Chinese Journal of Electronics
Vol.32, No.3, May 2023

Zero-Cerd: A Self-Blindable Anonymous Authentication System Based on Blockchain

YANG Kunwei, YANG Bo, WANG Tao, and ZHOU Yanwei

(*School of Computer Science, Shaanxi Normal University, Xi'an 710119, China*)

Abstract — While the Internet of things brings convenience to people's lives, it will also bring people hidden worries about data security. As an important barrier to protect data security, identity authentication is widely used in the Internet of things. However, it is necessary to protect users' identity privacy while authenticating their identity. Anonymous authentication technology is often used to solve the contradiction between legitimacy and privacy in the authentication process. The existing anonymous authentication scheme has many problems in practical application such as the inability to achieve complete anonymity, the high computational complexity of the algorithm, and the corruption of the central authority. Aiming at the privacy of authentication, we propose Zero-Cerd, a self-blindable anonymous authentication system based on blockchain and dynamic accumulator. The self-blinding properties of the credential enable the users themselves to generate a new validly pseudonymous credential. With the help of zero-knowledge proof technology, users can prove the validity of their credentials without disclosing any information. Security analysis shows that our scheme has achieved the expected security objectives. Compared with the existing schemes, our scheme has the advantages of complete anonymity and high efficiency, and is more suitable for IoT applications with privacy protection requirements.

Key words — IoT, Blockchain, Anonymous authentication, Privacy protection, Dynamic accumulator.

I. Introduction

The Internet of things (IoT), namely the Internet connected by all things, is a huge network formed by combining various information sensing devices with the network to realize the interconnection of people, machines, and things. The development of IoT has gradually penetrated into all aspects of people's lives, and traditional activities have been increasingly replaced by online activities. However, the complex and open characteristics of the IoT are also full of unknown hidden dangers. Along with the occurrence of privacy disclosure, information theft and other events, privacy protection has gradually become a hot research topic, and researchers have put forward many effective solutions [1]–[4].

Identity authentication is an important means to solve system security management [5]–[7]. It can effectively ensure the authenticity, legitimacy, and uniqueness of user identity and prevent illegal personnel from entering the system. The existing authentication schemes have many problems in practical application due to their defects or network environment problems, which embody in the following aspects: first, the schemes heavily rely on the third-party credential management center and give it too much power. This centralized authentication mode is prone to the single point of failure and trust crisis. Second, users need to show their credentials to prove their legitimacy in the authentication process, which often divulges the users' personal identity information. Third, most of the existing schemes do not support unlinkability which means it is easy for a malicious adversary to learn something about user information, or to link the execution of two authentication algorithms. Finally, when the user misbehaves or the credential is leaked, the credential needs to be revoked in time. The revocation problem is still relatively complex. In the distributed network environment with high privacy requirements, a decentralized, efficient and completely anonymous authentication scheme will be favored.

Ouaddah *et al.* [8] proposed a completely decentral-

Manuscript Received June 19, 2022; Accepted July 13, 2022. This work was supported by National Key R&D Program of China (2017YFB0802000), the National Natural Science Foundation of China (U2001205, 61772326, 61802241, 61802242), National Cryptography Development Fund during the 13th Five-year Plan Period (MMJJ20180217), and the Fundamental Research Funds for the Central Universities (GK202003079, GK202007033, 2020TS087).

 DOI:10.23919/cje.2022.00.047

ized anonymous access control mechanism based on the idea of bitcoin [9], which can realize end-to-end authentication. The mechanism uses access tokens instead of bitcoin to realize a variety of new transaction types, including resource registration, access token grant, delegation, and revocation of an access token. This paper holds that the idea of anonymous transactions with bitcoin addresses can realize the privacy protection of user identity. However, it should be pointed out that if the goal is to achieve complete privacy, only pseudonym is not enough. Several studies have shown that bitcoin provides a limited form of unlinkability, that is, users always create pseudonyms when connecting to the bitcoin system. However, due to the openness of the blockchain, anyone can find all transactions involving a given address, conduct static analysis of the blockchain or actively monitor network information to decrypt users, and mine the association between bitcoin address and users' real-world identity, that is, to achieve de-anonymization. Aiming at the problem of weak privacy of bitcoin, Miers *et al.* [10] proposed a zerocoin protocol, which is an extension of the bitcoin protocol. The protocol uses a strong RSA accumulator to realize completely anonymous e-money transactions without introducing a new trusted party and changing the bitcoin security model in other ways.

Combining the ideas in [8] and [10], this paper proposes Zero-Cerd, a completely anonymous authentication scheme based on blockchain and dynamic accumulator. The main innovations of this paper are summarized as follows.

- Firstly, we propose a distributed identity authentication scheme based on blockchain, in which blockchain is used as a bulletin board to record public parameters, public keys, and related transaction information. Different from the currency transaction form of traditional blockchain, our scheme realizes identity authentication through credential transactions.
- Secondly, by using accumulator and zero-knowledge proof technology, users can independently convert their credentials and prove the legitimacy of their credentials. At the same time, the corresponding credential information is not exposed in the showing phase.
- Finally, we use the dynamic accumulator as the credential revocation manager. In this scheme, the dynamic accumulator contains all valid user information. When credential authority (CA) revokes a user's credential, the accumulator value will be updated, and each legitimate user can update his evidence independently. It can simplify the management of revocation in the scheme.

The remainder of the paper is organized as follows. In Section II, we present the related work. The preliminaries are given in Section III, the system model and formal definition in Section IV. Section V describes the proposed system and analyzes the security of our system. In Section VI, we make comparisons and performance evaluations of our system. The last Section is the conclusion.

II. Related Work

There is a sequence of researches regarding anonymous identity authentication such as [11]–[21].

In 2004, Camenisch *et al.* [11] introduced an authentication scheme with weak anonymity and attribute privacy through randomization technology but the size of credential increases linearly with the number of attributes, and do not provide the selective revocation. Yang *et al.* [12] proposed a lightweight anonymous entity authentication scheme with revocation but they did not focus on the privacy of single attribute. Ruj *et al.* [13] proposed a decentralized access control technique with anonymous authentication based on attribute-based encryption, which provides user revocation and prevents replay attacks. One disadvantage is that the access policy is public, which will cause certain privacy disclosure. Kumar *et al.* [14] proposed a lightweight anonymous authentication scheme. In their scheme, identity anonymity is realized by using symmetric encryption, which will lead to serious symmetric key maintenance problems. Jia *et al.* [15] introduced an efficient identity-based anonymous authentication protocol for the privacy problem in mobile edge computing, and formally proved the security of their protocol. However, the protocol does not consider the problem of key management. Wang *et al.* [16] designed an anonymous authentication scheme by combining an identity mixer scheme [17] with cryptography components such as zero-knowledge proof. The anonymity of the scheme is reflected in: when the user presents the credential, the verifier can specify the user to show the corresponding attributes and hide the attribute values that do not need to be presented. However, the scheme does not realize the function of complete anonymity. Sonnino *et al.* [18] proposed a selective disclosure credential scheme, which integrates with blockchains to ensure confidentiality, authenticity, and availability. Unfortunately, the scheme does not address the issue of credential revocation. Yu *et al.* [19] proposed an anonymous authentication scheme BASS based on blockchain combined with cryptographic technologies such as dynamic accumulator, digital signature, and zero-knowledge proof. In the scheme, the blockchain is used to record necessary records such as public parameters, public keys, and credential revocation lists. CA can selectively revoke user credentials according to the actual situation. There are

many rounds of interaction in the credential issuance process, and the execution efficiency needs to be improved.

At present, references [22]–[24] use the special properties of group signature or ring signature to construct anonymous authentication schemes. The idea is that individuals sign on behalf of groups. The verifier can verify that the message is signed by a member of the group, but cannot know the specific member, so as to realize the function of anonymity of the signer. However, the computational complexity of these schemes is high and their efficiency needs to be improved.

III. Preliminaries

In this section, we showcase the associated basic knowledge. See Table 1 for the notations used herein.

Table 1. Notation description

Notations	Descriptions
G_1, G_2, G_T	Three cyclic multiplicative groups
$\mathbb{U} = \{u_1, u_2, \cdots, u_n\}$	The user's identification set
λ	A security parameter
(pk_{u_i}, sk_{u_i})	User's key pair registered in blockchain
(pk, sk)	CA's key pair
Δ	An accumulator maintained by the CA
Δ'	An accumulator calculated by the DU
ω	A witness against accumulator Δ
ω'	A witness against accumulator Δ'
CRL	A credential revocation list
$E(\cdot)$	Encryption algorithm
H	A collision-free hash function
σ	A credential issued by the CA
π	A zero-knowledge proof of knowledge

1. Blockchain

Blockchain was originally known as the underlying technology of Bitcoin. It was not until 2015 that blockchain became a prominent concept by researchers. Consisting of peer-to-peer (P2P) network, consensus protocol, transaction, smart contract, and a series of other technologies, blockchain can provide a trusted and distributed network environment. This new technology has solved the security risks brought by the centralization model. Applications based on blockchain technology can provide a new direction to reduce the middleman role.

2. Bilinear groups

Let $\mathcal{G}(1^\kappa)$ be a group generation algorithm and κ denotes a security parameter. The algorithm outputs public parameters $G = (G_1, G_2, G_T, e(\cdot,\cdot))$, such that G_1, G_2, and G_T are three multiplicative cyclic groups with the same order q. $e : G_1 \times G_2 \to G_T$ denotes a computable bilinear map that satisfies the following properties:

- Bilinearity. $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, for all $a, b \leftarrow_R \mathbb{Z}_N^*$ and $g_1 \leftarrow_R G_1, g_2 \leftarrow_R G_2$;
- Non-degeneracy. $e(g_1, g_2) \neq 1$;
- Computability. Given the elements $g_1 \leftarrow_R G_1$, $g_2 \leftarrow_R G_2$, $e(g_1, g_2)$ can be computed efficiently.

3. Zero-knowledge proof of knowledge

The definition of zero-knowledge proof is that the prover can make the verifier believe that a statement is correct without providing any useful information to the verifier. The zero-knowledge proof used in our protocol can be instantiated using the technique of Schnorr [25]. For instance, let $\text{ZKPoK}(x) : y = g^x$ denotes a ZKPoK protocol that proves the knowledge of $x \in Z_q$ such that $y = g^x$. More complex relation instances can be proved, e.g., $\text{ZKPoK}(x, y) : h = g^x \wedge c = g^y$ denotes a zero-knowledge proof of knowledge of the elements x and y that satisfy both $h = g^x$ and $c = g^y$. By using the Fiat-Shamir heuristics [26], we can convert a ZKPoK protocol to be noninteractive.

4. Accumulators

Accumulators were introduced by Benaloh and Mare [27] as a way to combine a set of values into one short accumulator, such that there is a short witness that a given value was incorporated into the accumulator. In this paper, we use the pairing-based dynamic accumulators in [28]. Set g_2 as generators of G_2, $\hat{g} \in G_1$, $\hat{Y} = g_2^y$ for $y \in Z_q$. For a set of values $(k_1, \ldots, k_n)$, the accumulator is computed by $\Delta = \hat{g}^{\prod_{i=1}^{n}(y+k_i)}$. At the same time, we can compute a witness $\omega_i = \Delta^{\frac{1}{y+k_i}}$ for value k_i, such that $e(\Delta, g_2) = e(\omega_i, \hat{Y} g_2^{k_i})$. We can prove k_i is accumulated in Δ without revealing any information about k_i and ω_i by use of a zero-knowledge proof of knowledge. The proof is denoted by

$$\text{ZKPoK}\{(k_i, \omega_i) : e(\Delta, g_2) = e(\omega_i, \hat{Y} g_2^{k_i})\}$$

5. Pedersen commitment scheme

Pedersen commitment [29] is based on discrete logarithm problem, which allows one party to generate a commitment to a secret message while keeping it hidden. The specific calculation process is as follows.

Let g and h be elements of G such that nobody knows $\log_g h$. In order to commit to a message m, the committer chooses a value, $r \in Z_q$, at random and computes the commitment $C = g^m h^r$ and sends it to the receiver. When the committer is required to reveal the message committed, the committer reveals the values m and r which are used by the receiver to compute $g^m h^r$ and compare it to the previously received C.

A Pedersen commitment scheme has two properties: binding and hiding. The binding property ensures that the committing party cannot change a commitment already made. The hiding property ensures that the commitment does not reveal any information about the committed secret.

IV. System Model and Formal Definition

1. System model

Zero-Cerd involves four entities: credential authority (CA), data owner (DO), data user (DU), and blockchain as shown in Fig.1.

CA: The CA is responsible for establishing the system, generating system public parameters, issuing credentials to legitimate users, and publishing the public information to the blockchain.

DU: A DU can obtain public parameters on blockchain and interact with CA to obtain its credential. To realize anonymous authentication, DU can hide their credentials through the Blind algorithm and prove to DO that they have legal credentials.

DO: A DO can obtain public parameters on blockchain and interact with DU to verify the legitimacy of their credentials. When the credential is verified, DO can provide corresponding resource services to DU.

Blockchain: In our scheme, the blockchain is regarded as a bulletin board for recording some public parameters, public keys, and encrypted information.

2. Formal definition of the Zero-Cerd

Zero-Cerd consists of Setup, CAKeygen, Grant, Blind, Showing, Verify, and Revocation algorithms. The specific process is as follows.

Setup$(1^\lambda) \to (params)$. It is run by the CA and takes a security parameter λ as input and outputs the public parameters $params$.

CAKeygen$(params) \to (\Delta, pk, sk, \text{CRL})$. It is run by the CA and takes params as input and outputs the initial accumulator Δ, a key pair (pk, sk), and an empty credential revocation list CRL.

Grant$(params, u_i) \to (\sigma)$. It is run by the CA and takes $params$, sk, and DU's identification u_i as input and outputs the DU's credential σ.

Blind$(\sigma, params) \to (c, skc)$. It is run by the DU and takes $params$ and σ as input and outputs a commitment c of a new credential, as well as a trapdoor skc.

Showing$(params, c, skc) \to (\pi)$. It is run by the DU and takes $params$, commitment c, trapdoor skc as input and outputs a proof π of possession a valid cre-

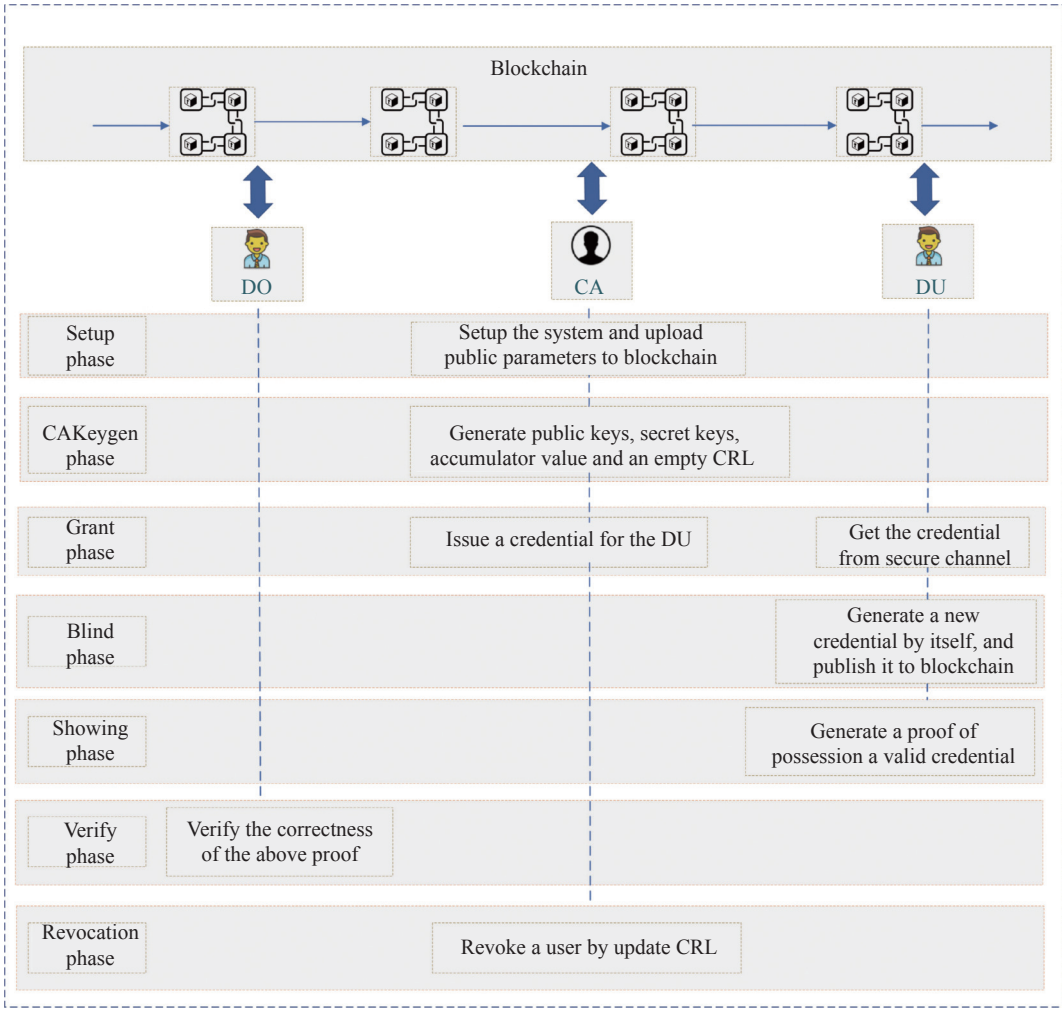


Fig. 1. Components of Zero-Cerd.

dential.

Verify$(params, c, \pi, \Delta) \rightarrow \{0,1\}$. It is run by the DO to verify a credential proof π. It takes *params*, c, π, Δ as input and outputs 1 if the credential is valid. Otherwise outputs 0.

Revocation$(\mathrm{CRL}, u_j) \rightarrow (\mathrm{CRL})$. It is run by the CA and takes *params*, CRL, u_j as input and outputs a new CRL. At the same time, CA updates the accumulator Δ.

3. Security requirements

The security of the Zero-Cerd system is defined by the following definition.

We first describe the anonymity experiment, which ensures that the adversary cannot link a given credential to the credential associated with it, even when the attacker provides many of the credentials used in the showing phase.

Anonymity: A Zero-Cerd system satisfies the anonymity requirement if every probabilistic polynomial time adversary has a negligible advantage in the following experiment.

- Setup. The challenger runs the Setup algorithm and returns parameters to the adversary.
- Phase 1. The challenger takes parameters as input and runs the Blind algorithm. Then, it outputs (c_b, skc_b), where $b \in \{0,1\}$.
- Challenge. The adversary takes $(params, c_0, c_1)$ as input and outputs a commitment set C. The challenger takes $(params, c_i, \mathrm{skc}_i, C \cup \{c_0, c_1\})$ as input, generates a proof π, and returns the proof π to the adversary.
- Guess. The adversary outputs a guess, b' of b. If $b = b'$, then the challenger returns 1; otherwise returns 0.

We define the adversary's advantage in the above game as $|Pr[b = b'] - \frac{1}{2}|$. Anonymity definition states that given two blind credential and one proof, one cannot do much better than guess which blind credential was showing.

Next, we define other security objectives.

Credential soundness: A malicious user cannot convince an honest verifier that he has a credential if he does not own it.

Credential revocation: In the Zero-Cerd system, CA can revoke the user's identity to ensure that the credential is invalid.

V. The Specific Process of the Zero-Cerd

1. Main idea

Among the known solutions to the authentication and revocation problem, the dynamic accumulator is one of the most promising solutions, which has excellent communication complexity. Moreover, when combined with zero-knowledge proof, it provides an ideal solution for anonymous authentication.

The construction idea of Zero-Cerd is inspired by [10]. We assume that all users share a bulletin board, that is, blockchain. A DU can initially obtain an original authentication credential from CA. To achieve anonymous authentication, DU needs to run a Blind algorithm to generate a new credential Zero-Cerd. It first selects two random numbers e, r and generates the commitment value c of the two random numbers, where e represents a new credential and r is a trapdoor. DU publishes c to the bulletin board and consumes the original authentication credential at the same time. In the authentication stage, DU uses the dynamic accumulator and zero-knowledge proof technology to prove that he does master the legal credential without exposing any information on the one hand and that his original credential is still valid without being revoked by CA on the other hand. Specifically, DU first produces a zero-knowledge proof π_1 for the two statements: 1) DU knows an e that is included in the global accumulator Δ' and 2) DU has a trapdoor that opens commitment c. Then, DU continues to generate a zero-knowledge proof π_2 for the statements: its original credential σ has not been revoked.

In our scheme, the user can only give value to the Zero-Cerd by consuming the original credential. Even if the user's original credential has any taints, it cannot be associated with the Zero-Cerd.

2. Our construction

We now describe the concrete Zero-Cerd scheme.

Setup$(1^\lambda) \rightarrow (params)$. Based on a security parameter 1^λ, the CA generates cyclic groups G_1, G_2, G_T with order q. Let $e : G_1 \times G_2 \rightarrow G_T$ be a bilinear map. Set g_1 and g_2 as generators of G_1 and G_2, respectively, and select collision-free hash function $H : \{0,1\}^* \rightarrow Z_q$. Let $\mathbb{U} = \{u_1, u_2, \ldots, u_n\}$ represent the DU's identification set, where n denotes the number of users. Then, CA puts the public parameters $(q, G_1, G_2, G_T, e, g_1, g_2, \mathbb{U})$ on the blockchain.

CAKeygen$(params) \rightarrow (\Delta, pk, sk, \mathrm{CRL})$. The CA takes the public parameters as input and randomly chooses $x, y, z \in Z_q$, $\hat{g} \in G_1$ to compute $pk = (g_2, g_2^x, g_2^z)$, the accumulator $\Delta = \hat{g}^{(y+u_1)\cdots(y+u_n)}$ and $Y = g_2^y$. The CA generates an empty credential revocation list CRL and puts $(pk, Y, \hat{g}, \Delta, \mathrm{CRL} = \varnothing)$ on the blockchain. The $sk = \{x, y, z\}$ is kept secretly by CA.

Grant$(params, sk, u_i) \rightarrow (\sigma)$. In this phase, CA issues credential for the DU. It randomly chooses $h \in Z_q$ and computes credential $\sigma = (\sigma_1, \sigma_2) = (g_1^h, g_1^{h\cdot(x+z\cdot u_i)})$ and witness $\omega_i = \Delta^{\frac{1}{y+u_i}}$ of u_i. It sends $\{\sigma, w_i\}$ to DU.

Blind$(\sigma, params) \rightarrow (c, skc)$. DU checks if $e(\sigma_1, g_2^x \cdot g_2^{z\cdot u_i}) = e(\sigma_2, g_2)$ holds to verify the validity of the credential. Then, DU randomly chooses $e_i, r_i \in Z_q$, and

computes $c = g_1^{e_i}\hat{g}^{r_i}$, where e_i represents a new credential for u_i and c represents a commitment of e_i and r_i. DU embeds c in the output of a blockchain transaction that spends the original credential σ granted by CA and keeps $skc = (e_i, r_i)$ in secret.

Showing$(params, c, skc) \to (\pi)$. DU chooses an arbitrary set of credentials E. If $e_i \notin E$, output $\perp$. Otherwise, DU randomly chooses $y', s_i \in Z_q$ and computes accumulator $\Delta' = \hat{g}^{(y'+e_1)\cdots(y'+e_n)}$ and witness $\omega' = (\Delta')^{\frac{1}{y'+e_i}}$, $Y' = g_1^{y'}$, $C_{\omega'} = \omega' g_1^{\frac{s_i}{e_i+y'}}$. Then, it generates a proof $\pi_1 = \text{ZKPoK}_1\{(e_i, s_i, r_i, y', \omega') : c = g_1^{e_i}\hat{g}^{r_i} \wedge \Delta' = (C_{\omega'})^{e_i+y'}(\frac{1}{g_1})^{s_i}\}$ as is shown in Table 2.

Table 2. ZKPoK$_1$

$\hat{g}, g_1, g_2, E, \Delta', Y', C_{\omega'}, C_{e_i}$		
Prover		Verifier
$r_\alpha, r_\beta, r_\varphi \in Z_q$		
$t_1 = g_1^{r_\alpha} \cdot \hat{g}^{r_\varphi}$		
$t_2 = C_{\omega'}^{r_\alpha} \cdot (\frac{1}{g_1})^{r_\beta}$		
$\eta = H(C_{\omega'}, t_1, t_2)$		
$s_\alpha = r_\alpha - \eta \cdot (e_i + y')$		
$s_\beta = r_\beta - \eta \cdot s_i$		
$s_\varphi = r_\varphi - \eta \cdot r_i$	$\xrightarrow[s_\alpha, s_\beta, s_\varphi]{t_1, t_2}$	Verify
		$t_1 = c^\eta \cdot Y'^\eta \cdot g_1^{s_\alpha} \cdot \hat{g}^{s_\varphi}$
		$t_2 = \Delta'^\eta \cdot C_{\omega'}^{s_\alpha} \cdot (\frac{1}{g_1})^{s_\beta}$

DU has to spend its original credential σ_i to give itself the validity of the newly generated credential e_i. At the same time, it generates a proof π_2 to prove that its original credential σ_i has not be revoked. DU randomly chooses $\phi \in Z_q$ to compute $S_i = Y^\phi$ and generates a proof $\pi_2 = \text{ZKPoK}_2\{(\phi, u_i, \omega_i) : S_i = Y^\phi \wedge e(\Delta, g_2) = e(\omega_i, Y g_2^{u_i})\}$ as shown in Table 3. Before sending proof π_2 to the verifier, the prover needs to do a conversion operation as in Table 4. Then, π_2 can be transformed into $\pi_2' = \text{ZKPoK}_2'\{(\kappa, r_w, u_i, \omega_i) : a = Y^{r_w} \wedge \frac{e(d,Y)}{e(\Delta,g_2)} = \frac{e(g_1,a)\cdot e(g_1,g_2)^\kappa}{e(d,g_2)^{u_i}}\}$.

Table 3. ZKPoK$_2'$

$\hat{g}, g_1, g_2, Y, S_i, \Delta$		
Prover		Verifier
$\rho_w, \rho_u, \rho_\kappa \in Z_q$		
$T_1 = Y^{\rho_w}$		
$T_2 = \frac{e(g_1,g_2)^{\rho_\kappa}}{e(d,g_2)^{\rho_u}}$		
$\eta' = H(T_1, T_2, S_i)$		
$s_w = \rho_w + \eta' \cdot r_w$		
$s_\kappa = \rho_\kappa + \eta' \cdot \kappa$		
$s_u = \rho_u + \eta' \cdot u_i$	$\xrightarrow{T_1, T_2, s_w, s_\kappa, s_u}$	Verify
		$Y^{s_w} = T_1 \cdot a^{\eta'}$
		$\frac{e(g_1,g_2)^{s_\kappa}}{e(d,g_2)^{s_u}} = T_2 \cdot \left(\frac{e(d,Y)}{e(\Delta,g_2)\cdot e(g_1,a)}\right)^{\eta'}$

Table 4. Transfer

g_1, g_2, Y, S_i, Δ	
Prover	Verifier
$r_w \in Z_q$	
$a = Y^{r_w}, d = \omega_i g_1^{r_w}$	
$\kappa = r_w \cdot u_i$	

Finally, DU outputs the values $(\pi_1, \pi_2, \Delta', E)$.

Verify$(params, c, \pi_1, \pi_2, E, \Delta) \to \{0, 1\}$. DO verifies the proof π_1, π_2 by using $params$, outputs 1 if π_1, π_2 is valid. Otherwise output 0.

Revocation$(\text{CRL}, u_j) \to (\text{CRL})$. To revoke a user u_j, CA updates CRL with u_j, where $\text{CRL} = \text{CRL} \cup \{u_j\}$. At the same time, CA computes a new accumulator $\Delta^{\text{new}} = \Delta^{\frac{1}{y+u_j}}$

3. Correctness analysis

For every user i $(i \neq j)$ who can use personal original witness ω_i and new accumulator Δ^{new} to compute a new personal new witness ω_i^{new}. It computes a new witness as follows:

$$\begin{aligned}\omega_i^{\text{new}} &= \omega_i^{\frac{1}{y+u_j}} \\ &= \left(\Delta^{\frac{1}{y+u_i}}\right)^{\frac{1}{y+u_j}} \\ &= \left(\frac{\Delta^{\frac{1}{y+u_i}}}{\Delta^{\frac{1}{y+u_j}}}\right)^{\frac{1}{u_j-u_i}} \\ &= \left(\frac{\omega_i}{\Delta^{\text{new}}}\right)^{\frac{1}{u_j-u_i}}\end{aligned}$$

Obviously, except for the revoked user u_j, other users have the ability to compute new witnesses alone and generate valid proof π_2.

The DO verifies the ZKPoK$_1$ as follows:

$$\begin{aligned}t_1 &= c^\eta \cdot Y'^\eta \cdot g_1^{s_\alpha} \cdot \hat{g}^{s_\varphi} \\ &= (g_1^{e_i} \cdot \hat{g}^{r_i})^\eta \cdot g_1^{y'\cdot\eta} \cdot g_1^{s_\alpha} \cdot \hat{g}^{s_\varphi} \\ &= g_1^{e_i\cdot\eta + s_\alpha + y'\cdot\eta} \cdot \hat{g}^{r_i\cdot\eta + s_\varphi} \\ &= g_1^{r_\alpha} \cdot \hat{g}^{r_\varphi}\end{aligned}$$

The verification of the equation shows that the DU does have e_i, r_i, y'. DO continues to verify the following equation.

$$\begin{aligned}t_2 &= \Delta'^\eta \cdot C_{\omega'}^{s_\alpha} \cdot \left(\frac{1}{g_1}\right)^{s_\beta} \\ &= (\omega')^{\eta\cdot(e_i+y')} \cdot \left(\omega' \cdot g_1^{\frac{s_i}{e_i+y'}}\right)^{s_\alpha} \cdot \left(\frac{1}{g_1}\right)^{s_\beta} \\ &= (\omega')^{\eta\cdot(e_i+y')+s_\alpha} \cdot g_1^{(\frac{s_i}{e_i+y'})\cdot s_\alpha} \cdot g_1^{-s_\beta} \\ &= (\omega')^{r_\alpha} \cdot g_1^{(\frac{s_i}{e_i+y'})\cdot r_\alpha} \cdot g_1^{-\eta\cdot s_i} \cdot g_1^{-s_\beta} \\ &= \left(\omega' \cdot g_1^{\frac{s_i}{e_i+y'}}\right)^{r_\alpha} \cdot \left(\frac{1}{g_1}\right)^{\eta\cdot s_i + s_\beta} \\ &= C_{\omega'}^{r_\alpha} \cdot \left(\frac{1}{g_1}\right)^{r_\beta}\end{aligned}$$

The verification of this equation shows that e_i is really accumulated to Δ' by DU.

Next, the DO verifies the ZKPoK$_2'$. The first verification process is as follows:

$$\begin{aligned} Y^{s_w} &= (g_2^y)^{\rho_w+\eta'\cdot r_w} \\ &= Y^{\rho_w}\cdot Y^{\eta'\cdot r_w} \\ &= T_1\cdot a^{\eta'} \end{aligned}$$

The verification of the equation shows that the DU does have r_w.

Obviously, the following equation holds.

$$e(d,Y)\cdot e(d,g_2)^{u_i} = e(\Delta,g_2)\cdot e(g_1,a)\cdot e(g_1,g_2)^{\kappa}$$

By transformation, we can obtain the following equation.

$$\frac{e(d,Y)}{e(\Delta,g_2)\cdot e(g_1,a)} = \frac{e(g_1,g_2)^{\kappa}}{e(d,g_2)^{u_i}}$$

Then, the second verification process is as follows:

$$\begin{aligned} T_2\cdot\left(\frac{e(d,Y)}{e(\Delta,g_2)\cdot e(g_1,a)}\right)^{\eta'} &= \frac{e(g_1,g_2)^{\rho_\kappa}}{e(d,g_2)^{\rho_u}}\cdot\frac{e(g_1,g_2)^{\kappa\cdot\eta'}}{e(d,g_2)^{\eta'\cdot u_i}} \\ &= \frac{e(g_1,g_2)^{s_\kappa}}{e(d,g_2)^{s_u}}. \end{aligned}$$

The verification of the equation shows that DU's original credential σ has not been revoked.

4. Security analysis

For a cryptographic protocol, it is necessary to first determine the security objectives to be achieved, such as the indistinguishability of the encryption scheme and the unforgeability of the signature scheme. Then it is necessary to construct a formal adversary model, and then reduce the attack on the cryptographic protocol to the attack on the known difficult problems by using probability theory and computational complexity theory. This is a general idea to prove the security.

The security of the Zero-Cerd system is defined by the following lemmas. The security goals including anonymity, credential soundness, revocation. The security properties of Zero-Cerd are derived from the security of dynamic accumulator [28] and Pedersen commitment [29]. In the process of security proof, the security attack on the Zero-Cerd system can be reduced to the attack on the commitment scheme and soundness of the ZKPoK.

Lemma 1 If the zero-knowledge proof of knowledge is computationally zero-knowledge, then our Zero-Cerd system satisfies the anonymity property.

Proof The Zero-Cerd system satisfies the anonymity requirement if every probabilistic polynomial time adversary has a negligible advantage in the following experiment.

- Setup. First, the challenger generates the system parameters $params = (q, G_1, G_2, G_T, e, g_1, g_2, \mathbb{U})$, where $\mathbb{U}$ represents the DU's identification set, and selects collision-free hash function $H : \{0,1\}^* \to Z_q$.
- Phase 1. The challenger takes parameters as input and randomly chooses $e_b, r_b \in Z_q$, and computes $c_b = g_1^{e_b}\hat{g}^{r_b}$, where c_b represents a commitment of e_b and r_b. Then, it output (c_b, skc_b), where $skc_b = (e_b, r_b)$ and $b \in \{0,1\}$.
- Challenge. The adversary takes $(params, c_0, c_1)$ as input and outputs a commitment set C. The challenger takes $(params, c_b, skc_b, C \cup \{c_0, c_1\})$ as input, generates a proof π, where the generation process of π refers to the above showing algorithm. Then, the challenger returns the proof π to the adversary.
- Guess. The adversary outputs a guess, b' of b. If $b = b'$, then the challenger returns 1; otherwise returns 0.

The security of our system stems from the fact that the commitment c is a perfectly-hiding commitment and the proof π is at least computationally zero-knowledge.

Note that, all values in the security game process provided to the adversary are distributed as in the real protocol with all but negligible probability. Moreover, all are independent of the bit b. The advantage of adversary $|Pr[b = b'] - \frac{1}{2}|$ is negligible.

Lemma 2 Zero-Cerd achieves credential soundness if ZKPoK$_1$ and ZKPoK$_2$ are sound.

Proof In the showing phase, DU computes the related tuples using $params, c, \mathrm{skc}$, random elements and produces two proofs, ZKPoK$_1$ and ZKPoK$_2$, that prove the validity of the DU's credential. The soundness property of ZKPoK$_1$ and ZKPoK$_2$ ensures that if a user can generate ZKPoK$_1$ and ZKPoK$_2$ that can pass the verification, then there exists an extract algorithm that outputs the witness.

Lemma 3 Zero-Cerd achieves credential revocable if ZKPoK$_2$ is sound.

Proof In the Zero-Cerd system, the CA is responsible for maintaining the CRL. When a user u_j is revoked, the CA updates the CRL list with $\mathrm{CRL} = \mathrm{CRL} \cup u_j$. At the same time, CA computes a new accumulator $\Delta^{\mathrm{new}} = \Delta^{\frac{1}{y+u_j}}$. Only users who have not been revoked can use personal original witness ω_i and new accumulator Δ^{new} to compute a new personal new witness ω_i^{new} and then generate a valid ZKPoK$_2$. The calculation process is described above.

The soundness property of ZKPoK$_2$ ensures that if a user can generate a ZKPoK$_2$ that can pass the verification, then there exists an extract algorithm that out-

puts the witness.

VI. Performance Analysis and Comparison

In this section, we implement Zero-Cerd to analyze the efficiency of the algorithm.

1. Complexity analysis

The algorithm complexity analysis of Zero-Cerd is shown in Table 5. The exponentiation operation and multiplication operation in G_1 and G_2 are denoted by E_1, E_2, M_1, and M_2, respectively. The pairing operation, exponentiation operation, and multiplication operation in G_T group are denoted by P, F, and T, respectively.

Table 5. Complexity analysis of Zero-Cerd

Algorithm	Computation cost
CA Keygen	$1E_1 + 3E_2$
Grant	$3E_1$
Blind	$2E_1 + 2E_2 + 1M_1 + 1M_2 + 2P$
Showing	$9E_1 + 3E_2 + 4M_1 + 2P + 1F$
Verify	$7E_1 + 2E_2 + 5M_1 + 1M_2 + 5P + 5F + 4T$
Revocation	$1E_1$

2. Efficiency evaluation

We implement Zero-Cerd on Intel Xeon(R) Gold 5118 CPU 2.30 GHz and 4.00 GB RAM with Ubuntu 20.04.3 LTS operating system. We run the algorithm 10 times and then adopt the average value. Table 6 shows the execution time of Zero-Cerd.

Table 6. Efficiency evaluation of Zero-Cerd

Algorithm	Execution times (s)
Setup	0.000,124,4
CA Keygen	0.008,593,5
Grant	0.042,060,6
Blind	8.404,571,2
Showing	16.873,546,8
Verify	18.593,575,3
Revocation	0.029,407,5

We compare the performance of Zero-Cerd and BASS [19], and the comparison of the time cost is shown in Fig.2 and Fig.3. We can see that in the Grant, Showing, and Verify phases, the efficiency of Zero-Cerd is significantly better than that of BASS. This is because in the Grant phase, to achieve the purpose of privacy protection, the BASS scheme realizes the anonymous issuance of credentials by using algorithms such as zero-knowledge proof, blind signature, and unblind. The computational complexity of these algorithms is higher than that of Zero-Cerd. In the Showing and the Verify phases, the BASS scheme uses more multiplication, exponentiation, and pairing operations in the G_T group than the Zero-Cerd scheme. The efficiency of other algorithms is basically the same, because there is not much calculation process in either scheme.

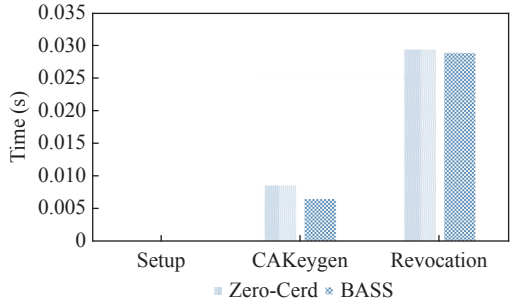


Fig. 2. Efficiency comparison (Setup, CAKeygen, Revocation).

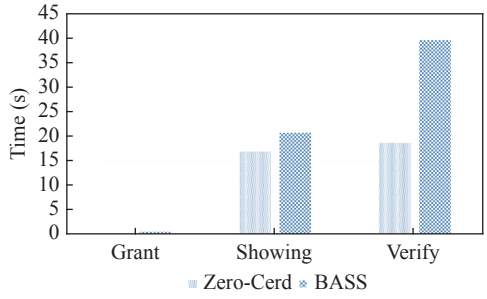


Fig. 3. Efficiency comparison (Grant, Showing, Verify).

3. Comparison with related works

We compare the Zero-Cerd with related work in terms of security properties and the credential size in Table 7. In terms of unlinkability, all the schemes compared have this property, so the attacker cannot distinguish whether the certificate originated from the same user in two sessions. As for the security feature of identity privacy, reference [12] does not consider it in its scheme. References [16], [17] need to present relevant attribute information according to the requirements of the verifier in the authentication process, so these two schemes are not completely private. In terms of revocation, references [11], [16]–[18] does not consider the issue of credential revocation, which will affect the practical application of the scheme. In [11], [16], [17], [19], the size of credential increases linearly with the number of attributes, while in other schemes, the credential size is constant. From the horizontal comparison, we can see that Zero-Cerd has advantages on the whole.

VII. Conclusions

Anonymous authentication technology can solve the contradiction between legitimacy and privacy in the authentication process. In this paper, we propose Zero-Cerd, a blockchain-based completely anonymous authentication scheme that supports revocation and credential soundness. We do theoretical analysis and simulation experiments to prove the security and enforceability of the scheme.

Table 7. Compared with related works

Scheme	Unlinkability	Identity privacy	Distributed ledgers	Revocation	Credential size
Camenisch *et al.* [11]	√	√	×	×	$O(m)$ elements
Yang *et al.* [12]	√	×	×	√	3 elements
Wang *et al.* [16]	√	◯	√	×	$O(m)$ elements
Camenisch [17]	√	◯	×	×	$O(m)$ elements
Sonnino *et al.* [18]	√	√	√	×	2 elements
Yu *et al.* [19]	√	√	√	√	$O(m)$ elements
Ours	√	√	√	√	2 elements

Note: m represents the number of attributes; ◯ represents partial privacy.

References

[1] S. Shang, X. Li, R. X. Lu, *et al.*, "A privacy-preserving multidimensional range query scheme for edge-supported industrial IoT," *IEEE Internet of Things Journal*, vol.9, no.16, pp.15285–15296, 2022.

[2] X. Li, J. B. He, P. Vijayakumar, *et al.*, "A verifiable privacy-preserving machine learning prediction scheme for edge-enhanced HCPSs," *IEEE Transactions on Industrial Informatics*, vol.18, no.8, pp.5494–5503, 2022.

[3] S. H. Zou, J. W. Xi, H. G. Wang, *et al.*, "CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Transactions on Industrial Informatics*, vol.16, no.6, pp.4206–4218, 2020.

[4] Y. Lu, Q. Tang, and G. L. Wang, "ZebraLancer: Private and anonymous crowdsourcing system atop open blockchain," in *Proceedings of the IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, pp.853–865, 2018.

[5] L. Q. Gong, D. M. Alghazzawi, and L. Cheng, "BCoT sentry: A blockchain-based identity authentication framework for IoT devices," *Information*, vol.12, no.5, article no.articleno.203, 2021.

[6] D. Tao, P. C. Ma, and S. Obaidat, "Anonymous identity authentication mechanism for hybrid architecture in mobile crowd sensing networks," *International Journal of Communication Systems*, vol.32, no.14, article no.e4099, 2019.

[7] H. Liu and M. G. Liang, "Efficient identity-based hierarchical access authentication protocol for mobile network," *Security and Communication Networks*, vol.6, no.12, pp.1509–1521, 2013.

[8] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new Blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol.9, no.18, pp.5943–5964, 2016.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Available at: *https://bitcoin.org/en/bitcoin-paper*, 2008.

[10] I. Miers, C. Garman, M. Green, *et al.*, "Zerocoin: Anonymous distributed E-cash from Bitcoin," in *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp.397–411, 2013.

[11] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Proceedings of the 24th Annual International Cryptology Conference*, Santa Barbara, CA, USA, pp. 56–72, 2004.

[12] Y. J. Yang, H. B. Cai, Z. Wei, *et al.*, "Towards lightweight anonymous entity authentication for IoT applications," in *Proceedings of the 21st Australasian Conference Information Security and Privacy*, Melbourne, Australia, pp.265–280, 2016.

[13] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol.25, no.2, pp.384–394, 2014.

[14] P. Kumar, A. Gurtov, M. Sain, *et al.*, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, vol.10, no.4, pp.4349–4359, 2019.

[15] X. Y. Jia, D. B He, N. Kumar, *et al.*, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Systems Journal*, vol.14, no.1, pp.560–571, 2020.

[16] Z. Wang, J. Fan, L. Cheng, *et al.*, "Supervised anonymous authentication scheme," *Journal of Software*, vol.30, no.6, pp.1705–1720, 2019.

[17] J. Camenisch, "Specification of the identity mixer cryptographic library", Version 2.3.4, Available at: *https://domino-oweb.draco.res.ibm.com/reports/rz3730_revised.pdf*, February 10, 2012.

[18] A. Sonnino, M. Al-Bassam, S. Bano, *et al.*, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," in *Proceedings of the 26th Annual Network and Distributed System Security Symposium*, San Diego, CA, USA, 2019.

[19] Y. Yu, Y. Q. Zhao, Y. N. Li, *et al.*, "Blockchain-based anonymous authentication with selective revocation for smart industrial applications," *IEEE Transactions on Industrial Informatics*, vol.16, no.5, pp.3290–3300, 2020.

[20] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Transactions on Smart Grid*, vol.10, no.4, pp.3953–3962, 2019.

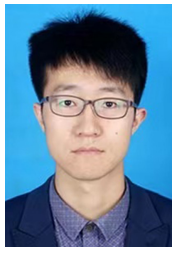
[21] K. Mahmood, X. Li, S. A. Chaudhry, *et al.*, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol.88, pp.491–500, 2018.

[22] H. B. Zheng, Q. H. Wu, B. Qin, *et al.*, "Linkable group signature for auditing anonymous communication," in *Proceedings of the 23rd Australasian Conference on Information Security and Privacy*, Wollongong, Australia, pp.304–321, 2018.

[23] J. Zhao, J. Q. Liu, Z. Qin, *et al.*, "Privacy protection scheme based on remote anonymous attestation for trusted smart meters," *IEEE Transactions on Smart Grid*, vol.9, no.4, pp.3313–3320, 2018.

[24] L. C. Ma, X. F. Liu, Q. Q. Pei, *et al.*, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," *IEEE Transactions on Services Computing*, vol.12, no.5, pp.786–799, 2019.

[25] C. P. Schnorr, " Efficient signature generation by smart cards," *Journal of Cryptology*, vol.4, no.3, pp.161–174, 1991.
[26] A. Fiat and A. Shamir, " How to prove yourself: Practical solutions to identification and signature problems," in *Proceedings of the 6th Conference on the Theory and Application of Cryptographic Techniques*, Santa Barbara, CA, USA, pp.186–194, 1987.
[27] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures (extended abstract)," in *Workshop on the Theory and Application of Cryptographic Techniques*, Lofthus, Norway, pp.274–285, 1993.
[28] L. Nguyen, " Accumulators from bilinear pairings and applications," in *Cryptographers' Track at the RSA Conference*, San Francisco, CA, USA, pp.275–292, 2005.
[29] T. P. Pedersen, " Non-interactive and information-theoretic secure verifiable secret sharing," in *Proceedings of the 11th Annual International Cryptology Conference*, Santa Barbara, CA, USA, pp.129–140, 1991.



YANG Kunwei received the M.S. degree in computer software and theory from the Shaanxi Normal University, in 2015. He is currently an Engineer with the School of Computer Science, Shaanxi Normal University, China. His research interests include access control and identity authentication.
(Email: yangkunwei@snnu.edu.cn)

YANG Bo (corresponding author) was born in 1963. He received the Ph.D. degree in cryptography from Xidian University. He is a Professor of Shaanxi Normal University. His research interests include information security and cryptography.
(Email: byang@snnu.edu.cn)

WANG Tao was born in 1980. He received the Ph.D. degree from the Northwestern Polytechnical University in 2012. He is currently an Associate Professor with School of Computer Science, Shaanxi Normal University, China. His current research interests include information security and computer network.
(Email: water@snnu.edu.cn)

ZHOU Yanwei was born in 1986. He received the B.E. degree in computer systems organization from Shaanxi Normal University. He is a Ph.D. candidate of Shaanxi Normal University. His research interests include anonymous communication and cryptography.
(Email: zyw@snnu.edu.cn)