SkyEye: A Traceable Scheme for Blockchain

Tianjun Ma†‡§, Haixia Xu†‡§*, Peili Li†§

†State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China
‡School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
§Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China

{matianjun,xuhaixia,lipeili}@iie.ac.cn

Abstract—Many studies focus on the blockchain privacy protection. Unfortunately, the privacy protection brings regulatory issues (e.g., countering money-laundering). Tracing users’ identities is a critical step in addressing blockchain regulatory issues. In this paper, we propose SkyEye, a traceable scheme for blockchain. SkyEye can be applied to the blockchain applications that satisfy the following conditions: (I) The users have public and private information, where the public information is generated by the private information; (II) The users’ public information is disclosed in the blockchain data. SkyEye enables the regulator to trace users’ identities. The design of SkyEye leverages some cryptographic primitives, including chameleon hash and zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK). Moreover, we demonstrate the security of SkyEye under specific cryptographic assumptions. Finally, we implement two prototypes of SkyEye, and evaluate the running time and related data storage requirements by performing the aforementioned prototypes.

I. INTRODUCTION

The blockchain was first introduced in Bitcoin [29], and quickly became the supporting technology of decentralized cryptocurrencies such as Litecoin [1], PPcoin [23], and Nextcoin [3]. The blockchain integrates multiple technologies (e.g., cryptography and peer-to-peer networking) and includes a variety of features: distributed, decentralized, anonymity, transparency, and so on. Today, the blockchain is not only applied in decentralized cryptocurrencies, but also has broad applications in other fields, including defense, finance, and smart contract.

The blockchain can be considered a distributed database that only appends data (e.g., transactions). The data is stored in the block that contains the block header and block body. Every block header includes the hash of the previous block, forming a chain. The strategy of appending a block to the blockchain uses a consensus mechanism such as proof of work (POW) [29], proof of stake (POS) [6], [14], [22], or practical byzantine fault tolerance (PBFT) [11]. In many blockchain applications, every user generally has public/private information (e.g., the public key address and the signature private key for each user in Bitcoin [29], more details about the public/private information are described in Section II-A).

Many studies focus on the blockchain privacy protection [8], [32]. Unfortunately, the privacy protection brings regulatory issues. On one hand, if a user’s private information is lost or stolen, the user loses control of the data corresponding to the private information forever. For example, if the Bitcoin’s user loses the signature private keys in his wallet, there is no way to recover the coins in this wallet. In other words, the user loses the coins controlled by these signature private keys forever. On the other hand, strong privacy protection in the blockchain facilitates many criminal activities (e.g., ransomware [2], money laundering). CipherTrace’s second quarter 2019 cryptocurrency anti-money laundering report shows that the total amount of funds that cybercriminals directly steal, scam, and misappropriate from users and trading platforms is approximately $4.3 billion in aggregate for 2019. These regulatory issues not only present a serious threat to the interests of users, but also have seriously hindered the development and application of the blockchain.

We stress that tracing users’ identities is a critical step in addressing blockchain regulatory issues. When each user’s identity in the blockchain data is determined, the regulator can conduct some regulatory operations (such as Big Data analysis) to decide who should be punished or who should own the lost data. Although there has been progress in designing traceable mechanisms, such as zkLedger [30] and several others [5], [15], [18], [21], these approaches are designed for specific application environments and do not seem to have been extended to other applications; see Section VIII for more details.

A. Contributions

The main contributions of this paper are the following.

First, we introduce the notion of a traceable scheme for blockchain and formalize the security properties to be satisfied, namely identity proof indistinguishability and identity proof unforgeability.

Second, we propose SkyEye, a traceable scheme for blockchain. SkyEye can be applied to the blockchain applications that satisfy the following conditions: (I) The users have public and private information, where the public information is generated by the private information; (II) The users’ public information is disclosed in the blockchain data. These blockchain applications are called the SkyEye-friendly blockchain applications. SkyEye requires the user to register only once, and enables the regulator to trace users’ identities. In our design strategy, we add identity proofs, associated with the users’ private information, to the blockchain data. SkyEye is designed by using some cryptographic primitives (including chameleon hash [25] and zk-SNARK [19]). In
addition, we demonstrate the security of SkyEye under specific cryptographic assumptions.

Finally, we implement two prototypes of SkyEye: SkyEye$_{HE}$ and SkyEye$_S$. These correspond to the two primary ways of generating public and private information in the blockchain applications. The first way is through a pseudorandom function, and the second way is using elliptic curve scalar multiplication. We evaluate the running time and related data storage requirements by performing SkyEye$_{HE}$ and SkyEye$_S$. Our evaluation results illustrate that using an i7 processor, a 16 GB RAM desktop machine, and a Merkle tree depth of 34, the time taken by a verifier to verify a user’s identity proof is nearly 4.6 ms in the first way and less than 25 ms in the second way.

B. Paper Organization

The remainder of this paper is organized as follows. Section II provides the background. Section III provides key ideas in SkyEye design and an overview of SkyEye. Section IV defines the algorithm and security of the traceable scheme for blockchain. Section V details SkyEye. Section VI describes our implementation and the evaluation results. We discuss remaining issues of SkyEye and future work in Section VII. We discuss related work in Section VIII and summarize this paper in Section IX.

II. BACKGROUND

A. SkyEye-friendly blockchain applications

We use $B_s$ to denote SkyEye-friendly blockchain applications. Next, we describe the blockchain data in $B_s$ and an overview of $B_s$.

1) The Blockchain Data in $B_s$: $B_s$ satisfies two conditions: (I) The users have public and private information, where the public information is generated by the private information; (II) The users’ public information is disclosed in the blockchain data.

We use equation $pub = gen(priv)$ to describe the generation relation in the condition (I), where $pub$ denotes the public information, $priv$ denotes the private information, and $gen(\cdot)$ denotes the generation algorithm between $pub$ and $priv$, which has one-wayness, i.e., it is easy to compute $pub$ using the private information $priv$ but is hard to invert. In many blockchain applications, every user generally has private information that corresponds to public information. For example, the public key address and the signature private key in Bitcoin [29] are the user’s public/private information.

In Zerocash [8], $(sn, (a_{sk}, \rho))$ is the user’s public/private information, where $sn$ is the serial number, $a_{sk}$ is the address private key, and $\rho$ is the random number used to generate the serial number. The public information is generated by the private information via a cryptographic method, such as the pseudorandom function, or elliptic curve scalar multiplication.

According to the condition (II), the blockchain data in $B_s$ can be divided into two parts: one part is the users’ public information, such as the input/output addresses in Bitcoin [29], and the other part is the data contents, such as the payment amount and the executable contract code. Therefore, the blockchain data in $B_s$ can be represented as the equation $data_{B_s} = [(pub_i)_{i \in \{1, \ldots, n\}}, C]_{crytool}$, where $(pub_i)_{i \in \{1, \ldots, n\}}$ denotes the set of the users’ public information, $n$ is the number of the users’ public information in the blockchain data, $C$ denotes the data contents, and $crytool$ denotes the cryptographic tools (e.g., digital signature) that guarantee blockchain features such as tamper-resistance and privacy protection.

For example, Bitcoin [29], Ethereum [34], and RScoin [13] are the applications that belong to $B_s$. In these blockchain applications, the public key address and the signature private key are the user’s public/private information, where the public key address is generated by the signature private key. Moreover, the user’s public key address is disclosed in the blockchain data.

2) $B_s$: An overview of $B_s$ is shown in Figure 1. In (1) and (2), the user generates the $(pub, priv)$, and publishes $pub$ to the node network. In (3), for creating data, the user obtains others’ $(pub_i)_{i \in \{1, \ldots, n\}}$ from the node network. In (4), the user creates $data_{B_s} = [(pub_i)_{i \in \{1, \ldots, n\}}, C]_{crytool}$, where the $pub_i$ denotes the user’s $pub$, and publishes $data_{B_s}$ to the node network. In (5) and (6), a verifier receives $data_{B_s}$ from the node network and verifies data contents. If the verification is successful, $data_{B_s}$ is valid and is added to the block generated by the verifier. In (7), the block is published in the node network by the verifier. In (8), according to a consensus mechanism, the nodes in the network select a final block and add it to the blockchain.

B. Cryptographic Preliminaries

The cryptographic building blocks in our construction include the following: chameleon hash scheme, zk-SNARK, and public key encryption. Below, we informally describe these notions.

Chameleon hash scheme. Compared with the traditional hash scheme, the chameleon hash scheme has a special property: the user who knows the trapdoor can easily find collision. A chameleon hash scheme $Chash = (G_{chash}, K_{chash}, H_{chash}, C_{F_{chash}})$ is described below:

- $G_{chash}(\lambda) \rightarrow ppc_{chash}$. Given a security parameter $\lambda$, $G_{chash}$ returns the public parameters $ppc_{chash}$.

Fig. 1: Overview of $B_s$. 
\( K_{chash}(pp_{chash}) \rightarrow (pk_{chash}, sk_{chash}) \). Given the public parameters \( pp_{chash} \), \( K_{chash} \) returns a pair of public/private keys \((pk_{chash}, sk_{chash})\), where \( sk_{chash} \) is also known as the trapdoor.

\( \mathcal{H}_{chash}(pk_{chash}, m, r) \rightarrow CH \). Given the public key \( pk_{chash} \), a message \( m \), and a random number \( r \), \( \mathcal{H}_{chash} \) returns a chameleon hash \( CH \) about \( m \).

\( CF_{chash}(sk_{chash}, m, m', r) \rightarrow r' \). Given the trapdoor \( sk_{chash} \), two messages \( m, m' \), and the random number \( r \), \( CF_{chash} \) returns \( r' \) such that \( C_{hash}(pk_{chash}, m, r) = C_{hash}(pk_{chash}, m', r') \).

A chameleon hash scheme satisfies three security properties: (i) collision resistance; (ii) trapdoor collision; and (iii) semantic security. More details are available in [4], [25].

There is a relationship between the public key \( pk_{chash} \) and the trapdoor \( sk_{chash} \), which we refer to as the generation relationship. As in [25], the \( pp_{chash} = (p, q, g) \), where \( p, q \) are prime numbers such that \( p = q^r + 1 \), and the order of \( g \) is \( q \). The public key \( pk_{chash} = h \) is computed as follows: \( h = g^r \pmod{p} \), where \( x \in \mathbb{Z}^*_q \) is the trapdoor. Let equation \( pk_{chash} = chash_{gen}(sk_{chash}) \) describe this relation, where \( chash_{gen}(\cdot) \) denotes the generation algorithm between the \( pk_{chash} \) and the \( sk_{chash} \).

Zero-knowledge succinct non-interactive arguments of knowledge. Let \( \mathcal{R}_{AC} = \{ (x, w) \in \mathbb{F}^n \times \mathbb{F}^h | AC(x, w) = 0 \} \) be an NP relation, where \( \mathbb{F} \) denotes a finite field, and \( AC : \mathbb{F}^n \times \mathbb{F}^h \rightarrow \mathbb{F} \) denotes an \( \mathbb{F} \)-arithmetic circuit. The language for \( \mathcal{R}_{AC} \) is \( \mathcal{L}_{AC} = \{ x \in \mathbb{F}^n | \exists w \in \mathbb{F}^h \text{ s.t. } AC(x, w) = 0 \} \).

A zk-SNARK scheme \( NIZK \) = \( (\mathcal{K}_{nizk}, \mathcal{P}_{nizk}, \mathcal{V}_{nizk}) \) corresponds to the language \( \mathcal{L}_{AC} \), which is described below:

- \( \mathcal{K}_{nizk}(\lambda, AC) \rightarrow (pk, vk) \). Given a security parameter \( \lambda \) and an \( \mathbb{F} \)-arithmetic circuit \( AC \), \( \mathcal{K}_{nizk} \) returns a pair of proving/verification keys \((pk, vk)\).

- \( \mathcal{P}_{nizk}(pk, x, w) \rightarrow \pi \). Given the proving key \( pk \), a statement \( x \), and a witness \( w \), \( \mathcal{P}_{nizk} \) returns a proof \( \pi \) for a statement \( x \) using a witness \( w \).

- \( \mathcal{V}_{nizk}(vk, x, \pi) \rightarrow \{0, 1\} \). Given the verification key \( vk \), the statement \( x \), and the proof \( \pi \), \( \mathcal{V}_{nizk} \) returns 1 if verification succeeds, or 0 if verification fails.

A zk-SNARK scheme satisfies five secure properties: (i) completeness; (ii) soundness; (iii) succinctness; (iv) proof of knowledge; and (v) perfectly zero knowledge. More details are available in [8], [10], [19].

Public key encryption. A public key encryption scheme \( Enc = (g_{enc}, K_{enc}, E_{enc}, D_{enc}) \) is described below:

- \( g_{enc}(\lambda) \rightarrow pp_{enc} \). Given a security parameter \( \lambda \), \( g_{enc} \) returns the public parameters \( pp_{enc} \).

- \( K_{enc}(pp_{enc}) \rightarrow (pk_{enc}, sk_{enc}) \). Given the public parameters \( pp_{enc} \), \( K_{enc} \) returns a pair of public/private keys \((pk_{enc}, sk_{enc})\).

- \( E_{enc}(pk_{enc}, m) \rightarrow c \). Given the public key \( pk_{enc} \) and a message \( m \), \( E_{enc} \) returns a ciphertext \( c \).

- \( D_{enc}(sk_{enc}, c) \rightarrow m \). Given the private key \( sk_{enc} \) and the ciphertext \( c \), \( D_{enc} \) returns a message \( m \), or returns \( \perp \) if decryption fails.

The public encryption scheme \( Enc \) satisfies a security property: ciphertext indistinguishability under adaptive chosen ciphertext attack (IND-CCA2 security). More details are provided in [12].

![Diagram](image)

**Fig. 2:** Design idea.

### III. Key Ideas and SkyEye Overview

In this section, we provide key ideas in SkyEye design and an overview of SkyEye.

**A. Key Ideas**

**Notation.** Let \( B_{se} \) denote the \( B_s \) using SkyEye. We use \( u \) to denote a user, \( id_u \) to denote the \( u \)'s identity and \( proof_{id_u} \) to denote the \( u \)'s identity proof. Let \((pub_u, priv_u)\) denote the \( u \)'s public/private information, \((pk_{chash_u}, sk_{chash_u})\) denote the chameleon hash public/private key pair that generated by the \( u \) user, and \( CH_{id_u} \) denote the chameleon hash value of identity \( id_u \). The \( pk_{chash_u}||CH_{id_u} \) denotes the concatenation of \( pk_{chash_u} \) and \( CH_{id_u} \), where \(|\) denotes the concatenate symbol. The \( MT = (rt; pk_{chash_1}||CH_{id_1}, \ldots, pk_{chash_n}||CH_{id_n}) \) denotes a Merkle tree, where \( rt \) denotes the root of the Merkle Tree, and \((pk_{chash_1}||CH_{id_1}, \ldots, pk_{chash_n}||CH_{id_n}) \) denotes the leaf nodes in the Merkle tree. Let \((pk_{reg}, sk_{reg})\) denote the encryption public/private key pair of the regulator.

As shown in Figure 2, our design idea is that we add identity proofs to \( data_{B_{se}} \). The blockchain data in \( B_{se} \) can be represented as the equation \( data_{B_{se}} = [(pub_1, proof_{id_1}) \in \{1, \ldots, n\}, C]_{crytool} \), where the \( proof_{id_1} \) denotes the identity proof of the user whose identity is \( id_1 \), and the other variables are the same as those in the equation \( data_{B_g} \). The \((pub_1, proof_{id_1}) \) can be viewed as the new public information \( pub' \) of the user whose identity is \( id_1 \).

The identity proof is the core of SkyEye. The two purposes of the identity proof are to prove the user’s legitimacy and to achieve tracing. Next, we briefly describe the identity proof according to the above two purposes. More details are described in Section V.

1) **Proving the user’s legitimacy:** We assume that the user \( u \) has generated \((pub_u, priv_u), (pk_{chash_u}, sk_{chash_u}) \) and \( CH_{id_u} = C_{hash}(pk_{chash_u}, id_u, r) \), where \( r \) is the random number sampled by \( u \).

**Step 1: user registration.** To prove the user’s legitimacy, there must be something (similar to a certificate) that can indicate the user’s legitimacy. In SkyEye, this is done through user registration. Here, we briefly introduce user registration in SkyEye. More details on user registration appear in Section V-A2.
As shown in Figure 3, the user $u$ sends registration information $(C_{inf_0}, \pi_{inf_0})$ to the regulator, where the $C_{inf_0}$ is the ciphertext that is the encryption of the plaintext $(pk_{chash_u}, id_u, CH_{id_u})$ under the regulator’s public key $pk_{reg}$ and the $\pi_{inf_0}$ is the zk-SNARK proof that is used to prove: “I know $(sk_{chash_u}, r)$ which can generate the $pk_{chash_u}$ and $CH_{id_u}$.”

If the verification of the $(C_{inf_0}, \pi_{inf_0})$ is successful, the regulator stores $(pk_{chash_u}, id_u, CH_{id_u})$, and adds $pk_{chash_u} || CH_{id_u}$ to the Merkle tree $MT$. The regulator publishes the Merkle tree $MT$ at the right time. The registration of $u$ is successful only if the $u$’s $pk_{chash_u} || CH_{id_u}$ appears in the Merkle tree $MT$.

The Merkle tree $MT$ can be regarded as a credential of proving the user’s legitimacy. In other words, to prove the $u$’s legitimacy, the user $u$ must prove that his or her $pk_{chash_u} || CH_{id_u}$ appears in the Merkle tree $MT$. Therefore, the proof$_{id_u}$ generated by the user $u$ must be able to prove the following.

“$I$ know $(sk_{chash_u}, id_u, r)$ that can generate the $pk_{chash_u}$ and $CH_{id_u}$, and the $pk_{chash_u} || CH_{id_u}$ appears as a leaf of the Merkle tree $MT$ with the root $r$”

**Step 2: establishing the binding relationship between the $pub_u$ and proof$_{id_u}$.** Although the proof$_{id_u}$ described above can prove the $u$’s legitimacy, an issue remains. It can be seen from Figure 4 that the $(pub_u, proof_{id_u})$ needs to be published in the node network. The adversary who has registered with the regulator can generate an identity proof proof$_{id_u}$, and publish the $(pub_u, proof_{id_u})$ to the node work. At this time, a $pub_u$ corresponds to two different users’ identity proofs (i.e., proof$_{id_u}$ and proof$_{id_u}$). This presents a great obstacle to trace. We need to establish a relation between the $pub_u$ and the proof$_{id_u}$ that only the user $u$ can generate the identity proof proof$_{id_u}$ corresponding to the $pub_u$.

The key idea behind establishing this relation is that we establish the binding relationship between the priv$_u$ and proof$_{id_u}$. Because the $pub_u$ is generated by the priv$_u$, there is binding relationship between the $pub_u$ and proof$_{id_u}$.

We leverage the special property of chameleon hash scheme (i.e., the user who knows the trapdoor can easily find collision) to establish the binding relationship between the priv$_u$ and proof$_{id_u}$. Given the private information priv$_u$, the user $u$ who knows the trapdoor $sk_{chash_u}$ can easily find $r'$ such that $CH_{id_u} = \mathcal{H}_{chash}(pk_{chash_u}, priv_u, r')$. To achieve the binding of priv$_u$ and proof$_{id_u}$, we require the identity proof proof$_{id_u}$ to prove the following.

1. The public information $pub_u$ is generated by the private information priv$_u$.
2. I know $(sk_{chash_u}, priv_u, r')$ which can generate the $pk_{chash_u}$ and $CH_{id_u}$.
3. The $pk_{chash_u} || CH_{id_u}$ appears as a leaf of a Merkle tree with the root $r$.

This binding relationship between proof$_{id_u}$ and priv$_u$ ensures that only the user $u$ who knows the private information priv$_u$ can generate the identity proof proof$_{id_u}$, and others cannot forge the identity proof corresponding to the $pub_u$.

Moreover, the special property of chameleon hash scheme makes the user $u$ just register once, and then can generate identity proofs without involving the regulator.

2) Achieving tracing: To achieve tracing, we add $C_{id_u}$ which is the ciphertext of the $pk_{chash_u}$ under the regulator public key $pk_{reg}$ to the proof$_{id_u}$, and require the proof$_{id_u}$ to prove that the plaintext corresponding to the ciphertext $C_{id_u}$ is $pk_{chash_u}$. Because the regulator has the record $((pk_{chash_1}, id_1, CH_{id_1}), ..., (pk_{chash_n}, id_n, CH_{id_n}))$, the regulator can decrypt the $C_{id_u}$, obtain the $pk_{chash_u}$, and determine the identity of the user $u$ based on the record. More details about the identity proof are provided in V-A3.

**Remark.** We use $id$ to denote the user’s real identity (such as identity card number or mobile phone number). Moreover, there are many ways to verify the user’s identity in reality, such as, face recognition, identity card, or short message service (SMS) verification. Therefore, we assume there is an efficient way of verifying the $id$ in the user registration of SkyEye.

**B. SkyEye Overview**

As can be seen from Figure 4, SkyEye’s application strategy in $B_u$ is that the user generates the identity proof proof$_{id_u}$ cor-
responding to the user’s public information pub, and publishes the \((pub, proof_{id})\) to the node network.

From Figure 4, it can also be seen that the SkyEye scheme mainly has the following operations between the regulator, users, and verifiers.

- **User registration.** The user generates registration information and sends it to the regulator. The regulator is responsible for the verification of registration information.
- **Generating identity proof.** The user who registers successfully can generate the identity proof \(proof_{id}\). There is a binding relationship between the \(proof_{id}\) and the \(priv\).
- **Verifying identity proof.** Different from traditional verification process in the blockchain, the verifier (e.g., the miner) verifies identity proofs in addition to verifying data contents. If the data contents and identity proofs are simultaneously verified successfully, the data will be added to the block generated by the verifier.

- **Tracing.** The regulator traces the users’ true identities in the blockchain data.

**Remark.** The SkyEye scheme provides an alternative tracing strategy for \(B_s\). If a blockchain application that does not belong to \(B_s\) wants to use SkyEye, this application must modify some rules to make it belong to \(B_s\).

## IV. DEFINITION OF A TRACEABLE SCHEME

### A. Definition

A traceable scheme for blockchain is a tuple of polynomial-time algorithms \(\Pi = (\text{Setup}, \text{Gen}_\text{info}, \text{Ver}_\text{info}, \text{Gen}_\text{proof}, \text{Ver}_\text{proof}, \text{Trace})\) described below:

- **Setup(\(\lambda\)) → pp.** Given a security parameter \(\lambda\), the Setup returns public parameters pp. This algorithm is executed by a trusted party and is done only once. The public parameters pp are published and made available to all parties.

- **Gen\(_{\text{info}}\)(pp, id) → reginfo.** Given the public parameters pp and a user identity id, this algorithm returns the registration information reginfo.

- **Ver\(_{\text{info}}\)(pp, reginfo, sk\(_{\text{reg}}\)) → b.** Given the registration information reginfo, the public parameters pp and the regulator private key sk\(_{\text{reg}}\), this algorithm returns a bit b. If verification succeeds, this algorithm returns 1; otherwise, it returns 0.

- **Gen\(_{\text{proof}}\)(pp, pub, priv, CH\(_{id}\), pk\(_{\text{chash}}\), sk\(_{\text{chash}}\), r, rt, path\(_{id}\)) → proof\(_{id}\).** Given the public parameters pp, a user’s public/private information \((pub, priv)\), the chameleon hash \(CH_{id}\), the chameleon hash public/private key \((pk_{\text{chash}}, sk_{\text{chash}})\), the random element \(r\) for computing the chameleon hash, the Merkle tree root rt, and the path \(path_{id}\) from \(pk_{\text{chash}}||CH_{id}\) to \(rt\), Gen\(_{\text{proof}}\) returns the user’s identity proof \(proof_{id}\).

- **Ver\(_{\text{proof}}\)(pp, pub, proof\(_{id}\)) → b.** Given the public parameters pp, a user’s public information pub and the user identity proof \(proof_{id}\), Ver\(_{\text{proof}}\) returns a bit b. If the verification of \(proof_{id}\) succeeds, this algorithm returns 1; otherwise, it returns 0.

- **Trace(data\(_{B_s}\)) → ID.** Given the blockchain data data\(_{B_s}\), Trace returns the identity set ID for data\(_{B_s}\).

### B. Security

We assume that in \(B_s\) relevant cryptographic techniques (e.g., digital signatures) have been used to ensure that the blockchain data generated by the users cannot be tampered with. Therefore, the users’ identity proofs added to the blockchain data also cannot be tampered with. We also assume that the regulator is trusted and has an efficient way of verifying user identity. Therefore, the goals of the adversary are to forge the user identity proof and to distinguish two distinct user identity proofs. The security of a traceable scheme must satisfy the following security properties:

- **Identity proof indistinguishability.** This property requires that even if the adversary can adaptively induce honest parties to perform operations of his choice, the identity proof reveals no information except for some public information, such as public addresses and serial numbers. In other words, even if the adversary queries two different honest parties (one identity is \(id_0\), and the other identity is \(id_1\)), no polynomial-time adversary can distinguish between the identity proofs \(proof_{id_0}\) and \(proof_{id_1}\). The meaning of this property is that if the blockchain is indistinguishable, adding the identity proofs to the blockchain data does not affect the indistinguishability in the blockchain.

- **Identity proof unforgeability.** This property requires that even if the adversary can adaptively induce honest parties to perform operations of his choice, no polynomial-time adversary can forge the identity proof of honest parties. This property ensures that the adversary cannot forge the honest user’s identity proof to create blockchain data for evading supervision.

We defer formal definition of each property to Appendix A.

**Definition 1** A traceable scheme \(\Pi = (\text{Setup}, \text{Gen}_\text{info}, \text{Ver}_\text{info}, \text{Gen}_\text{proof}, \text{Ver}_\text{proof}, \text{Trace})\) is secure if it satisfies identity proof indistinguishability and identity proof unforgeability.

## V. CONSTRUCTION

### A. SkyEye Construction

1) **SkyEye Initialization:** The public parameters pp created by the Setup algorithm include the following information: the zk-SNARK proving/verification key \((pk_{\text{info}}, vk_{\text{info}})\) used to generate and verify the zk-SNARK proof \(\pi_{\text{info}}\) for the NP relation \(R_{\text{info}}\) (see Section V-A2 for details), the zk-SNARK proving/verification key \((pk_{\text{proof}}, vk_{\text{proof}})\) used to generate and verify the zk-SNARK proof \(\pi_{\text{proof}}\) for the NP relation \(R_{\text{proof}}\) (see Section V-A3 for details), the regulator public key \(pk_{\text{reg}}\) for public key encryption, and the public parameters \(pp_{\text{chash}}\) of the chameleon hash scheme. Once the algorithm Setup returns pp, the pp will be published and made available to all parties. (See Setup algorithm in Algorithm 1 for specific operations.)

2) **User Registration:** The user registration is divided into two parts: the generation of user registration information and the verification of user registration information.
Algorithm 1 SkyEye Construction

Setup
Input: security parameter $\lambda$;
Output: public parameters $pp$;
1: construct arithmetic circuit $AC_{info}$ for relation $R_{info}$ at security $\lambda$;
2: construct arithmetic circuit $AC_{proof}$ for relation $R_{proof}$ at security $\lambda$;
3: $(pk_{info}, vk_{info}) = \mathcal{K}_{nizk}(\lambda, AC_{info})$;
4: $(pk_{proof}, vk_{proof}) = \mathcal{K}_{nizk}(\lambda, AC_{proof})$;
5: compute $pp_{enc} = \mathcal{G}_{enc}(\lambda)$;
6: compute $(pk_{reg}, sk_{reg}) = \mathcal{K}_{enc}(pp_{enc})$;
7: compute $pp_{chash} = \mathcal{G}_{chash}(\lambda)$;
8: return $pp := (pk_{info}, vk_{info}, pk_{proof}, vk_{proof}, pk_{reg}, pp_{chash})$.

$Gen_{info}$
Input:
public parameters $pp$,
user identity $id$;
Output:
registration information $reg_{info}$;
1: $(pk_{chash}, sk_{chash}) = \mathcal{K}_{chash}(pp_{chash})$;
2: randomly sample $r$;
3: compute $CH_{id} = H_{chash}(pk_{chash}, id, r)$;
4: set $x_{info} = (id, pk_{chash}, CH_{id}), w_{info} = (sk_{chash}, r)$;
5: $\pi_{info} = \mathcal{P}_{nizk}(pk_{info}, x_{info}, w_{info})$;
6: set $C_{info} = E_{enc}(pk_{reg}, x_{info})$;
7: store $(id, pk_{chash}, sk_{chash}, r, CH_{id})$;
8: return $reg_{info} = (C_{info}, \pi_{info})$.

$Ver_{info}$
Input:
public parameters $pp$,
registration information $reg_{info}$,
regulator’s private key $sk_{reg}$;
Output: bit $b$;
1: parse $reg_{info}$ as $(C_{info}, \pi_{info})$;
2: $x_{info} = D_{enc}(sk_{reg}, C_{info})$;
3: parse $x_{info}$ as $(id, pk_{chash}, CH_{id})$;
4: if id not valid then
5: return $b = 0$;
6: end if
7: if $\mathcal{V}_{nizk}(vk_{info}, x_{info}, \pi_{info}) = 0$ then
8: return $b = 0$;
9: else
10: store $(pk_{chash}, id, CH_{id})$;
11: publish $pk_{chash}||CH_{id}$ via the Merkle tree $MT$;
12: return $b = 1$;
13: end if

$Gen_{proof}$
Input:
public parameters $pp$,
user public/private information $(pub, priv)$,
chameleon hash $CH_{id}$,
chameleon hash public/private key $(pk_{chash}, sk_{chash})$,
random element $r$ for computing chameleon hash,
Merkle tree root $rt$,
path $path_{id}$ from $pk_{chash}||CH_{id}$ to $rt$;
Output:
user identity proof $proof_{id}$;
1: compute $r' = CF_{chash}(sk_{chash}, id, priv, r)$;
2: randomly sample $rn$ for encrypting;
3: compute $C_{id} = E_{enc}(pk_{reg}, pk_{chash}, rn)$;
4: set $u_{proof} = (rt, pk_{reg}, C_{id})$;
5: set $x_{proof} = (pub, u_{proof})$,
6: compute $\pi_{proof} = \mathcal{P}_{nizk}(pk_{proof}, x_{proof}, u_{proof})$;
7: set $proof_{id} = (u_{proof}, \pi_{proof})$;
8: return $proof_{id}$

$Ver_{proof}$
Input:
public parameters $pp$,
user public information $pub$,
identity proof $proof_{id}$;
Output: bit $b$;
1: parse $proof_{id}$ as $(u_{proof}, \pi_{proof})$;
2: set $x_{proof} = (pub, u_{proof})$;
3: if $\mathcal{V}_{nizk}(vk_{proof}, x_{proof}, \pi_{proof}) = 0$ then
4: return $b = 0$;
5: else
6: return $b = 1$;
7: end if

Trace
Input:
blockchain data $data_{B_{se}}$;
Output: identity set $ID$ for $data_{B_{se}}$;
1: set $ID = \emptyset$;
2: get ciphertext set $C = \{C_{id_i}\}_{i \in \{1,\ldots,n\}}$ from $data_{B_{se}}$, where $n$ is the number of the users’ public information in $data_{B_{se}}$;
3: for (each $C_{id_i} \in C$) do
4: compute $pk_{chash_i} = D_{enc}(sk_{reg}, C_{id_i})$;
5: search $(pk_{chash_i}, id, CH_{id})$ records, get $id_i$ corresponding to $pk_{chash_i}$;
6: put $id_i$ in $ID$;
7: end for
8: return $ID$;
As shown in Algorithm 1, a user generates his own \((pk_{\text{chash}}, sk_{\text{chash}})\) based on the chameleon hash public parameters \(p_{\text{chash}}\), then computes the chameleon hash value \(CH_{id}\) of identity \(id\), and stores \((id, pk_{\text{chash}}, sk_{\text{chash}}, r, CH_{id})\). At this point, the user can produce a zk-SNARK proof \(\pi_{\text{info}}\) for the following NP relation, which we call \(R_{\text{info}}\).

Given \(x_{\text{info}} = (id, pk_{\text{chash}}, CH_{id})\), I know \(w_{\text{info}} = (sk_{\text{chash}}, r)\) such that:

\[ \begin{align*}
\text{��} & \quad \text{The chameleon hash private key matches the chameleon hash public key: } pk_{\text{chash}} = \text{chash-gen}(sk_{\text{chash}}). \\
\text{��} & \quad \text{The chameleon hash is correctly computed: } CH_{id} = \mathcal{H}_{\text{chash}}(pk_{\text{chash}}, id, r).
\end{align*} \]

The \(\text{Gen}_{\text{info}}\) algorithm outputs registration information \(\text{reginfo}\), which consists of the ciphertext \(C_{\text{info}}\) and zk-SNARK proof \(\pi_{\text{info}}\). The ciphertext \(C_{\text{info}}\) is the encryption of \(x_{\text{info}}\) that uses the regulator public key \(p_{\text{reg}}\).

The \(\text{Ver}_{\text{info}}\) algorithm shown in Algorithm 1 is used to verify the user’s registration information \(\text{reginfo}\) by the regulator. The verification operations in algorithm \(\text{Ver}_{\text{info}}\) include verifying the identity \(id\) and verifying the zk-SNARK proof \(\pi_{\text{info}}\). If the above two operations are verified successfully, the regulator stores \((id, pk_{\text{chash}}, \text{reginfo}, \text{CH}_{id})\), and then publishes \(pk_{\text{chash}}||CH_{id}\) stored in the Merkle tree \(MT\) in which the root is denoted by \(rt\). Meanwhile, this algorithm returns 1.

3) Generating and Verifying Identity Proof: The \(\text{Gen}_{\text{proof}}\) shown in Algorithm 1 is used to generate the identity proof for each user. Assume a user has generated the public/private information \((pub, priv)\). According to the known trapdoor \(sk_{\text{chash}}\), the user can calculate a value \(r'\) such that \(CH_{id} = \mathcal{H}_{\text{chash}}(pk_{\text{chash}}, priv, r')\). Next, the user computes ciphertext \(C_{id} = \mathcal{E}_{\text{enc}}(p_{\text{reg}}, pk_{\text{chash}}, r)\), where \(pk_{\text{reg}}\) is the public key of the regulator, and \(r\) is the random number used for encryption. Finally, the user produces a zk-SNARK proof \(\pi_{\text{proof}}\) for the following NP relation, which we term \(R_{\text{proof}}\): Given a statement \(x_{\text{proof}} = (\text{path}_{id}, CH_{id}, sk_{\text{chash}}, pk_{\text{chash}}, priv, r', r)\), I know \(w_{\text{proof}} = (\text{path}_{id}, CH_{id}, sk_{\text{chash}}, pk_{\text{chash}}, priv, r', r)\) such that:

\[ \begin{align*}
\text{��} & \quad \text{The private information matches the public information: } pub = \text{gen}(priv). \\
\text{��} & \quad \text{The chameleon hash private key matches the chameleon hash public key: } pk_{\text{chash}} = \text{chash-gen}(sk_{\text{chash}}). \\
\text{��} & \quad \text{The chameleon hash } CH_{id} \text{ is computed correctly: } CH_{id} = \mathcal{H}_{\text{chash}}(pk_{\text{chash}}, priv, r'). \\
\text{��} & \quad \text{The ciphertext } C_{id} \text{ corresponds to the plaintext } pk_{\text{chash}}: C_{id} = \mathcal{E}_{\text{enc}}(pk_{\text{reg}}, pk_{\text{chash}}, r). \\
\text{��} & \quad \text{The } pk_{\text{chash}}||CH_{id} \text{ appears as a leaf of a Merkle tree with the root } rt.
\end{align*} \]

The \(\text{Ver}_{\text{proof}}\) algorithm in Algorithm 1 is used to verify the user’s identity proof \(\text{proof}_{id}\). The verification operation verifies the zk-SNARK proof \(\pi_{\text{proof}}\). This algorithm returns 1 if and only if the above operation verifies successfully.

4) Tracing: As shown in Algorithm 1, the algorithm \(\text{Trace}\) is used to trace the blockchain data \(\text{data}_{\text{bs}}\). The regulator obtains \(pk_{\text{chash}}\) by decrypting every ciphertext \(C_{id}\), and according to the record that stores each user’s chameleon hash public key \(pk_{\text{chash}}\), identity \(id\), and chameleon hash \(CH_{id}\), the regulator can determine the true identities of the users in the \(\text{data}_{\text{bs}}\). This algorithm returns the users’ identity set \(ID\).

B. SkyEye Security

**Theorem 1** Assuming the Chash scheme is collision resistant, trapdoor collision and semantic security, the NIZK scheme is perfectly zero-knowledge and simulation sound extractable, the encryption scheme Enc satisfies IND-CCA2 security, and \(\text{gen}(\cdot)\) has one-wayness property. Our scheme \(\Pi = \langle \text{Setup}, \text{Gen}_{\text{info}}, \text{Ver}_{\text{info}}, \text{Gen}_{\text{proof}}, \text{Ver}_{\text{proof}}, \text{Trace} \rangle\) described in Algorithm 1 is a secure (cf. Definition 1) traceable scheme.

We provide the proof of Theorem 1 in Appendix B.

VI. IMPLEMENTATION AND EVALUATION

A. Implementation

There are two main ways of generating public and private information in blockchain applications. One is through the pseudorandom function (e.g., Zerocash [8], Hawk [24]), i.e., \(pub = \text{PRF}_{\text{priv}}(s)\), where \(\text{PRF}\) denotes the pseudorandom function, \(pub\) is the pseudorandom number, \(priv\) is the private key used to generate \(pub\), and \(s\) is the uniform seed. The other way is to use elliptic curve scalar multiplication (e.g., Bitcoin) to generate the public and private information, i.e., \(pub = \text{priv} \cdot G\), where \(priv\) is a scalar, \(G\) is a base point on the elliptical curve, and \(pub\) is a point on the elliptical curve.

We use SkyEye\text{H} to represent the scheme that generates public and private information in the first way, and SkyEye\text{S} to represent the scheme that generates public and private information in the second way. We use the C++ programming language to implement the prototype of the above two different schemes based on the zk-SNARK library, libsnark [9].

There are some cryptographic building blocks in SkyEye\text{H}: the pseudorandom function, chameleon hash scheme, hash function in the Merkle tree, public encryption scheme, and zk-SNARK scheme. For the chameleon hash scheme, we use the chameleon hash scheme proposed by Hugo Krawczyk and Tal Rabin [25]. For efficiency, we use the SHA256 compression function to implement the pseudorandom function and hash function in the Merkle tree, which is similar to the approach used in Zerocash [8]. We use the practical public key encryption scheme proposed by Cramer and Shoup [12], an IND-CCA2 secure public encryption scheme, as our encryption scheme. We use the scheme proposed by Parno et al. [31] as the zk-SNARK scheme. In the concrete implementation, we use the Barreto-Naehrig elliptic curve [7] that provides 128-bit security as the underlying curve of the zk-SNARK scheme. The implementation of the chameleon hash and public key encryption scheme is based on a prime field of 254 bits.

In SkyEye\text{S}, the main cryptographic building block differs from the former in that the pseudorandom function is replaced by elliptic curve scalar multiplication. The chameleon hash scheme, public key encryption scheme, and zk-SNARK scheme are the same as those in the SkyEye\text{H}. In the concrete implementation, we use the MNT4 elliptic curve
TABLE I: Performance of SkyEye_H

<table>
<thead>
<tr>
<th>SkyEye_H</th>
<th>Tree depth</th>
<th>Configuration 1: intel(R) core(TM) i5-2450M @2.50GHz 4GB of RAM</th>
<th>Configuration 2: intel(R) core(TM) i7-6700 @3.40GHz 16GB of RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td></td>
<td>time(s)</td>
<td>jpk_{info}(KB)</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>69</td>
<td>114</td>
<td>156</td>
</tr>
<tr>
<td>Gen_{info}</td>
<td></td>
<td>time(s)</td>
<td>475.7</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>15.3</td>
<td>15.7</td>
</tr>
<tr>
<td>Gen_{proof}</td>
<td></td>
<td>time(s)</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>10.1</td>
<td>10.2</td>
<td>10.1</td>
</tr>
<tr>
<td>Trace</td>
<td></td>
<td>time(s)</td>
<td>0.13</td>
</tr>
</tbody>
</table>

TABLE II: Performance of SkyEye_S

<table>
<thead>
<tr>
<th>SkyEye_S</th>
<th>Tree depth</th>
<th>Configuration 1: intel(R) core(TM) i5-2450M @2.50GHz 4GB of RAM</th>
<th>Configuration 2: intel(R) core(TM) i7-6700 @3.40GHz 16GB of RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td></td>
<td>time(s)</td>
<td>jpk_{info}(KB)</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>187</td>
<td>296</td>
<td>403</td>
</tr>
<tr>
<td>Gen_{info}</td>
<td></td>
<td>time(s)</td>
<td>1398.0</td>
</tr>
<tr>
<td></td>
<td>51.8</td>
<td>52.4</td>
<td>53.4</td>
</tr>
<tr>
<td>Gen_{proof}</td>
<td></td>
<td>time(s)</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>47.8</td>
<td>47.9</td>
<td>48.0</td>
</tr>
<tr>
<td>Trace</td>
<td></td>
<td>time(s)</td>
<td>0.14</td>
</tr>
</tbody>
</table>

[28] as the underlying curve of the zk-SNARK scheme. The implementation of elliptic curve scalar multiplication is based on the MNT6 elliptic curve [28]. We implement the chameleon hash scheme and public key encryption scheme in a prime field of 298 bits. To improve efficiency, in the formation of the Merkle tree, because the length of the leaf node is 298 bits, two leaf nodes together cannot form 512 bits. Therefore, the upper node is generated by the leaf node using the standard SHA256. In addition, the data length of the node above the leaf node is 256 bits, so each node that is not generated through the leaf node is generated by the SHA256 compression function.

B. Evaluation

We evaluate the performance of every algorithm in the two aforementioned schemes in two different configurations: configuration 1, with an Intel i5 processor and 4 GB memory laptop; and configuration 2, with an Intel i7 processor and 16 GB memory desktop machine. The depth of the Merkle tree in our evaluation is 10, 20, 30, and 34, respectively. In other words, the maximum number of users which the Merkle tree supports is $2^{10}$, $2^{20}$, $2^{30}$, and $2^{34}$. This fully meets demand, because the current global population is about 7.5 billion, and $2^{34}$ reaches more than 17 billion. Moreover, we evaluate the performance of the Trace algorithm under the condition that there are already 1024 successfully registered users at the regulator.

Table I and Table II illustrate the performance results of the Setup, Gen_{info}, Ver_{info}, Gen_{proof}, Ver_{proof} and Trace algorithms in SkyEye_H and SkyEye_S, respectively (the time in the two tables is the average of 10 runs per algorithm). In the two tables, time represents the running time of the algorithm, and $\|\cdot\|$ represents the data length. For example, the $\|pk_{info}\|$ represents the length of the proving key in the registration. Without loss of generality, using an i7 processor, a 16 GB memory desktop machine, and with a tree depth of 34 in Table I, we can obtain the results of the SkyEye_H scheme:

- Setup algorithm takes 94 s.
- The size of the proving key and verification key used for user registration are 480 KB and 574 B, respectively.
- The size of the proving key and verification key used for user identity proof are 231 MB and 21 KB, respectively.
- Gen_{info} requires 272.4 ms, and the size of the zk-SNARK proof $\pi_{info}$ is 287 B.
- Ver_{info} algorithm takes 6.9 ms.
- Gen_{proof} algorithm takes 35 s to generate a user’s identity proof, and the size of the zk-SNARK proof $\pi_{proof}$ is 287 B.
SkyEye environment and tree depth change. The size of SNARK proof \( \pi \). As can be observed from the two tables, the length of the zk-SNARK proof is approximately 10 ms in configuration 1 and approximately 5 ms in configuration 2. From Table II, we can observe that the time taken for verifying the user registration information is approximately 53 ms in configuration 1 and approximately 28 ms in configuration 2; and the time taken for verifying the user identity proof is approximately 48 ms in configuration 1 and approximately 25 ms in configuration 2.

- Not all of the information in SkyEye must be on-chain. Only the information \( proof_{id} \) generated by the Gen\(_{proof}\) algorithm is added to the user data. Furthermore, the size of the user’s zk-SNARK proof \( \pi_{proof} \) in the \( proof_{id} \) is dominant. As can be observed from the two tables, the length of the zk-SNARK proof \( \pi_{proof} \) will not change as the configuration environment and tree depth change. The size of \( \pi_{proof} \) is small, and the length is 287 B in SkyEye\(_{H} \) and 337 B in SkyEye\(_{S} \).

VII. DISCUSSION AND FUTURE WORK

In SkyEye, the centralization of the regulator is a major issue. The regulator can arbitrarily trace the identity of blockchain data without any restrictions and oversight.

From the data tracing process of the regulator, it can be seen that the regulator must first use its private key \( sk_{reg} \) to decrypt the ciphertext of each user’s chameleon hash public key in the blockchain data. Therefore, we can restrict the regulator through the distributed key generation (DKG) protocol [20]. Specifically, the public/private key pair \((pk_{reg}, sk_{reg})\) is generated by a committee with a threshold of \( t \) through the DKG protocol. In this way, the \( pk_{reg} \) is made public, and each committee member has a share of \( sk_{reg} \). The regulator submits the data and tracing evidence to the committee. If at least \( t+1 \) members of the committee accept the data and tracing evidence, the regulator will obtain the \( sk_{reg} \) from the committee.

However, this approach does not completely restrict the regulator. Even if the committee regularly updates the public/private key pair, as long as the regulator obtains the private key \( sk_{reg} \) in a cycle, it can trace not only the data submitted to the committee, but also all user data in this cycle. In future work, we will consider how to restrict the regulator to make the regulator only trace the data submitted to the committee.

VIII. RELATED WORK

Blockchain research focuses primarily on enhancing blockchain privacy protection [8], [32], improving blockchain scalability [16], [35], analyzing blockchain security [17], [26], and applying blockchain to other areas [27], [33]. However, research on traceable mechanisms is limited.

Narula, Vasquez, and Virza proposed zkLedger [30], the first distributed ledger system, that provides strong privacy protection, public verifiability, and practical auditing. zkLedger uses table-construction in the ledger. Each user identity corresponds to each column in the ledger. Therefore, the regulator can determine every user identity through the ledger. However, this traceable mechanism in zkLedger cannot be applied to environments with a large number of users and is used only for auditing digital asset transactions over some banks.

Defrawy and Lampkins [15] proposed a proactively-private digital currency (PDC) scheme that can provide privacy-preserving and accountability. In their scheme, the ledger is kept by a group of ledger servers. Every ledger sever has a balance ledger that contains a share of every user identity. Therefore, the regulator can determine every user identity through these ledger servers. However, their traceable mechanism does not seem to have been extended to other applications.

Ateniese and Faonio [5] constructed a scheme that provides certified Bitcoin addresses to enable Bitcoin users to trade with certifiable users authenticated by the trusted certificate authority. The regulator can determine every user identity through the authority. However, if a user wants to use a new certified address for each transaction, the user must contact the certificate authority to obtain a certified address. This reduces the efficiency of the entire system and exerts considerable pressure on the certificate authority when the number of users is large. Moreover, their approach only applies to Bitcoin.

Garman, Green, and Miers [18] designed new decentralized anonymous payment (DAP) systems to address the regulatory issue by adding privacy preserving policy-enforcement mechanisms that guarantee regulatory compliance, allow selective user tracing, and admit tracing of tainted coins. The regulator can determine every user identity through the identity escrow policy. However, the DAP system are based on Zerocash [8].

The traceable mechanisms proposed above can only be applied to specific application environments and do not seem to have been extended to other applications. We propose SkyEye, a traceable scheme for blockchain. Our scheme can be applied to a class of blockchain applications, which is denoted by \( B_z \).

IX. CONCLUSION

In this paper, we design SkyEye, a traceable scheme for blockchain. SkyEye can be applied to the blockchain applications that satisfy the following conditions: (I) The users have public and private information, where the public information is generated by the private information; (II) The users’ public information is disclosed in the blockchain data. SkyEye just requires the user to register only once, and enables the regulator to trace users’ identities. Moreover, we implement two different SkyEye prototypes: SkyEye\(_{H} \) and SkyEye\(_{S} \). Our evaluation results show that even if the number of users...
is very large, the registration information and identity proof are verified quickly.

APPENDIX A
SECURITY OF THE TRACEABLE SCHEME

We describe identity proof indistinguishability and identity proof unforgeability. Every property is formalized as an experiment between an adversary \( A \) and a challenger \( C \). The behavior of the honest user with identity \( id \) is realized by the oracle \( O_{id} \), and the behavior of the regulator is realized by the oracle \( O_{reg} \). We assume that the honest users and adversary in the experiment have already registered successfully in the regulator, i.e., they can generate any identity proof. Below, we describe how \( O_{id} \) and \( O_{reg} \) work.

Oracles \( O_{id} \) and \( O_{reg} \) are initialized by challenger \( C \) using the public parameters \( pp \). The \( O_{reg} \) stores: (1) \textit{Record}, a set of information used to trace true identities of all registered users; (2) the encryption public/private key pair \((pk_{reg}, sk_{reg})\). The \( O_{reg} \) accepts different queries, which are described below:

- \( Q = (\text{judge}, \text{proof}_{id}, \text{proof}_{id}) \), the \( O_{reg} \) determines whether \( \text{proof}_{id} \) and \( \text{proof}_{id} \) belong to the same user, and sends the result to the inquirer.
- \( Q = (\text{chashset}, \text{proof}_{id}) \), the \( O_{reg} \) sends the chameleon hash set \( P_{\text{chash}} \) to the inquirer. The \( P_{\text{chash}} \) includes the chameleon hash of the user who generates the \( \text{proof}_{id} \).

The \( O_{id} \) stores: (1) \textit{RegPrinfo}, the secret information used to generate registration information; (2) \textit{IdProof}, a set of identity proofs generated by the user whose identity is \( id \); (3) \textit{IdProofPrinfo}, the set of evidence that the user uses to generate the identity proofs. The \( O_{id} \) accepts different queries, which are described below:

- \( Q = (\text{genidproof}) \), The adversary is not aware of the private information \( priv \). The oracle \( O_{id} \) first randomly selects \( priv \), and then generates the public information \( pub \). Finally, the oracle \( O_{id} \) calls the \( \text{GenProof} \) algorithm to generate the identity proof \( \text{proof}_{id} \), and sends the \( (\text{pub}, \text{proof}_{id}) \) to the inquirer.
- \( Q = (\text{genidproof}, \text{proof}_{id}) \), The adversary knows the private information \( priv \), and the oracle \( O_{id} \) uses the \( priv \) selected by the adversary to generate the public information \( pub \) and then calls the \( \text{GenProof} \) algorithm to generate the identity proof \( \text{proof}_{id} \). Finally, sends the \( (\text{pub}, \text{proof}_{id}) \) to the inquirer.
- \( Q = (\text{genidproof}, \text{pub}_i) \), here, \( \text{pub}_i \in T_{\text{pub}}, \) and \( T_{\text{pub}} = \{\text{pub}_1, ..., \text{pub}_n\} \) is the public information set of the user whose identity is \( id \). The oracle \( O_{id} \) calls the \( \text{GenProof} \) algorithm to generate the identity proof \( \text{proof}_{id} \), and sends the \( (\text{pub}_i, \text{proof}_{id}) \) to the inquirer.

A. Identity proof indistinguishability

Identity proof indistinguishability is formalized by \( \text{Exp}^{\text{IDP-IND}}_{\text{A}, \Pi} \), which is shown below:

1. The challenger \( C \) randomly samples \( b \in \{0, 1\} \), gets \( pp \) by running \( \text{Setup}(\lambda) \), and sends \( pp \) to adversary \( A \). Next, \( C \) initializes two separate oracles \( O_{id_0} \) and \( O_{id_1} \).

2. The adversary \( A \) issues queries \( q_1, ..., q_m \), where \( q_i \) is one of the following:
   - \( Q \) and \( Q' \) are both \( \text{genidproof} \) queries. \( C \) forwards \( Q \) to \( O_{id_0} \) and forwards \( Q' \) to \( O_{id_1} \), \( C \) replies to \( A \) with \((pub_b, proof_{id_b}), (pub_{1-b}, proof_{id_{1-b}})\), which is the two oracle answer.
   - \( \{Q, Q'\} = \{(\text{genidproof}, priv), (\text{genidproof}, priv')\} \), where \( priv = priv \cdot C \) forwards \( Q \) to \( O_{id_0} \), and forwards \( Q' \) to \( O_{id_1} \), \( C \) replies to \( A \) with \((pub, proof_{id}), (pub, proof_{id_{-1}})\), which is the two oracle answer.

3. At the end of the query, \( A \) sends \( C \) a guess \( b' \in \{0, 1\} \). If \( b = b' \), \( C \) outputs 1; otherwise, \( C \) outputs 0.

Identity proof indistinguishability requires that the adversary \( A \) wins the above experiment with only negligible probability. Next, we formally define this property.

Definition 2 A traceable scheme \( \Pi = (\text{Setup}, \text{Geninfo}, \text{Verinfo}, \text{Genproof}, \text{Verproof}, \text{Trace}) \) satisfies identity proof indistinguishability if for all probabilistic polynomial-time adversaries \( A \), there is a negligible function \( \text{negl}(\cdot) \) such that

\[
\text{Adv}^{\text{IDP-IND}}_{\text{A}, \Pi} \leq \text{negl}(\lambda),
\]

where \( \text{Adv}^{\text{IDP-IND}}_{\text{A}, \Pi} = \text{Pr}[\text{Exp}^{\text{IDP-IND}}_{\text{A}, \Pi}(\lambda) = 1] - 1/2 \) is \( A \)’s advantage in the experiment \( \text{Exp}^{\text{IDP-IND}}_{\text{A}, \Pi}(\lambda) \).

B. Identity proof unforgeability

Identity proof unforgeability is formalized by an experiment \( \text{Exp}^{\text{IDP-UNF}}_{\text{A}, \Pi} \), which is shown below:

1. The challenger \( C \) obtains \( pp \) by running \( \text{Setup}(\lambda) \), and sends \( pp \) to adversary \( A \). Next, \( C \) initializes two separate oracles \( O_{id} \) and \( O_{reg} \). Let \( T_{pub} = \{\text{pub}_1, ..., \text{pub}_n\} \) be the public information set for the user whose identity is \( id \).

2. The adversary \( A \) issues queries \( q_1, ..., q_m \), where \( q_i \) is \( (\text{genidproof}, \text{pub}_i) \), and \( \text{pub}_i \in T_{pub} \). \( C \) forwards \( Q \) to \( O_{id_0} \), \( C \) replies to \( A \) with \((\text{pub}_i, \text{proof}_{id_i})\), which is the oracle \( O_{id} \)’s answer.

3. At the end of the query, let \( P = \{\text{proof}_{f_1}, ..., \text{proof}_{f_m}\} \) is the identity proof set that is generated by \( O_{id} \). \( A \) sends \((\text{pub}, \text{proof}_{id})\) to \( C \). \( C \) checks as follows:
   - If \( \text{proof}_{f_i} \notin P \land \text{Verproof}(pp, \text{pub}, \text{proof}_{f_i}) = 1 \), \( C \) proceeds as follows; otherwise it aborts.
   - \( C \) sends \((\text{judge}, \text{proof}_{id}, \text{proof}_{f_i})\) to \( O_{reg} \), where \( i \in [1, m] \). If \( \text{proof}_{id} \), and \( \text{proof}_{f_i} \) belong to the user whose identity is \( id \), \( O_{reg} \) sends \( c = 1 \) to \( C \); otherwise it returns \( c = 0 \).

4. \( \text{proof}_{f_i} \notin P \land \text{Verproof}(pp, \text{pub}, \text{proof}_{f_i}) = 1 \land c = 1 \), \( C \) outputs 1; otherwise, \( C \) outputs 0.

The adversary \( A \) wins the above experiment if the \( \text{proof}_{f_i} \) such that (i) \( \text{proof}_{f_i} \notin P \); (ii) \( \text{Verproof}(pp, \text{pub}, \text{proof}_{f_i}) = 1 \); (iii) \( \text{proof}_{f_i} \) belongs to the user whose identity is \( id \). In other words, \( A \) can forge the identity proof of honest parties. Identity proof unforgeability requires that the adversary wins the above experiment with only negligible probability. Next, we formally define this property.

Definition 3 A traceable scheme \( \Pi = (\text{Setup}, \text{Geninfo}, \text{Verinfo}, \text{Genproof}, \text{Verproof}, \text{Trace}) \) satisfies identity proof
unforgeability if for all probabilistic polynomial time adversaries \( A \), there is a negligible function \( \text{negl}(\cdot) \) such that
\[
\text{Adv}_{A, \Pi}^{\text{DP-UNF}} \leq \text{negl}(\lambda),
\]
where
\[
\text{Adv}_{A, \Pi}^{\text{DP-UNF}} = \Pr[|\text{Exp}_{A, \Pi}^{\text{DP-UNF}}(\lambda) = 1| - 1/2] \text{ is } A's \text{ advantage in the experiment } \text{Exp}_{A, \Pi}^{\text{DP-UNF}}(\lambda).
\]

### APPENDIX B

**Proof of Theorem 1**

**A. Proof of identity proof indistinguishability**

**Theorem 2** Assuming that the NIZK scheme is perfectly zero-knowledge and simulation sound extractable, the encryption scheme Enc satisfies IND-CCA2 security, then, our scheme \( \Pi = (\text{Setup}, \text{Gen}_{\text{in} \text{fo}}, \text{Ver}_{\text{in} \text{fo}}, \text{Gen}_{\text{proof}}, \text{Ver}_{\text{proof}}, \text{Trace}) \) described in Algorithm 1 satisfies identity proof indistinguishability.

We prove the Theorem 2 through a sequence of hybrid experiments. Let \( q_{m} \) be the number of queries issued by the adversary \( A \).

- \( \text{Exp}_{\text{real}} \): The experiment \( \text{Exp}_{\text{real}} \) is the same as the \( \text{Exp}_{A, \Pi}^{\text{DP-IND(\lambda)}} \).
- \( \text{Exp}_{1} \): The experiment \( \text{Exp}_{1} \) is the same as the experiment \( \text{Exp}_{\text{real}} \) except that the challenger \( C \) simulates the NIZK. More precisely, \( C \) calls a polynomial-time simulator \( S_{\text{nizk}}(\lambda, A_{\text{proof}}) \) to obtain \( (pk_{\text{proof}}, vk_{\text{proof}}, \text{tra}) \), where \( \text{tra} \) is the trapdoor, instead of invoking \( K_{\text{nizk}}(\lambda, A_{\text{proof}}) \).
- \( \text{Exp}_{\text{final}} \): The experiment \( \text{Exp}_{\text{final}} \) is the same as the experiment \( \text{Exp}_{\text{real}} \) except that the challenger \( C \) replaces the \( C_{\text{id}} \) in \( \text{proof}_{\text{id}} \) by encrypting a random string. More precisely, when an oracle \( O_{\text{id}} \) sends an identity proof \( \pi_{\text{proof}} \) to \( C \), \( C \) replaces the \( C_{\text{id}} \) with a \( C'_{\text{id}} \) generated by \( E_{\text{enc}}(pk_{\text{reg}}, r, \text{rn}) \), where \( r \) is a random string sampled uniformly from the plaintext space of the encryption scheme.

Because the responses to the adversary \( A \) in \( \text{Exp}_{\text{final}} \) are independent of the bit \( b \), \( A_{\text{proof}} \) wins the experiment \( \text{Exp}_{\text{final}} \) with probability \( \text{Adv}_{\text{Exp}_{\text{final}}} = 0 \) in the experiment \( \text{Exp}_{\text{final}} \).

Next, we prove that no polynomial-time adversary can distinguish \( \text{Exp}_{1} \) from \( \text{Exp}_{\text{final}} \) except with negligible probability (see below lemma).

**Lemma 1** After \( q_{m} \) queries, \( |\text{Adv}_{\text{Exp}_{\text{final}}} - \text{Adv}_{\text{Exp}_{1}}| \leq q_{m} \cdot \text{Adv}_{\text{enc}} \), where \( \text{Adv}_{\text{enc}} \) denotes the adversary’s advantage in the IND-CCA2 experiment.

**Proof sketch.** We construct an algorithm \( B \), using \( A \) as a subroutine, to win the IND-CCA2 experiment. Define \( \epsilon = \text{Adv}_{\text{Exp}_{\text{final}}} - \text{Adv}_{\text{Exp}_{1}} \).

For some \( i \in \{1, \ldots, q_{m}\} \), when \( A \) issues an \( i \)-th query, \( B \) uses the NIZK extractor \( \epsilon \) to obtain plaintext \( m \) corresponding to \( C_{\text{id}} \). Then, \( B \) chooses a random string \( r \) that has the same length as \( m \). \( B \) sends \( (m_{0}, m_{1}) = (m, r) \) to the IND-CCA2 challenger and receives \( C' = E_{\text{enc}}(pk_{\text{reg}}, r, \text{rn}) \), where \( \overline{b} \) is the bit chosen by the IND-CCA2 challenger. \( B \) replaces \( C_{\text{id}} \) included in \( \text{proof}_{\text{id}} \) with \( C' \). We return \( b' \), which \( A \) outputs as the guess in the IND-CCA2 experiment. We know that when \( b = 0 \), \( A \)'s view of the interaction is distributed identically to that of \( \text{Exp}_{1} \). When \( b = 1 \), \( A \)'s view represents the \( \text{Exp}_{\text{final}} \), in which one ciphertext \( C_{\text{id}} \) has been replaced. Based on a standard hybrid argument over each of the \( q_{m} \) ciphertexts, we can conclude that over the randomness of the experiment, \( B \) must succeed in the IND-CCA2 experiment with the advantage of at least \( \epsilon/q_{m} \).

Therefore, \( |\text{Adv}_{\text{Exp}_{\text{final}}} - \text{Adv}_{\text{Exp}_{1}}| \leq q_{m} \cdot \text{Adv}_{\text{enc}} \).

**B. Proof of identity proof unforgeability**

**Theorem 3** Assuming that the Chash scheme is collision resistant, trapdoor collision and semantic security, the NIZK scheme is perfectly zero-knowledge and simulation sound extractable, \( \text{gen}(\cdot) \) is one-wayness, then, our scheme \( \Pi = (\text{Setup}, \text{Gen}_{\text{in} \text{fo}}, \text{Ver}_{\text{in} \text{fo}}, \text{Gen}_{\text{proof}}, \text{Ver}_{\text{proof}}, \text{Trace}) \) described in Algorithm 1 satisfies identity proof unforgeability.

From experiment \( \text{Exp}_{A, \Pi}^{\text{DP-UNF}}(\lambda) \), we can observe that \( A \) succeeds only if it outputs \( (\text{pub}^*, \text{proof}^\ast_{\text{id}}) \) such that: (i) \( \text{proof}^\ast_{\text{id}} \not\in P \); (ii) \( \text{Ver}_{\text{proof}}(\text{pp}, \text{pub}^*, \text{proof}^\ast_{\text{id}}) = 1 \); (iii) \( \text{proof}^\ast_{\text{id}} \) belongs to the user whose identity is \( \text{id} \). We define the two disjoint events which \( A \) succeeds: (i) \( \text{Event}, A \) succeeds, and \( \text{pub}^* \in T_{\text{pub}} \); (ii) \( \text{Event}, A \) succeeds, and \( \text{pub}^* \not\in T_{\text{pub}} \). Let \( \epsilon \) be the NIZK extractor for \( A \).

Obviously, \( \text{Adv}_{A, \Pi}^{\text{DP-UNF}} = \Pr[\text{Event}] + \Pr[\overline{\text{Event}}] \).

Define \( \epsilon_1 = \Pr[\text{Event}] \) and \( \epsilon_2 = \Pr[\overline{\text{Event}}] \).

When \( \text{Event} \) occurs, we construct the algorithm \( B \). It uses \( A \) as a subroutine, and solves the one-wayness of \( \text{gen}(\cdot) \). Let \( \epsilon \) be the NIZK extractor for \( A \). The algorithm \( B \) works as follows.

1. \( B \) randomly selects \( i \in \{1, \ldots, n\} \).
2. \( B \) performs the experiment \( \text{Exp}_{A, \Pi}^{\text{DP-UNF}}(\lambda) \) with \( A \) to obtain \( (\text{pub}^*, \text{proof}^\ast_{\text{id}}) \).
3. \( B \) runs the \( \epsilon(vk_{\text{proof}}, \pi_{\text{proof}}) \) to obtain \( w_{\text{proof}} = \{\text{path}^\ast_{\text{id}}, CH_{\text{id}}, pk^\ast_{\text{chash}}, sk^\ast_{\text{chash}}, \text{priv}^\ast, r^\ast, \text{rn}^\ast\} \).
4. If \( \text{pub}^* = \text{pub} \), then \( B \) outputs \( \text{priv}^\ast \); otherwise, \( B \) aborts.

Because the index \( i \) is selected at random, \( B \) succeeds with probability \( \epsilon_1/n \). Because of the one-wayness of the \( \text{gen}(\cdot) \), \( \epsilon_1 \) must be negligible in \( \lambda \).

When \( \text{Event} \) occurs, we construct algorithm \( Z \). It uses \( A \) as a subroutine and finds collision for the chameleon hash scheme. \( Z \) sends \( \langle \text{chashset}, \text{proof}^\ast_{\text{id}} \rangle \) to \( O_{\text{reg}} \), and obtains \( P_{\text{chash}} = \{CH_{\text{id}}, \ldots, CH_{\text{id}}\} \) from the oracle \( O_{\text{reg}} \), where \( k < \lambda \). The set \( P_{\text{chash}} \) includes the chameleon hash \( CH_{\text{id}} \) of the user whose identity is \( \text{id} \). The algorithm \( Z \) performs as follows:

1. \( Z \) randomly selects \( i \in \{1, ..., k\} \).
2. \( Z \) performs the experiment \( \text{Exp}_{A, \Pi}^{\text{DP-UNF}}(\lambda) \) with \( A \) to obtain \( (\text{pub}^*, \text{proof}^\ast_{\text{id}}) \).
3. \( Z \) runs the \( \epsilon(vk_{\text{proof}}, \pi_{\text{proof}}) \) to obtain \( w_{\text{proof}} = \{\text{path}^\ast_{\text{id}}, CH_{\text{id}}, pk^\ast_{\text{chash}}, sk^\ast_{\text{chash}}, \text{priv}^\ast, r^\ast, \text{rn}^\ast\} \).
4. If \( CH_{id} = CH_{id}, \) then \( \hat{Z} \) outputs \((priv^*, r^*)\); otherwise, \( B \) aborts.

Because the index \( i \) is selected at random, \( \hat{Z} \) succeeds with probability \( \epsilon_2/k \). Furthermore, because of the collision resistance of the chameleon hash scheme, \( \epsilon_2 \) must be negligible in \( \lambda \).

REFERENCES