IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 24, 2020, accepted March 6, 2020, date of publication March 11, 2020, date of current version March 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2980213

Identity-Based Signature With Server-Aided Verification Scheme for 5G Mobile Systems

MOHAMMED RAMADAN[1], YONGJIAN LIAO[1], (Member, IEEE), FAGEN LI[2], (Member, IEEE), AND SHIJIE ZHOU[1], (Member, IEEE)

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

Corresponding author: Yongjian Liao (liaoyj@uestc.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61472066, and in part by the Sichuan Science and Technology Program under Grant 2018GZ0180, Grant 2018GZ0085, Grant 2017GZDZX0001, and Grant 2017GZDZX0002.

ABSTRACT Recently, security and privacy issues in mobile communication systems became an enormous challenge due to the limited resources of mobile networks regarding communication overhead, computational cost, and battery power. 5G systems provide high performance and flexibility that can connect billion of objects through Heterogeneous Wireless Networks (HWN) concerning the Internet of Things (IoT). However, some of these security challenges can be addressed by using outsourced assistants such as Server-Aided Verification (SAV) to contribute partially with the authentication process among 5G network entities. In this paper, we propose an efficient and secure identity-based signature scheme with Server-Aided Verification for 5G mobile systems (IBS-SAV). We provide a performance evaluation based on security proof of the proposed IBS-SAV scheme under existential unforgeable in the random oracle model as well as the security against collusion and adaptive chosen message attack (EUF-CMA). The performance evaluation and security analysis demonstrate that our IBS-SAV scheme is not only secure but also can reduce the communication and computation complexity for mobile systems efficiently.

INDEX TERMS Public key cryptography (PKC), identity-based signature (IBS), server-aided verification (SAV), 5G mobile systems.

I. INTRODUCTION

5G mobile systems are designed to support a variety of applications to enable the significant growth in cloud-based mobile services which have caused an upwards trend in sensitive-data privacy using outsourced cloud servers. In traditional mobile communications networks, the network and user authenticate each other. Users and networks constitute a mutual trust model [1], [2]. 5G cellular systems serve not only individual consumers but also vertical industries in providing diverse services. The 5G era does not just entail faster mobile networks or more powerful smartphones, but also new services that connect the world [3]. Also, 5G systems can provide interfaces with third-party applications through the Authentication Center (AuC). Moreover, 5G mobile networks are designed to support a variety of applications to enable growth in mobile use of cloud-based services [4]. Consequently, there is an upward trend in the outsourcing of privacy-sensitive data to cloud servers. However, unsecured terminal devices and third-party applications may bring risks to 5G networks [5].

Despite the advantages of 5G systems such as faster mobile networks, more powerful smartphones, and new international services, 5G networks are vulnerable to new forms of attack [6].

By investigating the security of current authentication protocols, we pinpoint several of their vulnerabilities against different attacks including replay attack, Man-In-The-Middle attack (MITM), and Denial of Service (DoS) attack. Security is the main concern for 5G systems because these networks are not only meant to serve users but various other applications such as industrial IoT, traffic control, e-health, smart grid, etc. [7]. Compared to previous generations such as 2G, 3G, and 4G technologies. 5G can provide higher capacity and bit rates (more than 10 Gbps) and very low latency [1] which is one of the major features in the 5G-based Internet of Things (IoT) applications by connecting billions of objects through Heterogeneous Wireless Networks (HWN) [4]. This

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

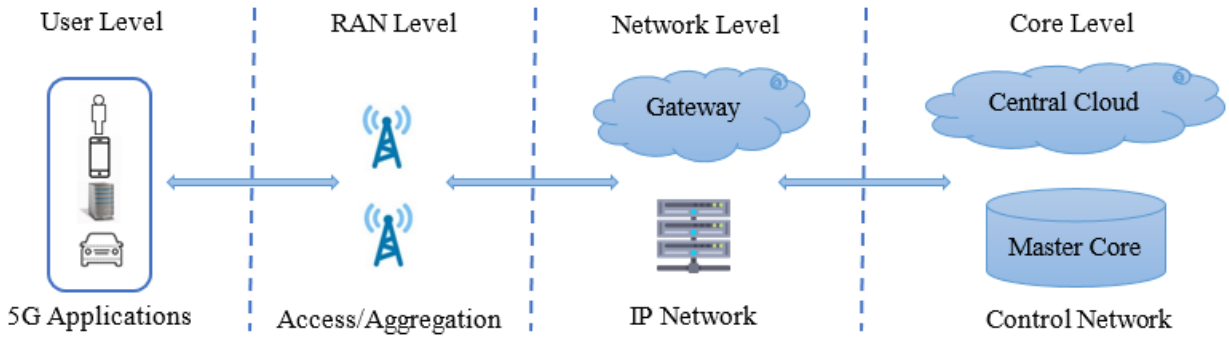


FIGURE 1. 5G overall architecture.

scenario is considered to be one of 5G vulnerabilities, especially under vertical handover processes. To overcome these issues and to achieve the authentication process, 5G needs some kind of outsourced assistance such as Server-Aided Verification (SAV) with flexible and lightweight cryptosystems [8], [9].

The main security weaknesses in IoT applications are related to authentication and unauthorized access to IoT resources. Integrity is to allow unauthorized users and data configuration and settings to be unobserved, and hence, vulnerabilities that delay and interrupt the continuous access to IoT would be related to availability. Therefore, these weaknesses are connected and related to several security requirements, each of these vulnerabilities might touch more than one security objective. The flexibility of IoT leads to some security issues, then reduces the trust in IoT applications and its implementation in the commercial markets in various fields such as industrial, medical, and Vehicular Ad-hoc Network (VANET) [10].

Also, one of the key technologies for 5G networks is Software-defined Network (SDN). SDN architecture separates the data plane from the control plane; and it roughly consists of an application layer, control layer, and infrastructure layer. Software-Defined Networking (SDN) is an evolving structure that is dynamic, manageable, cost-effective, and flexible, making it ideal for the high-bandwidth and dynamic infrastructure such as mobile communications systems. The major task of SDN architecture is to decouple the network data/control and progressing tasks that can enable the network control to become directly programmable and the core infrastructure to be inattentive for applications and network services [11].

Since 5G mobile system adopted some technologies (SDN, IoT) to provide system flexibility and high performance; then it became more vulnerable to several kinds of attacks such as Man-in-the-middle attacks (MITM), Distributed Denial of Service (DDoS), control plane saturation, flow table overloading, ID spoofing, link spoofing, etc. The security solutions for SDN and IoT are not our main focus in this research paper. Nonetheless, some of these solutions could be build based on network, host, or even cryptographic-based solutions [12].

5G requires new security architectures including secure models that cover all users in 5G systems. 4G networks integrate both the user (data) and control planes, while 5G networks separate these planes to provide more flexibility that can simplify centralized or decentralized control, and guarantee easy network slicing [1]. The 5G architecture consists of all RANs (Radio Access Network), aggregator, IP network, gateway, central cloud, and core system as described in the 3GPP document [2]. Figure 1 shows the 5G architecture that can provide different 5G applications with massive heterogeneous connection networks, and create many security challenges.

A. RELATED WORK

To avoid the security vulnerabilities in the previous mobile 2G, 3G, and 4G systems such as Man-in-the-Middle attacks (MITM), impersonation attacks, rogue base station attacks, and Denial of Service attacks, 5G security mechanisms provide more security features to achieve mutual authentication between the users and the network operator [13]. However, some proposed researches have shown how to implement Public Key Cryptography (PKC) protocols in mobile systems due to the flexibility of PKC schemes.

Sandhya *et al.* [14] proposed a mutual authentication scheme based on the SHA algorithm for Long Term Evolution using Hyper-Elliptic Curve Cryptography providing secure communication for data exchange. Haddad *et al.* [15] proposed a secure Authentication and Key Agreement protocol (EPS-AKA) for evolved packet systems in LTE-A networks using Public Key Cryptography (PKC) to provide confidentiality by using RSA as a basis to compute the temporary value for the International Mobile Subscriber Identity (IMSI). Abdo *et al.* [16] proposed a scheme called EPS mutual authentication and cryptanalysis (SPAKA), which based on self-certified protocol. SPAKA solves the issue of positive IMSI catch attacks during the user identification and key agreement process, even though the false base station is still a problem. Lai *et al.* [17] proposed a new scheme for group-based communication authentication called Secure and Efficient group Authentication and Key Agreement protocol for LTE networks (SEAKA) using the Elliptic curve Diffie-Hellman (EDH) to accomplish the key

forward/backward secrecy and also adopted an asymmetric cryptosystem for preserving user privacy. Cao *et al.* [18] proposed a handover authentication scheme between HeNB and eNB in mobile networks considered to be fast, secure, and compatible with handover authentication schemes in all mobility scenarios in the mobile networks.

Since the Third Generation Partnership Project (3GPP) released the first 5G security specifications [2], many researchers have been attracted to investigate the security weaknesses in 5G systems even the security has been enhanced from the previous generations. However, some recently published researches showed that the 5G system has serious security issues and is vulnerable to several attacks.

Basin *et al.* [19] proposed a comprehensive formal model to identify the security vulnerabilities of the 5G Authentication and Key Agreement protocol (5G-AKA) by using the security verification tool (Tamarin). This scheme showed that there are some critical security issues in 5G-AKA, and recommended some provably secure solutions to overcome these weaknesses. Recently, Braeken *et al.* [20] proposed a new version of 5G Authentication and Key Agreement protocol (5G-AKA) to overcome all the identified weaknesses in this protocol. The idea behind this new protocol is to replace the sequence numbers with random numbers, and hence to reduce the computational cost and the handshaking process as well. Also, a logic-based verification proof technique called (RUBIN) was used for formal verification to verify the security of the proposed protocol. Also, Gharsallah *et al.* [21] proposed a Secure Efficient and Lightweight Authentication and Key Agreement protocol (SEL-AKA) for 5G mobile networks to address the weaknesses in the basic protocol (5G-AKA), which is independent **of** the Global Public Key Infrastructure. This work used a formal verification tool called (AVISPA) to prove the security of the proposed scheme. Also, there are some other formal verification techniques such as (TAMARIN) that can be used to prove the security of authentication protocols [22].

However, the security issues and the limited computational capabilities in mobile networks will attract more researchers, at least shortly [23], [24]. Additionally, much research has targeted the field of mobile security using PKC cryptosystems such as [25]–[28]. Other research has focused on the idea of server-aided verification schemes such as [29]–[31], and some researchers have proposed digital signatures based on bilinear pairing [32].

The main research gaps in the field of mobile communications security are the lack of solutions based on public-key cryptographic protocols, to come up with solutions to secure the mobile systems 5G and the upcoming 6G by using secure authentication and key agreement cryptosystems. For instance, some new approaches of authentication scheme including (mutual authentication and end-to-end security) based on Public Key cryptography, Code-Based Cryptography, and quantum cryptography, which are compatible with mobile communication systems due to their high-security level and the flexibility [20]. The mobile system needs a lightweight cryptosystem due to its relatively limited resource. Hence, some cryptographic algorithms such as Identity-Based Cryptography (IBC), Certificateless Public Key Cryptography (CL-PKC), Designated Verifier Proxy Signature (DVPS), and Group/Ring signature protocols could be more practical to provide user-to-user schemes. Moreover, most of these protocols don't require a certificate to bind the public key. Thus, can provide low memory and bandwidth, and low computational cost features that are compatible with mobile applications to maintain the mobile communications security [23]. However, there exist some proposed researches have shown how to apply the flexibility of public-key cryptosystems to mobile systems.

To the best of our knowledge, until now, there is no PKC-based authentication scheme using SAV techniques for mobile systems that have been proposed with fulfilling the security requirements and proving low computational costs. This paper proposes such a security scheme.

B. SECURITY REQUIREMENTS

The security threats in mobile systems such as unauthorized access, MITM attack, and DoS attack increased the importance of identifying and improving the security requirements for mobile systems which include confidentiality, integrity, authentication, access control, nonrepudiation, and network availability. These security requirements can be explained as follows [24]:

Confidentiality: Is a process to guarantee that the transmitted information is only revealed to the authorized parties. Thus, to prevent sensitive information from being disclosed to the adversary.

Integrity: The received message can be corrupted due to transmission errors or malicious attacks. Data integrity is to guarantee that the message is not changed during the transmission process by some kind of malicious attack.

Authentication: Is the process of protecting sensitive information such as messages, users' identities, and network entities from the adversary and proving that this information is true and valid.

Access control: Is a process to allow only authorized parties to get access to specific service in the network and to use the network resources

Nonrepudiation: Is a process to guarantee that the sender of a message cannot later repudiate or deny sending the message as well as the receiver cannot deny receiving the message.

Network availability: This is to guarantee that all the network resources are always valid, available, and utilized by authorized parties. Thus, protecting the mobile network from several kinds of attacks such as DoS attack.

For mobile communications systems; and both mobile users and network operators. The authentication process is considered to be the major security requirement that can ensure a high level of security and can achieve integrity, nonrepudiation, and network availability altogether [22].

C. OUR CONTRIBUTIONS/GOALS

The security issues in 5G system include confidentiality, authentication, authorization, access control, and privacy preserving. These issues will be a high-layer problem to solve using cryptographic methods. 5G system will function as core infrastructure and involve billions of resource-constrained devices, especially regarding 5G-IoT. Therefore, the proposed IBS-SAV scheme provides a lightweight, efficient, and flexible security solution with low-delay mobility (handshaking process), low computational cost, and low communication overhead. Server-Aided Verification (SAV) signature consists of a digital signature scheme and a server-aided verification protocol. Such signatures can be verified by executing the SAV protocol with the server, where the verification requires less computation than the original verification algorithm of the digital signature [9]. The major contributions of this paper can be summarized as follows:

- We propose a concrete Identity-Based Signature (IBS) scheme with Server-Aided Verification (SAV), which provides a secure and efficient security model for 5G mobile systems.
- Our proposed IBS-SAV scheme provides an identity-based signature with low computational cost and low power consumption due to SAV technique.
- We prove the security of the IBS-SAV scheme. The security of our construction is based on Existential Unforgeable EUF under CDH assumption in the random oracle.
- The proposed scheme is EUF secure against Collusion and adaptive chosen message attack EUF-CMA.
- For formal verification proof, we use the BAN logic model to show that our scheme securely achieved SAV authentication.
- We show that the computational cost of our proposed scheme is more efficient compared to other proposed schemes. Also, we show that the proposed scheme has low communication overhead, which is more efficient and compatible with 5G systems.
- Finally, and from the performance analysis, we show that our proposed IBS-SAV supports the authentication of mobile devices through server assistant to accomplish the standards of a high-performance security system.

D. PAPER ORGANIZATION

The rest of the paper is organized as follows. In Section 2, we review some preliminaries of our proposed scheme. In Section 3, we define our proposed IBS-SAV scheme and its system model and security notions. In Section 4, we explain our IBS-SAV scheme and describe the proposed model. In Section 5, we evaluate the proposed scheme and include security proofs and computational cost aspects. Finally, we conclude the paper in Section 6.

II. PRELIMINARIES

This section discusses some basic notions required in this paper namely; bilinear pairing, DDH, and CDH assumptions [33], [34].

- Bilinear Pairing: Let G_1 and G_2 be two cyclic groups generated by P, with the same order prime p. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:
  Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in Z_p^*$.
  Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
  Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.
- Computational Diffie-Hellman Assumption (CDH): Consider a multiplicative cyclic group G of order p, with generator P. A probabilistic polynomial-time adversary has a negligible probability of computing (abP) from (P, aP, bP) for random $a, b \in Z_p^*$.
- Decisional Diffie-Hellman Assumption (DDH): Consider a multiplicative cyclic group G of order p, with generator P. A probabilistic polynomial-time adversary has a negligible probability of distinguishing $\left(P^a, P^b, P^{ab}\right)$ for random $a, b \in Z_p^*$ and $\left(P^a, P^b, P^c\right)$ for random $a, b, c \in Z_q^*$.

III. SYSTEM AND SECURITY MODELS

A. SYSTEM MODEL

The proposed IBS-SAV scheme is a combination of identity-based signature (IBS) [35] and server-aided verification (SAV) techniques [36], [37]. We employ a server-aided verification technique to reduce the computational cost of the verification process which is less in our scheme than the proposed approaches in [36], [37]. The proposed technique delegates an untrusted third party (server) to assist in the verification process from the user equipment (UE) prospective. Therefore, providing more flexibility and high security than the proposed scheme in [35] by adopting identity-based signature technique. 5G system will use the network core entity or the cloud server as an assistant to partially verify the users' signatures. The private key is calculated by a trusted third party, i.e. the network Authentication Center (AuC) using the master key, and the public key is the mobile users' identifiers such as International Mobile Subscriber Identity (IMSI), or Globally Unique Temporary UE Identity (GUTI) in case of rooming status. Figure 2 illustrates the proposed system model and the handshaking process of the IBS-SAV scheme.

There are two mobility and handover modes in the 5G system. The first one is the home-state in which the two users who are willing to authenticate each other belong to the same Radio Access Network (RAN). In this case, the users request the security parameters from the home network i.e. core entity which is computed in advance by the Authentication Center (AuC). The second mode is the roaming-state in which the two users belong to different RAN. In this case, the authentication process can be done separately in each RAN side and the security parameters will be shared via secure channels in advance from the home network. In this case, the RAN

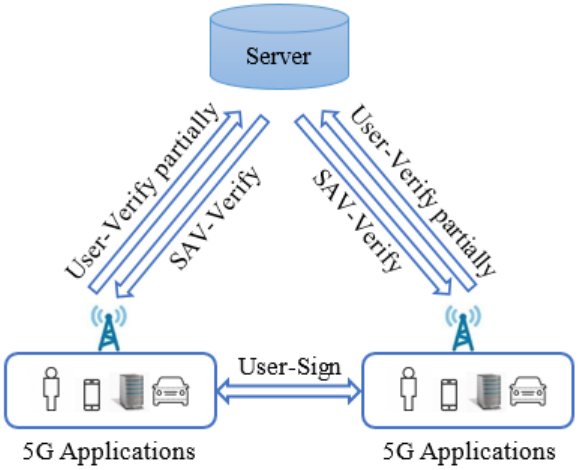


FIGURE 2. IBS-SAV system model.

entities can perform as an assistant server for the server-aided verification SAV process [23].

The proposed IBS-SAV scheme consists of five algorithms (*Setup*, *KeyGen*, *User-Sign*, *User-Verify*, *SAV-Verify*) as follows:

- *Setup*: This algorithm takes a security parameter k and returns system parameters *params*, which includes the description of the required elements in the signature.
- *KeyGen*: This algorithm takes *params*s as input and outputs a key pair (*Sk*, *Pk*), where *Sk* is the signing key and *Pk* is the verification key.
- *User-Sign*: The user takes *params*, message $m \in$ M, and the key pair (*Sk*, *Pk*) as inputs, and outputs the signature σ.
- *User-Verify*: The user takes *params*, message $m \in$ M, the public key ID, and the signature σ as input, and outputs the partially verified signature σ_1 and sends it to the server.
- *SAV-Verify*: The server takes *params*, and the partially verified signature σ_1 as inputs, and outputs another partially verified signature σ_2 and sends it to the corresponding user to complete the verification.

B. SECURITY MODEL

Definition 1: For the security, an adversary aims to forge the signature existentially. Our proposed IBS-SAV scheme is secure if the basic signature scheme involved is existentially unforgettable under adaptive chosen message attack EUF-CMA secure. Assume that $\mathcal{Ch}$ denotes a challenger, and $\mathcal{A}$ denotes an adversary. The EUF-CMA security can be described by the following games:

- *Setup*: The challenger $\mathcal{Ch}$ runs the algorithms Setup and *KeyGen* to obtain the master secret key x and the system parameters *params* and the key pair (*Sk*, *Pk*). The adversary $\mathcal{A}$ is given (*params*, *Pk*).
- *Queries*: The adversary $\mathcal{A}$ is allowed to make at most q*s* sign queries. For each sign query $m_i \in \{m_1, \ldots, m_{qs}\}$, the challenger $\mathcal{Ch}$ returns $\sigma_i = \text{Sign}(params, m_i, S, Q_{\text{ID}})$ to $\mathcal{A}$.
- *Output*: The adversary $\mathcal{A}$ outputs (m^*, σ^*) and wins the game if $m^* \notin \{m_1, \ldots, m_{sq}\}$, and verify (*params*, m^*, σ^*, ID) is valid. We say that IBS-SAV is existentially unforgeable under adaptive chosen message attacks if there exists no adversary that $(t, \text{qs}, \varepsilon)$ can break the scheme.

Definition 2: Security against collusion and adaptive chosen message attack of IBS-SAV. We can present this security in the following game.

- *Setup*: The challenger $\mathcal{Ch}$ runs the algorithms Setup, *KeyGen*, and SAV-Verify to obtain the system parameter *params*, the key pair (*Sk*, *Pk*). The adversary $\mathcal{A}$ is given (*params*, *Sk*, *Pk*).
- *Queries*: The adversary $\mathcal{A}$ is permitted to make at most $q$sv server-aided verification queries adaptively, and here the adversary $\mathcal{A}$ acts as the server and the challenger $\mathcal{Ch}$ acts as the verifier. The challenger $\mathcal{Ch}$ answers by run the algorithm SAV-Verify with the adversary $\mathcal{A}$, then $\mathcal{Ch}$ returns the output of SAV-Verify to the adversary $\mathcal{A}$.
- *Output*: The adversary $\mathcal{A}$ outputs a message m^*. The challenger $\mathcal{Ch}$ chooses a random invalid signature σ^* on the message m^* and $\mathcal{A}$ wins the game if the verification on (m^*, σ^*, ID) is valid. We say that IBS-SAV is secure against collusion and adaptive chosen message attacks if there exists no adversary that $(t, q_{\text{sv}}, \varepsilon)$ can break the scheme.

IV. IBS-SAV: CONSTRUCTION

In this section, we present a secure and efficient IBS-SAV scheme. A detailed description of the scheme as follows:

- *Setup*
  This algorithm takes as input a security parameter k, and it performs as follows:
  G_1, G_2 are two cyclic groups of prime order p, with an arbitrary generator P for G_1. Let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. Choose cryptographic hash functions: $H_1, H_2 : \{0,\ 1\}^* \rightarrow G_1$. Computes: $g = e(P, P)$. Picks a secret master key $x \in Z_{\text{p}}^*$ and computes: $P_0 = xP$.
  The system parameters are
  $params = \{e, G_1, G_2, p, P, P_0, g, H_1, H_2\}$.
- *KeyGen*
  Given a user's identity ID as a public key, compute $Q_{\text{ID}} = H_1(\text{ID})$ and the corresponding private key is $S = xQ_{\text{ID}}$.
- *User-Sign*
  Given the user's (*S*, ID, *m*, *params*), picks $a \in Z_{\text{p}}^*$ randomly, then computes:

$$U = aP$$
$$h = H_2(U, \text{ID}, m)$$
$$V = S + ah$$

  The signature is $\sigma = (U, V, h)$.

- *User-Verify*
  Given $\sigma = (U, V, h)$, the user picks $r, d \in Z_p^*$ randomly and computes:

$$h_1 = rh$$
$$V_1 = rV + dP$$

  Then the user sends $\sigma_1 = (U, V_1, h_1)$ to the server.
- *SAV-Verify*: Given $(\sigma_1, params)$, the SAV computes:

$$g_1 = e(V_1, P)$$
$$g_2 = e(Q_{ID}, P_0)$$
$$g_3 = e(h_1, U)$$

  Then SAV sends $\sigma_2 = (g_1, g_2, g_3)$ to the user.
  The user accepts the signature if the following equation holds:

$$g_1 = g_2^r g_3^{d^{-1}} g^d$$

- *Correctness*

$$\begin{aligned} g_1 &= g_2^r g_3^{d^{-1}} g^d \\ &= e(Q_{\mathrm{ID}}, P_0)^r \, e(h_1, U)^{d^{-1}} \, e(P, P)^d \\ &= e(xQ_{\mathrm{ID}}, P)^r \, e(rdh, aP)^{d^{-1}} \, e(P, P)^d \\ &= e(S, P)^r \, e(ah, P)^r \, e(P, P)^d \\ &= e(V, P)^r \, e(P, P)^d \end{aligned}$$

  We have,

$$\begin{aligned} g_1 &= e(V_1, P) = e(rV + dP, P) \\ &= e(rV, P) \, e(dP, P) \\ &= e(V, P)^r \, e(P, P)^d \end{aligned}$$

  Thus,

$$g_1 = g_2^r g_3^{d^{-1}} g^d$$

- *Computation-Saving*
  From Table 1, we can see that our proposed IBS-SAV reduces the computational cost on the user side, only needs *one* ECC-based point multiplication operation, and one Exponentiation operation. All the high computational cost operations such as bilinear pairing are done by the server. Thus, Φ-User_Verify < Φ-Server_Verify to satisfy the SAV property.

V. IBS-SAV: PERFORMANCE EVALUATION

A. INFORMAL SECURITY PROOF

In this section, we give security proof of the above signature scheme involved in our IBS-SAV scheme in the random oracle model.

Theorem 1: There exists an adversary $\mathcal{A}$ that could break the IBS-SAV scheme with advantage ε in time t, after making at most q_k times *KeyGen* queries, q_s times *Sign* queries, and q_{h1}, q_{h2} times random oracle queries to H_1 and H_2 respectively, there would be an algorithm able to solve the CDH problem with a non-negligible advantage of at least $\varepsilon_0 \geq (1/q_{h1})\,\varepsilon$ in running time $t_0 \leq t + (q_{h1} + q_{h2} + q_k + 4q_s)\,.t_{sc}$,

TABLE 1. Ban logic basic notations.

Notation	Meaning
$\mathrm{A} \mid\equiv \mathrm{M}$	A believes M
$\mathrm{A} \lhd \mathrm{M}$	A received M
$\mathrm{A} \mid\sim \mathrm{M}$	A sent M
$\mathrm{A} \mid\Rightarrow \mathrm{S}$	A controls S (jurisdiction)
$\#(\mathrm{X})$	X is a fresh statement
$\mathrm{A} \xrightarrow{S} \mathrm{B}$	S is a shared secret key between A and B
$\xrightarrow{P} A$	P is the public key of A
$\{\mathrm{M}\}_{\mathrm{K}}$	M is encrypted with secret K
$(\mathrm{S})_{\mathrm{K}}$	S is hashed with key K
$\langle \mathrm{X} \rangle_{\mathrm{Z}}$	X Combined with Z
(S, Y)	S or Y is one part of the formula (S, Y)

where t_{sc} denotes the time required for computing a scalar multiplication.

Proof: Assume $\mathcal{A}$ can break the EUF-CMA security of the scheme. Given the challenger $\mathcal{CH}$ a random tuple (P, aP, bP) of the CDH problem, then there exists an algorithm that can obtain the value of abP, here $\mathcal{CH}$ acts as a CDH problem solver. We can present the security of this theorem by the following game.

- *Setup*: $\mathcal{CH}$ set $P_0 = aP$ and generates system parameters $params = \{e, G_1, G_2, p, P, P_0, g, H_1, H_2\}$, the hash functions H_1 and H_2 are random oracles controlled by $\mathcal{CH}$. Then pick a random integer $\lambda \in [1, q_{h1}]$, let λ_{th} query to H_1 is on the target identity ID*.
- H_1 *Queries*: When $\mathcal{CH}$ receives an H_1 query on ID. In case of $(i \neq \lambda)$, $\mathcal{CH}$ randomly picks $T_{1i} \in Z_p^*$, computes $Q_i = H_1(\mathrm{ID}_i) = T_{1i}P$. In case of all the possible q_{h1} times queries $(i = \lambda)$, set $T_{1\lambda} = \perp$, $Q_\lambda = bP$, then add the corresponding tuple (ID, T_1, Q_i) to H_1_list.
- H_2 *Queries*: When $\mathcal{CH}$ receives an H_2 query on $(U_i, \mathrm{ID}_i, m_i)$. $\mathcal{CH}$ randomly picks $T_{2i} \in Z_p^*$, computes $H_2(U_i, \mathrm{ID}_i, m_i) = T_{2i}P$, then adds the corresponding tuple $(U_i, \mathrm{ID}_i, m_i, T_{2i}, T_{2i}P)$ to H_2_list.
- *KeyGen Queries*: When $\mathcal{CH}$ receives a *KeyGen* query on an identity ID_i. For all the possible q_{h1} times' queries $(i = \lambda)$, $\mathcal{CH}$ aborts the game. Otherwise, $\mathcal{CH}$ makes H_1 queries on ID_i and searches H_1_list for a tuple $(T_{1i}, \mathrm{ID}_i, Q_i)$ and generates the user's private key $S_i = T_{1i}P_0$.
- *Signing Queries*: When receiving a signing query on (ID_i, m_i), and for all the possible q_{h1} times' queries $(i = \lambda)$, $\mathcal{CH}$ generates a signature as follows:

Randomly pick $a_1, a_2 \in Z_p^*$
Compute $U = a_1 P_0$, $V = a_2 P_0$
Set $H_2\left(U, \mathrm{ID}^*, m\right) = a_1^{-1}\left(a_2 P - H_1\left(\mathrm{ID}^*\right)\right)$
If there has been a tuple $(U, \mathrm{ID}^*, m, \perp)$ in H_2_list, then $\mathcal{Ch}$ chooses another $a_1 \in Z_p^*$ and repeat the above signature.

- *Forge*: $\mathcal{A}$ generates a forgery on $\sigma^* = \left(U^*, V^*, \mathrm{ID}^*, m^*\right)$. If it is a valid signature, then can pass the following verification:

$$e\left(V^*, P\right) = e\left(P_0, Q^*\right) e\left(U^*, h^*\right)$$

where, $Q^* = H_1\left(\mathrm{ID}^*\right) = bP$, $h^* = H_2\left(U^*, \mathrm{ID}^*, m^*\right)$
Search the H_2_list for $H_2\left(U^*, \mathrm{ID}^*, m^*\right) = T_2 \lambda P$.
Then $\mathcal{Ch}$ can get, $e\left(V^*, P\right) = e\left(aP, bP\right) e\left(U, T_2 \lambda P\right)$
Then, $abP = V^* - T_2 \lambda U^*$

According to the assumption, there exist an algorithm can solve the CDH problem with an advantage: $\varepsilon_0 \geq (1/q_{\mathrm{h1}})\,\varepsilon$ in running time: $t_0 \leq t + (q_{\mathrm{h1}} + q_{\mathrm{h2}} + q_{\mathrm{k}} + 4q_{\mathrm{s}})\,.t_{\mathrm{sc}}$, where t_{sc}: the time required for computing a scalar multiplication.

Theorem 2: The IBS-SAV scheme is secure against collusion and adaptive chosen message attack. Adversary $\mathcal{A}$ that could break the signature under $(t, q_{\mathrm{sv}}, 1/(p-1))$ if $\mathcal{A}$ runs in time at most t, makes at most q_{sv} SAV queries. We say that IBS-SAV is secure against collusion and adaptive chosen message attacks if there exists no adversary that can break the scheme.

Proof: We will show that the adversary can only prove an invalid signature as a valid one with at most probability $1/(p-1)$ as follows.

- *Setup*: $\mathcal{Ch}$ picks a random $x \in Z_p^*$ then computes $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$ and the corresponding private key $S = xQ_{\mathrm{ID}}$, and generates system parameters $params = \{e, G_1, G_2, p, P, P_0, g, H_1, H_2\}$. Then $\mathcal{Ch}$ sends $(params, Sk, Pk)$ to $\mathcal{A}$.
- *Queries*: $\mathcal{A}$ is permitted to make at most q_{sv} server-aided verification queries, and here the adversary $\mathcal{A}$ acts as the server and the challenger $\mathcal{Ch}$ acts as the verifier. The challenger $\mathcal{Ch}$ answers by run the algorithm SAV-Verify with the adversary $\mathcal{A}$, then $\mathcal{Ch}$ returns the output of SAV-Verify to the adversary $\mathcal{A}$.
- *Output*: $\mathcal{Ch}$ randomly picks $r^*, d^* \in Z_p^*$, and computes $h_1^* = r^* d^* h$, $V_1^* = r^* V + d^* P$ and sends $\sigma_1^* = \left(U, V_1^*, h_1^*\right)$ to $\mathcal{A}$. Then $\mathcal{A}$ returns $\sigma_2^* = \left(g_1^*, g_2^*, g_3^*\right)$ to $\mathcal{Ch}$.
  In the following, we will show that $g_1 = g_2^r g_3^{d^{-1}} g^d$ happens with probability $1/(p-1)$.
  $\mathcal{Ch}$ sends σ_1^* to $\mathcal{A}$ as follows:

$$h_1^* = r^* d^* h$$
$$V_1^* = r^* V + d^* P$$

We assume a strong-collusion attack in which the adversary $\mathcal{A}$ can have all the abilities of the sender and the untrusted server besides the system parameters. When $\mathcal{A}$ receives $\sigma_1^* = \left(U, V_1^*, h_1^*\right)$ with some random elements $r^*, d^* \in Z_p^*$ randomly chosen by $\mathcal{Ch}$.

From the adversary viewpoint, h_1^*, V_1^* are linearly independent and uniquely determined by r^*, d^* which are chosen by $\mathcal{Ch}$. Then $\mathcal{A}$ output σ_2^* such that $g_1 = g_2^r g_3^{d^{-1}} g^d$ holds. We can rewrite this equation as follows:

$$g_1 = r^*.\mathrm{DL}_g g_2 + d^{*-1}.\mathrm{DL}_g g_3 + d^*$$

Then $\mathcal{Ch}$ sends
$\sigma_2^* = [e\left(V_1, P\right), e\left(Q_{\mathrm{ID}}, P_0\right), e\left(h_1, U\right)]$ to $\mathcal{A}$.

According to the assumption, σ_2^* is an invalid signature and uniquely determined by r^*, d^* and the equality:

$e\left(V_1, P\right) = e\left(Q_{\mathrm{ID}}, P_0\right)^{r*} e\left(h_1, U\right)^{d*^{-1}} e\left(P, P\right)^{d*}$ does not hold. Thus, the adversary can only output g_1, g_2, g_3 to satisfy the above equation by guessing the randoms r^*, d^* with probability $1/(p-1)$.

Theorem 3: The IBS-SAV scheme is secure against replay attack, Man-In-The-Middle attack (MITM), and Denial of Service attack (DoS).

- *Replay attack*: This happens when the adversary gets some security information from the previous session and using it in the current session to impersonate a valid user.
  Proof: The proposed IBS-SAV scheme is secure against this attack due to the changeable private keys: $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$, $S = xQ_{\mathrm{ID}}$. This private key derived from the hash value of the temporary identities in case of roaming which is changeable according to the user's location area. Therefore, when the adversary uses the previous security parameters, the request will be rejected and invalid.
- *Man-In-The-Middle attack*(*MITM*): Also known as false base station attack in mobile security. This happens when the adversary intercepts actively or passively the communication between the network entities. Then the adversary acts as one or more of the network entities.
  Proof: The proposed IBS-SAV scheme is secure against this attack due to the difficulties for the attacker to get or recover any information, and this is because of the use secure signature against collusion and adaptive chosen message attack with negligible probability for the adversary to recover the signature or any random elements, even if the server collude with the adversary or with other valid users. If the signature is invalid, then the network entities recognize this is a false base station, then outputs invalid to the Authentication Center (AuC).
- *Denial of Service attack*(*DoS*): This happens when the adversary impersonates as a valid user and sends false messages requests to access the network. However, 5G system considered to be secure against DoS and Distributed Denial of Service attack (DDoS) due to the distributed security functionality by the isolation between network slices which makes cyber-attacks be limited to specific slices without impacting other network parts.
  Proof: The proposed IBS-SAV scheme is secure against this attack because of the security against existentially unforgettable under adaptive chosen message attack EUF-CMA secure. In the proposed protocol, the

user generates the signature by choosing $a \in Z_p^*$ randomly. Then the other user partially verifies the signature by choosing $r, d \in Z_p^*$ randomly and use some assistance from the server. Finally, verify the signature using the same random elements ($g_1 = g_2^r g_3^{d^{-1}} g^d$). This makes the network entities independently secure under the CDH assumption. Moreover, the proposed scheme provided integrity and non-repudiation features by hashing the contents of the message and signing this hash with the sender's private key, then both the message and the hash value $\sigma = (U, V, h)$ is sent to the receiver as follows: $U = aP$, $h = H_2(U, \mathrm{ID}, m)$, $V = S + ah$ and the two parties (user, server) cannot generate the same signature. Therefore, these two security features can provide resistance against DoS attack.

Analysis: Through the above analysis of three theorems, we can conclude that our IBS-SAV scheme for 5G mobile system is EUF-CMA secure by the respect of the hardness of CDH assumption in the random oracle as well as is secure against collusion and adaptive chosen message attack, replay attack, MITM attack, and DoS attack. Hence, it can provide a secure cryptosystem and ensure the users' authentication and the data integrity for mobile users. Also, the proposed scheme has more security features by providing a secure and lightweight authentication algorithm, then by using the network administrator entity as a second defense line to protect users against capture attack and false base-station attack by the mean of network security and access control.

B. FORMAL SECURITY PROOF

In this section, we prove our proposed IBS-SAV scheme using the BAN logic. The BAN logic [38] is a well-established formal technique used for analyzing and evaluating authentication protocols to ensure that these protocols achieve the authentication process securely.

BAN logic is a logic on belief that can construe the proof of security of authentication protocols through some rules [39], [40]. Moreover, BAN logic works as a tool to analyze and verify authentication protocols. BAN logic is divided into four specification processes, which consists of general protocol specifications (BAN notations), assumptions to represent this idealized protocol (assumptions), idealized process, which uses BAN notations to translate the protocol parameters into BAN logic form (idealized form), and the steps of proof that is the main purpose of the protocol security proof and verification (proof-steps) [41]. Consequently, to proof the security features using BAN logic, we must first define some assumptions and identify and specify the idealized protocol form by using the protocol specifications (BAN notations), then we use the logical meaning of rules to proof and verify the security of authentication protocols [42].

For our IBS-SAV, we use the BAN logic to validate formally the authentication and trust properties of the proposed scheme between users (A), (B), and server (C). Some basic concepts and notations of the BAN logic are explained in Table 1 as the initial requirements of the formal verification proof [39].

There are other common rules such as inference rules for freshness, message-meaning, jurisdiction, and nonce-verification properties. However, these rules are useful for the informal security proof of challenge-response protocols and handover-based authentication schemes [38], [39]. This proof can be modified to achieve mutual authentication property by some modifications in (*Goals*, *G*1:*G*5).

Proof: Building on the above rules and notations, we verify the proposed IBS-SAV scheme as follows:

- *Assumptions*
  - (*A*1) $\mathrm{A}| \Rightarrow \mathrm{S}$
  - (*A*2) $\mathrm{B}| \equiv \xrightarrow{Q} \mathrm{A}$
  - (*A*3) $\mathrm{A}| \equiv \#(\sigma)$
  - (*A*4) $\mathrm{B}| \equiv \#(\sigma_1)$
  - (*A*5) $\mathrm{C}| \equiv \#(\sigma_2)$
  - (*A*6) $\mathrm{B}| \equiv \mathrm{A}| \Rightarrow \sigma$
  - (*A*7) $\mathrm{C}| \equiv \mathrm{B}| \Rightarrow \sigma_1$
  - (*A*8) $\mathrm{B}| \equiv \mathrm{C}| \Rightarrow \sigma_2$
- *Idealized Form*
  - (*I*1) $\mathrm{A}| \rightarrow \mathrm{B}| : \{U, V, h\}_S$
  - (*I*2) $\mathrm{B}| \rightarrow \mathrm{C}| : \{U, V_1, h_1\}_{(r,d)}$
  - (*I*3) $\mathrm{C}| \rightarrow \mathrm{B}| : \{g_1, g_2, g_3\}_Q$
- *Goals*
  - (*G*1) $\mathrm{B}| \equiv \mathrm{A}| \Rightarrow \mathrm{S}$
  - (*G*2) $\mathrm{C}| \equiv \mathrm{B}| \Rightarrow (r, d)$
  - (*G*3) $\mathrm{B}| \equiv \mathrm{A}| \sim \sigma$
  - (*G*4) $\mathrm{C}| \equiv \mathrm{B}| \sim \sigma_1$
  - (*G*5) $\mathrm{B}| \equiv \mathrm{C}| \sim \sigma_2$
- *Steps*

  From the above assumptions, we can write the following rules:

$$\mathrm{A}| \Rightarrow \mathrm{S}$$
$$\mathrm{B}| \triangleleft aP, \{V\}_S, H_2(aP, \mathrm{ID}, m)$$
$$\mathrm{B}| \equiv \xrightarrow{Q} \mathrm{A}$$
$$\mathrm{B}| \equiv \mathrm{A}| \sim aP, \{V\}_S, H_2(aP, \mathrm{ID}, m)$$
$$\mathrm{B}| \equiv \mathrm{A}| \Rightarrow \mathrm{S}$$
$$\mathrm{B}| \equiv \mathrm{A}| \sim \sigma$$

  Then

$$\frac{\mathrm{B} |\equiv (\mathrm{A}| \Rightarrow \sigma), \mathrm{B} |\equiv (\mathrm{A}| \equiv \{\sigma\}_{\mathrm{S}})}{\mathrm{B} |\equiv \mathrm{A}| \equiv \sigma}$$

  And

$$\mathrm{C}| \equiv \mathrm{B}| \Rightarrow (\mathrm{r,d})$$
$$\mathrm{C}| \triangleleft aP, \{V\}_{(r,d)}, H_2(aP, \mathrm{ID}, m)$$
$$\mathrm{C}| \equiv \mathrm{B}| \sim aP, \{V\}_{(r,d)}, H_2(aP, \mathrm{ID}, m)$$
$$\mathrm{C}| \equiv \mathrm{B}| \sim \sigma_1$$

  Then

$$\frac{\mathrm{C} |\equiv (\mathrm{B}| \Rightarrow \sigma_1), \mathrm{C} |\equiv (\mathrm{B}| \equiv \{\sigma_1\}_{(\mathrm{r,d})})}{\mathrm{C} |\equiv \mathrm{B}| \equiv \sigma}$$

And

$$\mathrm{C}| \equiv \xrightarrow{Q} \mathrm{A}$$
$$\mathrm{B}| \equiv \mathrm{C}| \sim g_1, g_2, g_3$$
$$\mathrm{C}| \equiv \mathrm{B}| \Rightarrow (\mathrm{r,d})$$
$$\mathrm{B}| \equiv \mathrm{C}| \sim \sigma_2$$

Then

$$\frac{\mathrm{B}| \equiv (\#(\sigma_2)), (\mathrm{C}| \Rightarrow \sigma_2), \mathrm{B} |\equiv (\mathrm{C}| \equiv \sigma_2)}{\mathrm{B} |\equiv \mathrm{C}| \equiv \sigma_2}$$

From the above steps, we can proof that:

$$\frac{\mathrm{B}| \equiv \mathrm{A}| \Rightarrow \sigma, \mathrm{B}| \triangleleft \{\sigma\}_s}{\mathrm{B}| \equiv \mathrm{A}| \sim \sigma}$$
$$\frac{\mathrm{C}| \equiv \mathrm{B}| \Rightarrow (r, d), \mathrm{C}| \triangleleft \{\sigma_1\}_{(r,d)}}{\mathrm{C}| \equiv \mathrm{B}| \sim \sigma_1}$$
$$\frac{\mathrm{B}| \equiv \mathrm{C}| \equiv \xrightarrow{Q} \mathrm{A}|, \mathrm{B}| \triangleleft \{\sigma_2\}_Q}{\mathrm{B}| \equiv \mathrm{C}| \sim \sigma_2}$$

Thus, we have satisfied the required goals ($G1$), ($G2$), ($G3$), ($G4$), and ($G5$) for formal security of our proposed IBS-SAV scheme according to the above-mentioned formulas in the proof steps. Consequently, we can conclude that users (A) and (B) successfully achieved the authentication process through the assistant of server (C) in a secure manner using the proposed IBS-SAV scheme.

C. COMPUTATIONAL COST EFFICIENCY

In this section, we evaluate the performance of our proposed IBS-SAV scheme as well as the performance of the schemes mentioned in [35]–[37], mainly in terms of computational costs. To get the implementation time of the basic operations through this comparison, we execute our experiments on a desktop PC platform adhering to the following settings: PIV; Windows XP OS 64 (bits); 3 (GHz) CPU; 1 (GB) RAM. We employed MIRACL and PBC Libraries in [42], [43], and the existing experimental in [44]–[46]. The running time for each operation is defined below:

T_1: ECC-based point multiplication operation = 1.97 (ms)
T_2: Exponentiation operation = 2.573 (ms)
T_3: Bilinear pairing operation = 20.04 (ms)
T_4: General hash function = 0.009 (ms)

Other lightweight operations (e.g. XOR, addition, symmetric encryption, etc.) < 0.008 (μs) (Omitted).

TABLE 2. Comparison of computational cost efficiency (ms).

Scheme	[35]	[36]	[37]	Ours
User-Sign	$2T_1 + T_4$ = 3.949	$T_1 + 3T_2$ = 9.689	$T_2 + T_4$ = 2.582	$2T_1 + T_4$ = 3.949
User-Verify	$3T_3 + 2T_4$ = 60.138	$T_1 + 2T_3$ = 42.050	$2T_3 + T_4$ = 40.089	$T_1 + T_2 + T_4$ = 4.552
Total	64.087	51.739	42.671	8.501

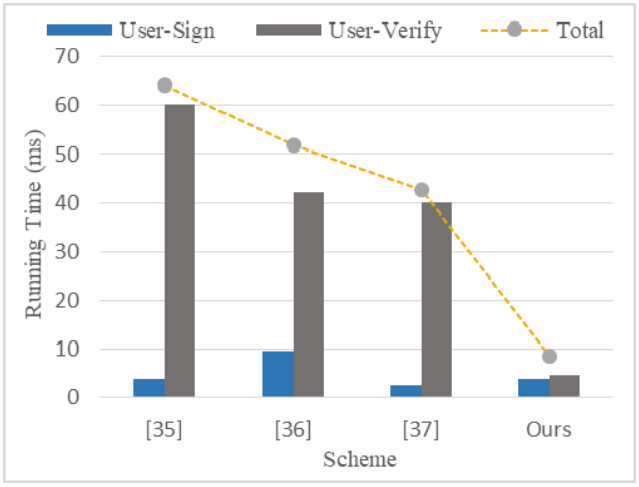


FIGURE 3. Comparison of computational cost efficiency (ms).

D. COMMUNICATION OVERHEAD EFFICIENCY

Mobile systems have extremely limited power. The most important issues that heavily consumed this power are the computation cost and communication cost. Communication overhead is a significant factor in constrained environments such as mobile systems. However, our proposed IBS-SAV scheme lowers the communication overhead by reducing the size of the transmitted data. We adopted the 80 (bits) security level, RSA-1024 (bits), and ECC-160 (bits). Assume that $|G_1| = |G_2| = |\mathrm{ID}| = |m| = 160$ (bits).

TABLE 3. Comparison of communication overhead efficiency (bits).

Scheme	[35]	[36]	[37]	Ours
User	$2\,\|G_1\| + \|\mathrm{ID}\| + \|m\|$ = 640	$2\,\|G_1\| + \|G_2\| + \|m\|$ = 640	$2\,\|G_1\| + \|m\|$ = 480	$3\,\|G_1\|$ = 480
Server	$2\,\|G_1\| + \|ID\| + \|m\|$ = 640	$3\,\|G_2\|$ = 480	$2\,\|G_2\| + \|G_1\|$ = 480	$2\,\|G_2\|$ = 320
Total	1280	1120	960	800

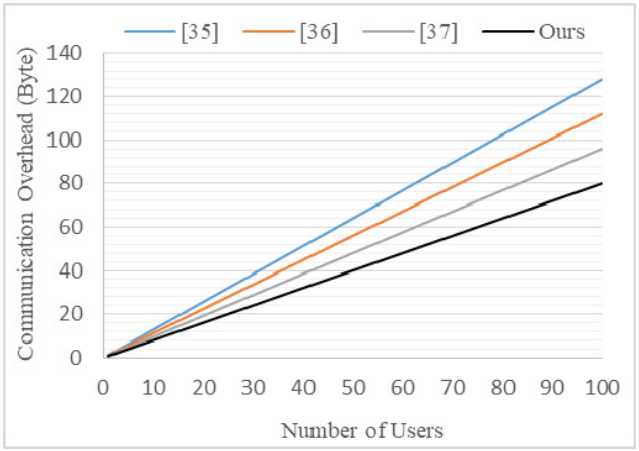


FIGURE 4. Comparison of communication overhead efficiency (Byte).

E. COMPARISON ANALYSIS

In the field of wireless communications, mobile communications, or any other low-power communication systems, the power consumptions, computational cost, and communications overhead cause severe problems due to the restrictions of lightweight communication systems performance, especially for PKC cryptosystem. Many other approaches have proposed techniques that require the use of PKC to improve the security level in such lightweight communication systems [47], [48]. As depicted in both Table 2 and Figure 3, the computational cost of our scheme decreases compared to the computational costs in schemes [35]–[37]. Also, it is essential to consider the communication overhead which is limited to the power and bandwidth resources and can affect the performance of communication systems.

Note that the total computational cost for schemes [35], [36], [73] are 64.087 (ms), 51.739 (ms), and 42.671 (ms), respectively. Meanwhile, the computational cost of our scheme is 8.501 (ms). Thus, our scheme reduces the computational cost by at least 50% of the above-mentioned schemes. On the other hand, we note that the communication overhead for schemes [35]–[37] are 1280 (byte), 1120 (byte), and 960 (byte), respectively, and 800 (byte) for our proposed scheme. Thus, our scheme requires lower communication overhead than other proposed approaches.

As a result, our proposed IBS-SAV scheme provides low communication overhead compared to other proposed approaches as shown in Table 3 and Figure 4. Therefore, our scheme can achieve better computational and communication performance than the previously mentioned proposed schemes, and more importantly, our scheme could be compatible with 5G mobile applications.

The future security solutions for mobile communications systems could be some public-key cryptosystems for 5G-based IoT applications in which can solve the problem of the false base station and replay attacks by making the private key changeable by the mean of handover authentication and can provide end-to-end security [49]. Thus, this solution allows mobile users to authenticate each other and authenticate the network core system as well before providing any services. Furthermore, this solution could use designated verifier proxy signature and key agreement protocol based on bilinear pairing with some changes in both security algorithms and the 5G-IoT security architecture within the 5G standardization [50].

VI. CONCLUSION

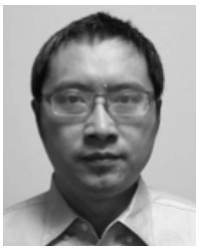
Mobile systems required lightweight cryptosystems to reduce the computational cost, data processing, and data transmission. This paper proposed a secure and efficient identity-based signature with a server-aided verification scheme for 5G mobile systems that reduces the computational cost to a minimum. Moreover, we prove that our scheme achieves high-security standards under the CDH assumption in the random oracle model. The results show that the proposed scheme meets the security requirements for 5G mobile systems. Thus, the proposed scheme is efficient and compatible with 5G applications. Our future research and investigations will focus on designing and implementing more efficient and reliable authentication and privacy preservation schemes for mobile systems.

REFERENCES

[1] *System Architecture for the 5G System*, document 3GPP, TS 23.501, Version 15.2.0, Release 15, Jun. 2018.
[2] *3GPP System Architecture Evolution (SAE); Security Architecture*, document 3GPP, TS 33.401, Version 10.3.0, Release 10, Jul. 2012.
[3] X. Zhang, A. Kunz, and S. Schroder, "Overview of 5G security in 3GPP," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 181–186.
[4] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014.
[5] I. F. Akyildiz, P. Wang, and S.-C. Lin, "SoftAir: A software defined networking architecture for 5G wireless systems," *Comput. Netw.*, vol. 85, pp. 1–18, Jul. 2015.
[6] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
[7] Y. Deng, H. Fu, X. Xie, J. Zhou, Y. Zhang, and J. Shi, "A novel 3GPP SAE authentication and key agreement protocol," in *Proc. IEEE Int. Conf. Netw. Infrastruct. Digit. Content*, Nov. 2009, pp. 557–561.
[8] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *J. Netw. Comput. Appl.*, vol. 96, pp. 39–61, Oct. 2017.
[9] M. Girault and D. Lefranc, "Server-aided verification: Theory and practice," in *Advances in Cryptology—ASIACRYPT* (Lecture Notes in Computer Science), vol. 3788. Berlin, Germany: Springer, 2005, pp. 605–623.
[10] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.
[11] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Li, "SecSDN-cloud: Defeating vulnerable attacks through secure software-defined networks," *IEEE Access*, vol. 6, pp. 8292–8301, 2018.
[12] B. Yuan, D. Zou, S. Yu, H. Jin, W. Qiang, and J. Shen, "Defending against flow table overloading attack in software-defined networks," *IEEE Trans. Services Comput.*, vol. 12, no. 2, pp. 231–246, Mar. 2019.
[13] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5G HetNets," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 20–24.
[14] P. Sandhya, S. Poovizhi, and R. Varun, "SHA-based mutual authentication in long term evolution using hyper elliptic curve cryptography," *Int. J. Emerg. Sci. Eng.*, vol. 6378, no. 10, pp. 54–55, Aug. 2013.
[15] Z. J. Haddad, S. Taha, and I. A. S. Ismail, "SEPS-AKA: A secure evolved packet system authentication and key agreement scheme for LTE-A networks," *Comput. Sci. Inf. Technol.*, vol. 1, pp. 57–70, Dec. 2014.
[16] J. B. Abdo, J. Demerjian, K. Ahmad, H. Chaouchi, and G. Pujolle, "EPS mutual authentication and crypt-analyzing SPAKA," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Jan. 2013, pp. 303–308.
[17] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, Dec. 2013.
[18] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, May 2012.
[19] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Jan. 2018, pp. 1383–1396.
[20] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks," *IEEE Access*, vol. 7, pp. 64040–64052, 2019.
[21] I. Gharsallah, S. Smaoui, and F. Zarai, "A secure efficient and lightweight authentication protocol for 5G cellular networks: SEL-AKA," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 1311–1316.

[22] D. Basin, L. Hirschi, and R. Sasse, "Symbolic analysis of identity-based protocols," in *Foundations of Security, Protocols, and Equational Reasoning*. Cham, Switzerland: Springer, 2019, pp. 112–134.
[23] M. Ramadan, F. Li, C. X. Xu, A. Mohamed, H. Abdalla, and A. Abdalla, "User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System," *Int. J. Netw. Secur.*, vol. 18, no. 4, pp. 769–781, Jul. 2016.
[24] M. Ramadan, F. Li, C. X. Xu, A. Abdalla, and H. Abdalla, "An efficient end-to-end mutual authentication scheme for 2G-GSM system," in *Proc. IEEE Int. Conf. Big Data Anal. (ICBDA)*, Hangzhou, China, Mar. 2016, pp. 1–6, doi: 10.1109/ICBDA.2016.7509848.
[25] M. Ramadan, F. Li, C. X. Xu, K. Oteng, and H. Ibrahim, "Authentication and key agreement scheme for CDMA cellular system," in *Proc. IEEE Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jun. 2015, pp. 118–124, doi: 10.1109/ICCSN.2015.7296138.
[26] Y. Xu, M. Wang, H. Zhong, J. Cui, L. Liu, and V. N. L. Franqueira, "Verifiable public key encryption scheme with equality test in 5G networks," *IEEE Access*, vol. 5, pp. 12702–12713, 2017, doi: 10.1109/ACCESS.2017.2716971.
[27] J. Guan, Z. Wei, and I. You, "GRBC-based network security functions placement scheme in SDS for 5G security," *J. Netw. Comput. Appl.*, vol. 114, pp. 48–56, Jul. 2018.
[28] Q. Liu, H. Xiao, X. Qiu, and L. Yu, "Impact of social interaction on the capacity of hybrid wireless networks," *IEEE Access*, vol. 6, pp. 46683–46694, 2018.
[29] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li, "Server-aided attribute-based signature with revocation for resource-constrained Industrial-Internet-of-Things devices," *IEEE Trans Ind. Informat.*, vol. 14, no. 8, pp. 3724–3732, Aug. 2018.
[30] C. H. Lim and P. J. Lee, "Security and performance of server-aided RSA computation protocols," in *Advances in Cryptology—CRYPT0* (Lecture Notes in Computer Science), vol. 963. Berlin, Germany: Springer, 1995, pp. 70–83.
[31] F. Guo, Y. Mu, W. Susilo, and V. Varadharajan, "Server-aided signature verification for lightweight devices," *Comput. J.*, vol. 57, no. 4, pp. 481–493, Apr. 2014.
[32] Y. Liao, Y. He, F. Li, and S. Zhou, "Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement," *Comput. Standards Inter.*, vol. 56, pp. 101–106, Feb. 2018, doi: 10.1016/j.csi.2017.09.008.
[33] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003.
[34] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Public Key Cryptography. PKC* (Lecture Notes in Computer Science), vol. 2947. Berlin, Germany: Springer, 2004, pp. 277–290.
[35] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient ID-based aggregate signature scheme for wireless sensor networks," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 546–554, Apr. 2017.
[36] L. Xu, J. Li, S. Tang, and J. S. Baek, "Server-aided verification signature with privacy for mobile computing," *Mobile Inf. Syst.*, vol. 2015, Mar. 2015, Art. no. 626415.
[37] W. Wu, Y. Mu, W. Susilo, and X. Huang, "Provably secure server-aided verification signatures," *Comput. Math. Appl.*, vol. 61, no. 7, pp. 1705–1723, Apr. 2011.
[38] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[39] R. Amin and G. P. Biswas, "Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment," *Wireless Pers. Commun.*, vol. 84, no. 1, pp. 439–462, Sep. 2015.
[40] W. Yadi, S. Nina, H. Jihong, and W. Na, *Cryptographic Protocol Formal Analysis*, Beijing, China: Machine Press, 2006.
[41] Y. Shiping and L. Xiang, "Key guessing drawback in authentication protocol analysis with BAN logic," *Comput. Eng.*, vol. 32, no. 9, pp. 126–127, 2006.
[42] M. Scott. (2003). MIRACLE-Multiprecision Integer and Rational Arithmetic C/C++ Library. Shamus Software Ltd, Dublin, Ireland. [Online]. Available: http://www.shamus.ie
[43] B. Lynn, "On the implementation of pairing-based cryptography," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Appl. Cryptogr. Group, Secur. Lab, PBC Library, Stanford, CA, USA, 2007.
[44] D. He, J. Chen, and R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Comput. Electr. Eng.*, vol. 37, no. 4, pp. 444–450, Jul. 2011.
[45] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
[46] S. Canard, N. Desmoulins, J. Devigne, and J. Traoré, "On the implementation of a pairing-based cryptographic protocol in a constrained device," in *Proc. Int. Conf. Pairing-Based Cryptogr.*, M. Abdalla and T. Lange, Eds. Berlin, Germany: Springer, Mar. 2013, pp. 210–217.
[47] M. Ramadan, G. Du, F. Li, and C. Xu, "A survey of public key infrastructure-based security for mobile communication systems," *Symmetry*, vol. 8, no. 9, p. 85, 2016.
[48] M. Ramadan, L. Yongjian, F. Li, S. Zhou, and H. Abdalla, "IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area network," *Mobile Netw. Appl.*, vol. 25, pp. 223–233, Apr. 2019, doi: 10.1007/s11036-019-01215-9.
[49] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599–8609, 2018.
[50] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

MOHAMMED RAMADAN received the Ph.D. degree in information security from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2016. He is currently a Postdoctoral Research Fellow at the School of Information and Software Engineering, UESTC. His main research interests include information security, cryptographic protocols, and wireless/mobile security.



YONGJIAN LIAO (Member, IEEE) received the Ph.D. degree in applied electronic science and technology from the College of Information Science and Electronic Engineering, Zhejiang University, in 2007. He is currently an Associate Professor at the School of Information and Software Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China. His main research interests include public key cryptography and information security, in particular, cryptographic protocols.

FAGEN LI (Member, IEEE) received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2007. He is currently a Professor at the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China. From 2008 to 2009, he was a Postdoctoral Fellow in Future University Hakodate, Hokkaido, Japan, which is supported by the Japan Society for the Promotion of Science (JSPS). He worked as a Research Fellow with the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan, from 2010 to 2012. He has published more than 80 articles in international journals and conferences. His recent research interests include cryptography and network security.

SHIJIE ZHOU (Member, IEEE) received the Ph.D. degree in computer science and technology from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2004. He is currently a Professor at the School of Information and Software Engineering, UESTC. His research interests include communication and security in computer networks, peer-to-peer networks, sensor networks, cloud security, and big data.