, respectively. In Section 8, we state the conclusions of the paper.

2. Related Work

By using cryptographic approaches, a number of achievements to guarantee the security of ADS-B messages [6], [9], [10], [11]. They can be divided into two types: symmetric key-based authentication methods, like Message Authentication Code (MAC), and asymmetric key-based authentication solutions, such as digital certificate. Important studies in the area as follows: Samuelson et al. [12] considered a method that uses the MAC. Pan et al. [11] offered an encryption algorithm that uses elliptic curve cryptography as a public key. Baek et al. proposed a staged identity-based encryption (SIBE) method that can solve the confidentiality of ADS-B [4]. SIBE provides high efficiency by classifying “key encryption” and “data encryption.” But these methods are impractical because every aircraft should pre-load the same key [13].

Digital signatures are a good means of optimizing symmetric cryptography, but some requirements need to be met when using ADS-B. The signatures should be short as the payload of the ADS-B message is usually no more than 1000 bits. Signatures should be verified quickly as each aircraft broadcasts and receives a large number of ADS-B messages from surrounding aircraft. A number of identity-based batch verification (IBV) signatures have been proposed to address these challenges. Yang et al. [6] proposed an IBV signature method for ADS-B systems, but it is unsecure because some signatures cannot pass single signature verification but can pass batch verification. Anjia Yang et al. [10] defined three levels of the ADS-B system and proposed two identity-based signature (YTBW1 and YTBW2) schemes accordingly. He et al. [9] described three weaknesses of the YTBW1 and YTBW2 schemes. First, the performance of YTBW1 is impractical as the hash-to-point operations increase in number when the number of signatures increases. Second, the YTBW1 scheme supports only partial batch verification. Third, the YTBW2 scheme is impractical as it demands an authority to ensure identities and public keys. He et al. concluded that neither the YTBW1 nor the YTBW2 scheme can be used in ADS-B systems, and offered an improved scheme (HKCW) to enforce security.

Recently, the IBV protocol was put forward to ensure vehicular ad-hoc networks (VANETs) more secure and efficient. Zhang et al. [14], [15] developed an IBV method (ZLLHS-IBV) for VANET communication using an identity-based one-time signature to eliminate the use of certificates for public keys. Lee and Lai [16] found two weaknesses in the ZLLHS-IBV [15] scheme: It is not secure against replaying attack, and it can’t provide non-repudiation. For these two weaknesses, an improved method [16] was proposed to improve security and maintain the efficiency of ZLLHS-IBV. Recently, Tzeng et al. noted that the improved scheme [16] suffers from the infringement of privacy and forgery attacks [17]. They introduced a new modified proposal to meet the demands of security wanted in vehicles.

However, ZLLHS-IBV schemes and the HKCW scheme require bilinear pairing operations. In modern cryptography, they are the costliest calculation. Our proposed IBV signature avoids

bilinear pairing, which reduces the cost of calculation. It can thus be deployed in ADS-B systems.

3. Preliminaries

In this section, we describe the ADS-B system model, threat model, and design goals.

3.1 ADS-B System Model

As shown in **Fig. 1**, each aircraft comes fitted with a global positioning system (GPS) as the primary source of information for navigation. The aircraft flies according to messages from other aircraft and the ADS-B ground stations. Moreover, it broadcasts traffic beacons by using the *ADS-B Out* capability once or twice per second. ADS-B data link standards include the universal access transceiver (UAT) and 1090 MHz Extended Squitters (1090 ES) [18, 19]. As the 1090 ES is highly congested owing to its current use by the air traffic control radar beacon system [20], this paper considers only the authentication of ADS-B messages in the UAT data link. Each aircraft also has a universally unique permanent identifier that can be considered its unique identity in the identity-based setting of our broadcast message signature scheme.

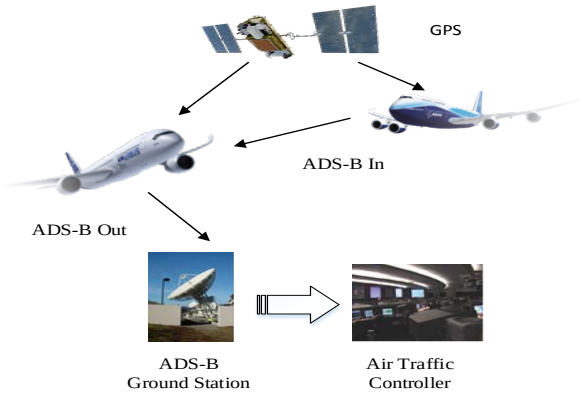

Fig. 1. System model

3.2 ADS-B System Threat Model

As the ADS-B data link is a broadcast-type shared link and messages are broadcast in the form of plaintext, they are vulnerable to attacks. In [21], the authors claimed that ADS-B can easily suffer from cyberattacks, such as message injection, modification, and deletion, ranging from comparatively easy discontinues using interference device to the more harder target ghost inject to denial of service. Costin et al. [22] showed that both active and passive attacks are practical in ADS-B. Tampering information can be realized by bit-flipping and overshadowing [23].

This paper focuses on ensuring the authenticity of ADS-B information. We thus assume only that the adversary can carry out active attacks, by spoofing false target aircraft or destroying transfer data for example. Passive eavesdropping and recording broadcasts are not considered here. Jamming threats that do not influence the authenticity of the message are studied.

3.3 Design Goals

To ensure the authentication of the broadcasted information in ADS-B system, the following

features are needed.

- Authenticity and integrity: To solve such a problem as the insertion of fake targets or damage to traffic data [5], ADS-B broadcast messages should be authentic and complete. For example, messages should be transmitted by legitimate aircrafts that have the ADS-B system such that they have not been counterfeited or tampered.
- Scalability: It becomes increasingly challenging to administer the ADS-B system because of the increase in the number of aircraft. Thus, the IBV signature scheme requires a reasonable interaction mechanism that can easily increase or reduce the number of aircraft.
- Low cost of communication: The cost of communication should be low because the data space of *ADS-B Out* is finite in the UAT data link.
- Low cost of computation: The computational cost should be low because participants are usually avionics devices with limited resources.

3.4 Security Requirements

It is essential to guarantee the safety and privacy of ADS-B systems. A safe signature should meet the following demands:

1) *Message authentication*. Ground stations and aircraft should be capable of confirming that the message has been transmitted by a legitimate aircraft, and has not been tampered with or counterfeited by an attacker.

2) *Non-repudiation.* A spiteful aircraft cannot to broadcast messages to misguide ground stations or other aircraft and deny behaviors when the ATC traces it by its digital signatures.

3) *Replaying resistance*. A spiteful aircraft cannot collect and store a signed message, and attempt to deliver it at a later time when the original message is invalid.

4. Definitions

4.1 System Notations

This subsection introduces the notations used in this paper (**Table 1**). Note in particular that all arithmetic operations in this paper are based on the modular operation of finite fields F_q.

Table 1. Notations

Notation	Description
k	Security parameter
$RPKC$	Root private key center; it is the air traffic controller to set-up all parameters
G	Cyclic group
P	Generator of group G
$H_i : \{0,1\}^* \to Z_q^*, (i = 1,3)$	Hash functions [24]
$H_2 : G \to \{0,1\}^*$	Cryptographic one-way hash function
T	Timestamp
ΔT	The predefined endurable transmission delay
$\|\|$	Concatenation operator

4.2 Harness Problem

The security of our signature protocol is based on the elliptic curve discrete logarithm problem (ECDLP):

Definition 1. ECDLP: Let G be an elliptic curve of order q. P be a generator of group G. For element $E \in G$, the problem of ECDL is to compute $e \in Z_q^*$ to cause the equation $E = eP \mod q$ to hold.

4.3 Bilinear Map

Let and G_2 be cyclic groups of prime order q. Let P denote a generator of group G_1. e: $G_1 \times G_1 \to G_2$ is a bilinear map when the three conditions hold listed below:

- Bilinearity: $e(xM, yN) = e(M, N)^{xy}$ for all $M, N \in G_1$ and $x, y \in Z_q^*$.
- Non-degeneracy: $e(P, P) \neq 1$.
- Computability: For all $M, N \in G_1$, $e(M, N)$ can be computed efficiently.

4.4 The IBV Signature Scheme Framework

The IBV signature scheme contains the following five algorithms: *System initialization, Registration, Sign, Verify,* and *BVerify*.

- *System initialization*: This algorithm takes as input a security parameter k to generate the master secret key s and the public parameters $params$.
- *Registration*: Let ID_{AL} be airline AL's identity and ID_{AC} be aircraft AC's identity. This algorithm inputs ID_{AL}, ID_{AC}, s, and $params$ to generate AC's private key sk_{AC} and its public key PK_{AC}.
- *Sign*: Let sk_{AC} be AC's private key. This algorithm takes as inputs message m, sk_{AC}, and $params$ to generate a signature σ.
- *Verify*: This algorithm takes as inputs message m, signature σ, AC identity ID_{AC}, AC public key PK_{AC}, and $params$ to determine whether σ is legitimate.
- *BVerify*: This algorithm takes as inputs a group of messages $\{m_1, m_2, \cdots, m_n\}$, group of digital signatures $\{\sigma_{m_1}, \sigma_{m_2}, \cdots, \sigma_{m_n}\}$, group of identities $\{ID_{AC_1}, ID_{AC_2}, \cdots, ID_{AC_n}\}$, group of public keys $\{PK_{AC_1}, PK_{AC_2}, \cdots, PK_{AC_n}\}$, and $params$ to simultaneously determine whether $\{\sigma_{m_1}, \sigma_{m_2}, \cdots, \sigma_{m_n}\}$ are legitimate.

5. Proposed ADS-B Signature Scheme

5.1 Scheme Description

The scheme contains the following five algorithms: *system initialization, registration, sign, signature verification,* and *batch verification.*

(1) *System initialization*

In this phase, air traffic controllers act as $RPKC$ to set-up all parameters as follows:

1) Choose a large prime number q and a cyclic groups G of order q randomly.

2) P is a generator of G chosen at random.

3) Randomly pick an element $s \in Z_q^*$ and compute $P_{pub} = sP$.

4) Select three hash functions $H_i : \{0,1\}^* \to Z_q^* (i = 1,3)$, $H_2 : G \to \{0,1\}^*$, publish $params = \{q, G, P, P_{pub}, H_2, H_3\}$, and keep s, H_1 secret.

(2) *Registration*

In this phase, $RPKC$ generates an identity ID_{AL} for each airline, and an identity ID_{AC} and a secret key sk_{AC} for each aircraft.

1) Generate identity ID_{AL} for each airline.

2) Generate identity ID_{AC} for each aircraft.

3) Compute $sk_{AC} = sH_1(ID_{AL} \| ID_{AC} \| s)$, $PK_{AC} = H_1(ID_{AL} \| ID_{AC} \| s)^{-1} P$.

(3) *Sign*

In this phase, AC generates a signature for message m.

1) Generate current time stamp T.

2) Randomly produce $r_m \in Z_q^*$ and compute $R_m = r_m PK_{AC}$, $\alpha_m = ID_{AC} \oplus H_2(sk_{AC} P_{pub})$ and $S_m = r_m + sk_{AC} H_3(R_m \| m \| \alpha_m \| T)$.

3) Output a signature $\sigma = \{R_m, \alpha_m, S_m, T\}$ on message m.

Finally, AC broadcasts signature $\{R_m, \alpha_m, S_m, T\}$ through the ADS-B data link to the ground stations and neighboring aircraft.

(4) *Signature verification*

Upon the receipt of signature $\sigma_m = \{R_m, \alpha_m, S_m, T\}$ of message m from broadcaster AC, each recipient verifies it as follows:

1) Let the receipt time be ; the verifier computes $\Delta T \geq T_v - T$ to determine whether it is correct. If it is correct, go to step 2; otherwise, reject the message.

2) If

$$S_m PK_{AC} = R_m + H_3(R_m \| m \| \alpha_m \| T) P_{pub} \tag{1}$$

holds, output 1; otherwise, output 0.

(5) *Batch verification*

When a recipient receives ADS-B broadcast messages from different aircraft at the same time, it can verify the signatures of the messages in a batch-wise manner. Assume that the verifier receives l signatures $\sigma_{m_i} = \{R_{m_i}, \alpha_{m_i}, S_{m_i}, T_{m_i}\}_{i=1}^{l}$ concerning messages $\{m_i\}_{i=1}^{l}$.

1) Let the time of receipt be T_v . The verifier determines whether $\Delta T \geq T_v - T_{m_i}$ ($1 \leq i \leq l$) is correct. If it is correct, the verifier goes to the next step. Otherwise, it rejects the signature.

2) Pick a group of numbers $\{t_1, t_2, \cdots, t_l\}$ with a small number of bits l_s (e.g., 80).

3) If the following equation

$$\sum_{i=1}^{l} t_i S_{m_i} PK_{AC_i} = \sum_{i=1}^{l} t_i R_{m_i} + \sum_{i=1}^{l} t_i H_3 \left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i} \right) P_{pub} \tag{2}$$

holds, output 1; otherwise, output 0.

Note: Note that a spiteful verifier can choose t_i=1. This contributes to a BVerify vulnerability, also called the false acceptance problem, and has been described in [25]. We thus assume that the verifier is honest in the proposed scheme.

5.2 Correctness of Verification and Batch Verification

The correctness of verification and batch verification can be illustrated in the following two theorems, respectively:

Theorem 1: Verification of the broadcasted message is correct.

Proof: The correctness of the verification in Eq. (1) is justified as below. For simplicity, we denote $H_1 \left(ID_{AL} \| ID_{AC} \| s \right)^{-1} P$ by PK_{AC}.

We have

$$\begin{aligned}
S_m PK_{AC} &= \left(r_m + sk_{AC} H_3 \left(R_m \| m \| \alpha_m \| T \right) \right) PK_{AC} \\
&= r_m PK_{AC} + sk_{AC} H_3 \left(R_m \| m \| \alpha_m \| T \right) PK_{AC} \\
&= R_m + sH_1 \left(ID_{AL} \| ID_{AC} \| s \right) H_3 \left(R_m \| m \| \alpha_m \| T \right) PK_{AC} \\
&= R_m + sH_1 \left(ID_{AL} \| ID_{AC} \| s \right) H_3 \left(R_m \| m \| \alpha_m \| T \right) H_1 \left(ID_{AL} \| ID_{AC} \| s \right)^{-1} P \\
&= R_m + H_3 \left(R_m \| m \| \alpha_m \| T \right) sP \\
&= R_m + H_3 \left(R_m \| m \| \alpha_m \| T \right) P_{pub}
\end{aligned}$$

Theorem 2: Batch verification for the broadcasted message is correct.

Proof: The correctness of the batch verification in Eq. (2) is justified as follows:

$$\begin{aligned}
\sum_{i=1}^{l} t_i S_{m_i} PK_{AC_i} &= \sum_{i=1}^{l} t_i \left(r_{m_i} + sk_{AC_i} H_3 \left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i} \right) \right) PK_{AC_i} \\
&= \sum_{i=1}^{l} t_i \left(r_{m_i} PK_{AC_i} + sk_{AC_i} H_3 \left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i} \right) PK_{AC_i} \right) \\
&= \sum_{i=1}^{l} t_i r_{m_i} PK_{AC_i} + \sum_{i=1}^{l} t_i sk_{AC_i} H_3 \left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i} \right) PK_{AC_i} \\
= \sum_{i=1}^{l} t_i R_{m_i} &+ \sum_{i=1}^{l} t_i H_3 \left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i} \right) sk_{AC_i} PK_{AC_i}
\end{aligned}$$

$$= \sum_{i=1}^{l} t_i R_{m_i} + \sum_{i=1}^{l} t_i H_3\left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i}\right) s H_1\left(ID_{AL} \| ID_{AC} \| s\right) H_1\left(ID_{AL} \| ID_{AC} \| s\right)^{-1} P$$

$$= \sum_{i=1}^{l} t_i R_{m_i} + \sum_{i=1}^{l} t_i H_3\left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i}\right) s H_1\left(ID_{AL} \| ID_{AC} \| s\right) H_1\left(ID_{AL} \| ID_{AC} \| s\right)^{-1} P$$

$$= \sum_{i=1}^{l} t_i R_{m_i} + \sum_{i=1}^{l} t_i H_3\left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i}\right) sP$$

$$= \sum_{i=1}^{l} t_i R_{m_i} + \sum_{i=1}^{l} t_i H_3\left(R_{m_i} \| m_i \| \alpha_{m_i} \| T_{m_i}\right) P_{pub}$$

5.3 Discussion

5.3.1 Replay attack

Eavesdroppers can block and resend both information and their signatures. To deal with the replay attack, this method utilizes the current timestamp T to get the signature, and makes sure that the ground station and the aircraft receive the latest messages. In this way, even if the attackers have monitored the signatures, they still cannot counterfeit the new signatures.

5.3.2 Identification of invalid signatures

The ADS-B receiver can obtain a large amount of ADS-B information and signatures transmitted by aircraft or stations. If a message has an invalid signature, there is no need to determine the information as new information with a valid signature will arrive shortly (information on position and speed are included, and these values change a little from previously reported ones, which can thus be ignored). However, a large number of invalid signatures means a high likelihood of being attacked. To identify false signatures, a recursive divide-and-conquer method is feasible. In particular, when verification fails, the signatures can be separated into two parts and verified again. If a group of the signatures is verified as valid by the algorithm, we can be sure that the false signatures are in the other part. This process can be repeated until the false signatures have been found [10].

6. Security Analysis

In this section, we give a formal proof of the security of the proposed IBV signature scheme.

6.1 Security Model

An IBV signature scheme should be secure against existential forgery under an adaptively chosen message attack in the random oracle model. For a formal definition of existential unforgeability, an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$ should interact through a game. The game consists of three phases as follows:

Setup phase. $\mathcal{B}$ executes an initialization algorithm to generate the master secret key and the public parameters $params$, and returns $params$ to $\mathcal{A}$.

Oracle simulation phase. $\mathcal{A}$ adaptively issues H_2 oracle, H_3 oracle, and a sign oracle. $\mathcal{B}$ provides respective responses as follows:

H_2-oracle: After receiving AC's identity ID_{AC}, $\mathcal{B}$ selects an element $r \in \{0,1\}^*$ randomly. It then sends r to $\mathcal{A}$ and stores $\left(P_{pub}, ID_{AC}, r\right)$ in the list H_2^{list}.

H_3-oracle: After receiving a signature $\left(R_m, m, \alpha_m, T\right)$, $\mathcal{B}$ selects an element $t \in Z_q^*$, randomly. It sends t to $\mathcal{A}$ and stores $\left(R_m, m, \alpha_m, T, t\right)$ in the list H_3^{list}.

Signing query. After receiving message m and ID_{AC}, $\mathcal{B}$ generates a signature σ for message m, and sends σ to $\mathcal{A}$.

Output phase. In this phase, $\mathcal{A}$ forges message m^*'s signature σ^* corresponding to ID_{AC} and a current time stamp T^*.

We say that $\mathcal{A}$ wins in the above game if $Verify\left(m^*, ID_{AC^*}, T^*, \sigma^*\right) = 1$ holds.

Definition 2. We say that an IBV signature scheme is existentially unforgeable against a selective chosen message attack in the random oracle model if there is no polynomial-time adversary $\mathcal{A}$ that can win the above game with a non-negligible advantage.

6.2 Proof of Security

Theorem 3: The proposed IBV signature scheme is provably secure against forgeability attacks in the random oracle model if the ECDL problem is hard.

Proof: Assuming that $\mathcal{A}$ is an adversary, we build an adversary $\mathcal{B}$ to solve the ECDLP. $\mathcal{B}$ takes an ECDLP challenge $\left(P, xP\right)$ for $x \in Z_q^*$ and $P \in G$. To use $\mathcal{A}$ to solve x, $\mathcal{B}$ needs to simulate the oracles and a challenger for $\mathcal{A}$. $\mathcal{B}$ runs $\mathcal{A}$ by carrying out the steps below.

Setup: $\mathcal{B}$ sets common parameters $params = \left\{q, G, P, P_{pub}, H_2, H_3\right\}$, where H_2, H_3 are random oracles controlled by $\mathcal{A}$, and transmits them to the attacker. Note that the master key is the value of s, which is unknown to algorithm $\mathcal{B}$.

Oracle simulation: $\mathcal{B}$ simulates the oracles as follows:

H_2-oracle: Suppose $\mathcal{A}$ does not know how to compute the hash function $H_2(\cdot)$. $\mathcal{B}$ maintains a list H_2^{list} to respond to H_2 queries, where H_2^{list} is originally empty. $\mathcal{B}$ returns the query made by $\mathcal{A}$ makes with message $\left(P_{pub}, ID_{AC_i}\right)$, as follows: When the query $\left(P_{pub}, ID_{AC_i}\right)$ appears in H_2^{list} already in a tuple $\left(P_{pub}, ID_{AC_i}, H_{2_i}\right)$, $\mathcal{B}$ outputs H_{2_i} to $\mathcal{A}$ immediately. If not, it outputs a random value $H_{2_i} \in Z_q^*$ to $\mathcal{A}$, and inserts a new tuple $\left(P_{pub}, ID_{AC_i}, H_{2_i}\right)$ into H_2^{list}.

H_3-oracle: Suppose A does not know how to compute the hash function $H_3(\cdot)$. $\mathcal{B}$ maintains a list H_3^{list} to respond to H_3 queries, where H_3^{list} is originally empty. When $\mathcal{A}$ makes a query through message $\left(R_{m_i}, m_i, \alpha_{m_i}, T_{m_i}\right)$, $\mathcal{B}$ returns it, at which $\mathcal{A}$ queries with message $\left(R_{m_i}, m_i, \alpha_{m_i}, T_{m_i}\right)$ as follows: When the query $\left(R_{m_i}, m_i, \alpha_{m_i}, T_{m_i}\right)$ **is** already in

H_3^{list} in a tuple $\left(R_{m_i}, m_i, \alpha_{m_i}, T_{m_i}, H_{3_i}\right)$, $\mathcal{B}$ outputs H_{3_i} to $\mathcal{A}$ directly. Otherwise, it outputs a random value $H_{3_i} \in Z_q^*$ to $\mathcal{A}$ and inserts a new tuple $\left(R_{m_i}, m_i, \alpha_{m_i}, T_{m_i}, H_{3_i}\right)$ into H_3^{list}.

Sign oracle: When a signing query for a message is received, B can build the signature without the private key. It chooses $S_{m_i}, H_{2_i}, H_{3_i} \in Z_q^*$ at random. Then, it calculates $R_{m_i} = S_{m_i} PK_{AC} - H_{3_i} P_{pub}$. $\left(R_{m_i}, S_{m_i}, \alpha_{m_i}, T_{m_i}\right)$ can be checked to be a valid signature as follows: $S_{m_i} PK_{AC} = R_{m_i} + H_{3_i} P_{pub}$.

If tuple $\left(R_{m_i} = r_{m_i} P, m_i, \alpha_{m_i}, T_{m_i}, H_{3_i}\right)$ already appears in H_3^{list}, $\mathcal{B}$ selects another $S_{m_i}, H_{2_i}, H_{3_i} \in Z_q^*$ and tries again. Then, $\mathcal{B}$ returns $\left(R_{m_i}, S_{m_i}, \alpha_{m_i}, T_{m_i}\right)$ to $\mathcal{A}$ and stores $\left(R_{m_i} = r_{m_i} P, m_i, \alpha_{m_i}, T_{m_i}, H_{3_i}\right)$ in H_3^{list}. It is difficult for the adversary to distinguish all signatures produced by $\mathcal{B}$ from signatures provided by the legitimate aircraft.

Output: By the forking lemma [26], after replaying $\mathcal{A}$ with the same random tape, $\mathcal{B}$ receives two valid signatures $\left(R_{m_i} = r_{m_i} P, S_{m_i}, \alpha_{m_i}, T_{m_i}\right)$ and $\left(R_{m_i}^* = r_{m_i}^* P, S_{m_i}, \alpha_{m_i}, T_{m_i}^*\right)$ in a polynomial time, where

$$S_{m_i} = r_{m_i} + sk_{AC} H_{3_i}$$
$$S_{m_i} = r_{m_i}^* + sk_{AC} H_{3_i}^*$$

Then, $\mathcal{B}$ calculates $sk_{AC} = \left(H_{3_i} - H_{3_i}^*\right)^{-1} \left(r_{m_i}^* - r_{m_i}\right)$. Finally, $\mathcal{B}$ outputs sk_{AC} according to $\left(P_{pub}, PK_{AC} = sk_{AC} P_{pub}\right)$ for $sk_{AC} \in Z_q^*$ and $P_{pub} \in G$, which can solve the ECDLP instance.

We cannot show that $\mathcal{B}$ solves the given instance of the ECDLP to complete the proof because this contradicts the assumption that the ECDLP is difficult. This means that ground stations or other aircraft cannot be cheated by a signature of a message forged by an attacker. Therefore, integrity, message authentication, and non-repudiation are ensured.

Similar to the approach proposed by Camenisch et al. [27], we demonstrate that the new BVerify algorithm is secure by the following theorem:

Theorem 4: The proposed batch verification scheme for the ADS-B system is provably secure in the random oracle model if the ECDL problem is hard.

6.3 Security Comparison

We compare the proposed IBV signature scheme with prevalent schemes, i.e., the YKLY scheme [6], the HKCW scheme [9], and the YTBW2 scheme [10], in terms of the security properties listed in Section 3.4. The YKLY scheme [6] is vulnerable to non-repudiation and forgery attacks as any malicious aircraft or outside attacker can generate two valid signatures for any message. Moreover, the YKLY scheme [6], HKCW scheme [9], and YTBW2 scheme [10] all fail to prevent the replay attack because any malicious attacker can implement reply attacks. The proposed scheme uses the current timestamp to ensure that the ground station and aircraft receive the latest messages and generate the signature to avoid the replay attack.

Table 2. Security comparison

	Proposed scheme	**[6]**	**[9]**	**[10]**
Non-repudiation	yes	no	yes	yes
Avoiding replaying attack	yes	no	no	no
Avoiding forgery attack	yes	no	yes	yes
Batch message verification	yes	yes	yes	yes

Table 2 lists a comparison of the security functions in the ADS-B system. The results show that our scheme is more advantageous than prevalent schemes.

7. Performance Evaluation

As shown in **Fig. 1**, the ADS-B messages broadcasted by an aircraft are received either by ground stations or other aircraft. In general, the ground stations have powerful processing capacity and large storage capability, but aircraft have limited computation power and small storage space owing to the size-related limitation in avionics. Hence, the low computational cost of the signature is important for an aircraft with limited resources. As a result, in the following, the performance evaluation focuses on cases involving aircraft.

We evaluated the proposed signature scheme in terms of computational, verification-related, and communication overhead. In our experiments, we used the Ate pairing $e: G_1 \times G_1 \to G_2$, where G_1 was generated by a point on a super-singular elliptic curve $E(F_P): y^2 = x^3 + 1$ defined on the finite field F_P. The order q was 160 bits and p was 512 bits. We defined the time cost of these operations as follows:

T_{bp}: The time to calculate one pairing operation $e: G_1 \times G_1 \to G_2$.

T_{mtp}: The time to calculate a map-to-point hash function $H: \{0,1\}^* \to G$.

T_{pm}: The time to perform a general point multiplication operation $s.P$, where s is represented by160 bits.

T_{spm}: The time to calculate a short point multiplication operation $s.P$, where s is represented by 80 bits.

T_{pa}: The time to calculate a point addition operation.

T_{exp}: The time to execute an exponentiation operation g^r.

T_{mul}: The time to perform a multiplication operation.

T_h: The time to calculate a general hash operation.

We implemented the above operations on a 3.2 GHz Intel I5-3470 machine for fair comparison [9]. The running results are shown in **Table 3**.

Table 3. Runtimes of related operations (in ms)

Operation	T_{mtp}	T_{bp}	T_{pm}	T_{spm}	T_{pa}	T_{exp}	T_{mul}	T_h	T_{iv}
Runtime	9.773	11.515	3.740	2.089	0.022	0.591	0.003	0.053	2.892

7.1 Computational Cost

We compared the proposed signature scheme with the YKLY scheme [6], HKCW scheme [9], and YTBW2 scheme [10] in computational complexity. **Table 4** shows the operational costs of the four schemes.

In the YKLY scheme, the times needed to generate aircraft AC's private key were $T_h + T_{pm} + T_{iv}$ =0.053 + 3.740 + 2.892 = 6.685 ms , T_{bp} +3× T_{pm} + 2× T_{pa} + T_{exp} +2× T_h = 11.515 + 3×3.740 + 2×0.022 + 0.591 + 2×0.053 =23.476 ms for the signature generation, and T_{bp} + T_{pm} + T_{exp} + T_{pa} + 2× T_h = 11.515 + 3.740 + 0.591 + 0.022 + 2×0.053 = 15.974 ms for verifying the legitimacy of the signature. To verify n signatures $\sigma_i = \{ID_i, m_i, r_i, S_i\}_{i=1}^{n}$ from the batch verification equation, the verifier in the YKLY scheme needed to calculate $2T_{bp}$, nT_{pm} , nT_{mul} , $(2n-2)T_{pa}$, $2nT_h$ and T_{exp} . Hence, the verifier's runtime was 3.893 n +23.577 ms (=2 × T_{bp} + n × T_{pm} + n × T_{mul} + $(2n-2)\times T_{pa}$ + $2n\times T_h$ + T_{exp} = 2×11.515 + n ×3.740 + n ×0.003 + $(2n-2)$ ×0.022 + $2n$ ×0.053 + 0.591).

In the YTBW2 scheme, the times needed to generate airline AL's private key were $T_{mpt} + T_{pm}$ = 9.773+3.740 =13.513 ms, 2× T_{mpt} +3× T_{pm} + T_{pa} = 2×9.773+3×3.740+0.022 = 30.788 ms for aircraft AC's private key, 2× T_{sm} + T_{pa} + T_h = 2×3.740+0.022+0.053 =7.555 ms for the signature generation, and 3 × T_{bp} + T_{pm} + T_{pa} + T_h = 3 × 11.515 + 3.740 + 0.022 +0.053 = 38.360 ms for verifying the legitimacy of the signature. To verify n signatures $\sigma_{m_i} = \{R_{AL}, R_{AC_i}, R_{m_i}, S_{m_i}\}_{i=1}^{n}$ from the batch verification equation, the verifier in the YTBW2 scheme needed to execute $3T_{bp}$, nT_{pm}, $3T_{spm}$, $(4n-3)T_{pa}$ and nT_h. Hence, the verifier's runtime was 10.148 n +34.479 ms (= 3 × T_{bp} + n × T_{pm} + $3n$ × T_{spm} + $(4n-3)\times T_{pa}$ + $n\times T_h$ = 3×11.515 + n ×3.740 + $3n$ ×2.089 + $(4n-3)$ ×0.022 + n ×0.053).

In the HKCW scheme, the needed to generate airline AL's private key was 2 × T_{pm} + T_h = 2 × 3.740 +0.053 = 7.533 ms, 2 × T_{pm} + T_{pa} + T_h = 2 × 3.740 + 0.022 +0.053 = 7.555 ms for generating aircraft AC's private key, 2× T_{pm} + T_{pa} + T_h =2 × 3.740 + 0.022 + 0.053 = 7.555 ms for the signature generation, and 2 × T_{bp} + 3 × T_{pm} + 3 × T_{pa} + 3 × T_h =2 × 11.515 + 3 × 3.740 + 3 × 0.022 + 3 × 0.053 = 34.475 ms for verifying the legitimacy of the signature. To verify n signatures $\sigma_{m_i} = \{R_{AL}, R_{AC_i}, R_{m_i}, S_{m_i}\}_{i=1}^{n}$ simultaneously, the verifier in the HKCW scheme needed to execute $2T_{bp}$, T_{pm}, nT_{mpm}, nT_{pa} and $3nT_h$. Hence, the verifier's runtime was 8.005 n + 26.77 ms (= $2\times T_{bp} + T_{pm} + n\times T_{spm} + n\times T_{mpm} + n\times T_{pa} + 3n\times T_h$ = 2×11.515 + 3.740 + n ×2.089+ n × 5.735 + n × 0.022 + $3n$ × 0.053).

For the proposed IBV signature scheme, the runtimes were 2 × T_h + T_{iv} + T_{pm} + T_{mul} = 2 × 0.053 + 2.892+3.740 +0.003 = 6.741 ms for generating aircraft AC's private key, T_{mul} + T_{pm} + 2× T_h = 0.003 + 3.740 +2 × 0.053 = 3.849 ms for signature generation, and 2 × T_{pm} +

$T_{pa} + T_h = 2 \times 3.740 + 0.022 + 0.053 = 7.555$ ms for verifying the legitimacy of the signature. To verify n signatures $\sigma_{m_i} = \{R_{m_i}, \alpha_{m_i}, S_{m_i}, T_{m_i}\}_{i=1}^{n}$ simultaneously, the verifier in the proposed scheme needed to execute $(n+1)T_{pm}$, $2(n-1)T_{pa}$, nT_{spm}, and nT_h. Hence, the verifier's runtime was $5.926n + 3.696$ ms ($= (n+1) \times T_{pm} + 2(n-1) \times T_{pa} + n \times T_{spm} + n \times T_h$ = （n+1） × 3.740 + （2n-2） × 0.022 + n × 2.089 + n × 0.053).

Table 4. Comparative summary: Computational costs (in ms)

Scheme	*Registration*		*Sign*	*Verify*	*Bverify*
	$Extract^{AL}$	$Extract^{AC}$			
YKLY scheme [6]	6.685		23.476	15.974	$3.893n$ +23.577
HKCW scheme [9]	7.533	7.555	7.555	34.475	8.005.n+26.77
YTBW2 scheme [10]	13.513	30.788	7.555	38.360	10.148.n+34.479
Our scheme	6.741		3.849	7.555	$5.926n$ + 3.696

We compared our proposed IBV signature scheme with those of the YKLY scheme, HKCW scheme, and YTBW2 scheme (see **Table 4**) in terms of the computational cost. Obviously, our signature scheme had lower computation complexity in the *Registration* (*Extract AL*, *Extract AC*), *Sign*, *Verify*, and *BVerify* algorithms than the YKLY, HKCW, and YTBW2 schemes.

In the *Registration* (*Extract AL*, *Extract AC*) algorithm, our IBV signature scheme recorded improvements of 123.82% and 557.19% over the HKCW scheme and the YTBW2 scheme, respectively. On the *Sign* algorithm, the proposed scheme improved by 509.92%, 96.28%, and 96.28% over the YKLY, HKCW, and YTBW2 schemes, respectively.

It is thus clear that our scheme outperformed the YKLY, HKCW, and YTBW2 schemes.

7.2. Transmission Overhead

The transmission cost of the IBV signature method was analyzed and compared with those of the YKLY [6], HKCW [9], and YTBW2 schemes [10]. The transmission overhead was that generated by transmitting data from an aircraft to a ground station, and by communication between aircraft. The evaluation focused on the communication cost of the signature and timestamp but the information was considered. **Table 5** shows the communication costs of all schemes.

Table 5. Comparative summary: Communication costs (in bits)

Scheme	**Communication cost**
YKLY scheme [6]	1536
HKCW scheme [9]	4096
YTBW2 scheme [10]	4096
The proposed scheme	2656

According to the results, p was 512 bits and T was 96 bits. Thus, an element in G was 512+512=1024 bits. The signature produced by the YKLY scheme was $\{r, S\}$, where $S \in G$, $|s| = 512$. Therefore, the transmission cost of the YKLY method was 1024+512=1536 bits. The signature produced by the HKCW method was $\{R_{AL}, R_{AC}, R_m, S_m\}$, where $R_{AL}, R_{AC}, R_m, S_m \in G$. The transmission cost of He et al.'s second method was 1024×4=4096 bits. The signature produced by the YTBW2 scheme was $\{U, V, P, R\}$, where $U, V, P, R \in G$. Hence, the transmission cost of He et al.'s scheme was 1024×4=4096 bits. The signature produced by our method was $\{R_m, \alpha_m, S_m, T\}$, where $R_m, S_m \in G$, $|\alpha_m| = 512$. Hence, the transmission cost of our method was 1024×2+512+96= 2656 bits.

8. Conclusion

In recently developed e-enabled aircraft, advanced network technologies make an important contribution to improving safety and efficiency. The ADS-B system is among the important parts of e-enabled aircraft, and its security is thus important when communicating, especially given that the airspace is now considered cyberspace and aircraft act as intelligent nodes that are vulnerable to cyberattacks.

In this paper, we propose an identity-based batch verification signature scheme of the ADS-B system while dealing with the intractability of the ECDL. A comparative analysis showed that the proposed scheme better than the YKLY scheme [6], HKCW scheme [9], and YTBW2 scheme [10]. Its outstanding security and lightweight computation show that this method can be deployed in the ADS-B. The next step in this research is to evaluate this method in a practical environment, improve it, and design a scheme secure in the post-quantum epoch.

References

[1] S. Meijer, "Secure location verification for ADS-B," *Radboud University, Bachelor's thesis*, 2016. Article (CrossRef Link)

[2] M. Strohmeier, M. Schafer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: The case of ADS-B," *IEEE Communications Society*, vol. 52, no. 5, pp. 111-118, 2014. Article (CrossRef Link)

[3] Civil Aviation Administration of China, "China Civil Aviation ADS-B implementation plan," 2017. Article (CrossRef Link)

[4] J. Baek, E. Hableel, Y. J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to protect ads-b: confidentiality framework and efficient realization based on staged identity-based encryption," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 690-700, 2017. Article (CrossRef Link)

[5] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Proc. of Applied Cryptography and Network Security conference 2013, Lecture Notes in Computer Science*, vol. 7954, pp. 253-271, 2013. Article (CrossRef Link)

[6] H. M. Yang, H. Kim, H. W. Li, E. Yoon, X. F. Wang, and X. F. Ding, "An efficient broadcast authentication scheme with batch verification for ADS-B messages," *KSII Transactions on Internet & Information Systems*, vol. 7, no. 10, pp. 2544-2560, 2013. Article (CrossRef Link)

[7] Y. Kim, J. Y. Jo, and S. Lee, "ADS-B vulnerabilities and a security solution with a timestamp," *IEEE Aerospace & Electronic Systems Magazine*, vol. 32, no. 11, pp. 52-61, 2017. Article (CrossRef Link)
[8] M. Leonardi, E. Piracci, and G. Galati, "ADS-B jamming mitigation: a solution based on a multichannel receiver," *IEEE Aerospace & Electronic Systems Magazine*, vol. 32, no. 11, pp. 44-51, 2017. Article (CrossRef Link)
[9] D. B. He, N. Kumar, K. K. R. Choo, and W. Wu, "Efficient Hierarchical Identity-Based Signature with Batch Verification for Automatic Dependent Surveillance-Broadcast System," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 2, pp. 454-464, 2017. Article (CrossRef Link)
[10] A. J. Yang, X. Tan, J. Baek, and D. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165-175, 2017. Article (CrossRef Link)
[11] W. J. Pan, Z. L. Feng, and Y. Wang, "ADS-B Data Authentication Based on ECC and X.509 Certificate," *Journal of Electronic Science and Technology*, vol. 10, no. 1, pp. 51-55, 2012. Article (CrossRef Link)
[12] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ads-b research," *IEEE Aerospace & Electronic Systems Magazine*, vol. 22, no. 5, pp. 35-38, 2006. Article (CrossRef Link)
[13] K. Sampigethaya, R. Poovendran, S. Shetty, et al., "Future E-Enabled aircraft communications and security: the next 20 years and beyond," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 2040-2055, 2011.Article (CrossRef Link)
[14] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. of 27th IEEE INFOCOM*, pp. 816-824, 2008. Article (CrossRef Link)
[15] C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, 2011. Article (CrossRef Link)
[16] C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441-1449, 2013. Article (CrossRef Link)
[17] S F Tzeng, S J Horng, T Li, et al., "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235-3248, 2017. Article (CrossRef Link)
[18] RTCA DO-282, "Minimum Operational Performance Standards for Universal Access Transceiver (UAT) automatic dependent surveillance - broadcast," 2009. Article (CrossRef Link)
[19] RTCA DO-260A, "Minimum Operational Performance Standard for 1090 MHz Extended Squitter ADS-B and TIS-B," 2002.
[20] Federal Aviation Administration, "Aeronautical Information Manual," *Washington: Government Printing Office*, 2012. Article (CrossRef Link)
[21] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78-87, 2011. Article (CrossRef Link)
[22] A. Costin, and A. Francillon, "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Proc. of Black Hat '2012, July 21-26, Las Vegas, NV, USA*, pp. 1-10, 2012. Article (CrossRef Link)
[23] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ads-b: State of the art and beyond," *arXiv preprint arXiv:1307.3664*, 2013.
[24] U.S. Department of Commerce, "Secure Hash Standard - SHS: Federal Information Processing Standards Publication 180-4," *CreateSpace Independent Publishing Platform*, 2015. Article (CrossRef Link)
[25] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559-2564, 2014. Article (CrossRef Link)

[26] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, Jul. 2000. Article (CrossRef Link)
[27] J. Camenisch, S. Hohenberger, and M. ∅. Pedersen, "Batch verification of short signatures," in *Proc. of Advances in Cryptology - EUROCRYPT 2007*, pp. 246-263, 2007. Article (CrossRef Link)

Jingxian ZHOU received the B.S. degree in mathematics from Xuchang University in 2004, the M.S. degree in Mathematics from Zhengzhou University in 2010, and the Ph.D. degree in cryptography from Beijing University of Posts and Telecommunications, in 2013. Now, he is an associate research fellow with Information Security Evaluation Center, Civil Aviation University of China. His research interests are security authentication protocol, data privacy protection and security architecture for the Internet of Things.

Jianhua YAN received a B.S. degree in Chemistry from Jilin University, Changchun, Jilin, China, in 2002 and an M.S. degree in Computer Science Technology from Liaoning University of Petroleum and Chemical Technology, Fushun, Liaoning, China in 2005, and a Ph.D. in cryptography from Beijing University of Posts and Telecommunications, Beijing, China in 2015. He is currently employed by Ludong University. Meanwhile, he is also a associate researcher of Yantai research institute of new generation information technology, Southwest Jiaotong University. His research interests include post quantum cryptography and Internet security.