AIJR Preprints
Section: Working Paper
Article Id: 346, Version: 1, 2021
DOI: https://doi.org/10.21467/preprints.346
URL: https://preprints.aijr.org/index.php/ap/preprint/view/346

{Click on above link or DOI to see the latest available version of this article}

NOT PEER-REVIEWED

Version 1: Received: 22 October 2021 / Approved: 22 October 2021 / Online: 22 October 2021

Hierarchical Identity-based Broadcast Cryptography and its Application in Blockchain

Chenchen Han*

Advanced Machinery Research Institute, Xinghua Hongwei Fluid Equipment Factory

School of Intelligent Engineering, Taishan Institute of Technology

*Corresponding author's email: hanchen0973@gmail.com

ABSTRACT

Blockchain as an emerging cryptographic database technology has gained wide attention in many directions. Among them, data security is one of the hot spots of research in blockchain. In this paper, we first analyze the security problems of blockchain and then propose to solve them with hierarchical identity-based broadcast encryption (HIBBE). HIBBE, as a variant of hierarchical identity-based cryptography, can effectively improve the data security. HIBBE has all the characteristics of hierarchical identity-based cryptography, so it has potential in decentralized application scenarios. Then we made an overview of the several existing HIBBE scheme. This paper also gives a formal definition of HIBBE and concludes with the research direction of HIBBE-based blockchain.

Keywords: Blockchain technology, Hierarchical identity-based broadcast encryption, Database

1 Introduction

Derived from the underlying technology of Bitcoin, blockchain is a database that relies on technologies such as cryptography and P2P networks [1]. Early applications were primarily cryptocurrency, and as the technology evolved, potential applications for blockchain in other areas were discovered. For example, the blockchain 2.0 era, represented by Ethereum, then emerged [2]. Traditional blockchain mainly relies on hash signature technology to guarantee the integrity of the stored data. However, this was not enough

How to Cite:

Chenchen Han, "Hierarchical Identity-based Broadcast Cryptography and its Application in Blockchain". *AIJR Preprints*, 346, Version 1, 2021.

considering other needs such as anonymity and verifiability. So various cryptographic techniques were used to construct new blockchains, the most typical ones being zero-knowledge proofs and ring-signature schemes [3-5].

Hierarchical identity-based encryption (HIBE) is a variant of identity-based cryptography that extends the identity-based cryptography scheme by organizing users into a tree structure [6]. HIBE supports a key delegation mechanism for advanced users to issue keys to their descendants. During encryption, an identity vector can be specified for a cipher-text instead of a single identity. Users whose identities appear in the specified identity vector can be decrypted. HIBBE further extends HIBE by allowing a person to broadcast a message to multiple recipients in a hierarchical social organization [7, 8]. Similar to HIBE, HIBBE organizes users in a hierarchical structure, and users can delegate their decryption capabilities to subordinates. In encryption, the set of identity vectors containing the intended recipients is associated with the cipher-text. Only users with identities in the identity vector set can decrypt the cipher-text correctly. We believe that HIBBE can be integrated with blockchain to improve the security of blockchain with the features of HIBBE. In this paper, we analyze the possibility of this idea.

The contributions of this paper can be summarized as follows.

1. This paper analyzes the various security issues that exist in blockchain technology today.
2. This paper gives a formal definition of the HIBBE scheme and a definition of security.
3. In this paper, we analyze the possibility of constructing a HIBBE-based blockchain and give future research directions.

The paper is organized as follows. In Section 2, we analyze the security problems of existing blockchains. In Section 3, we introduce the existing HIBBE scheme and give its definition. In Section 4, we present the possibility of constructing a HIBBE-based blockchain and conclude in Section 5.

2 Security Problems in Blockchain Technology

Blockchain is a cryptographic database that focuses on security, but it is not completely secure. So far, there are still many problems. This section summarizes several security issues facing the blockchain, mainly as follows.

2.1 Low Throughput

In Bitcoin, for example, it takes about 10 minutes to confirm a new block, which is very slow. The designers have sacrificed Bitcoin's performance and scalability to some extent to ensure Bitcoin's security. If you adjust the block generation interval or block size on a traditional Bitcoin network, you compromise its security. Low throughput is prone to fork, which is one of the attacks that blockchain often faces and needs to be resolved [9].

2.2 High Energy Consumption

PoW, the consensus mechanism of the blockchain, has serious drawbacks of high energy consumption. The reason is that with the continuous advancement of CPU technology, the computing power of computers has increased geometrically. Since the total amount of Bitcoin remains unchanged (21 million), it is necessary to increase the difficulty of mining to ensure the speed of Bitcoin's block production.

Stable, the use of the PoW consensus algorithm makes it only possible to obtain the right to accounting by constantly trying methods (the most energy-consuming way), thereby increasing energy consumption.

2.3 Privacy Protection

In addition, the blockchain also needs to solve the problem of privacy protection. The public chain is public, which means that everyone can access all the information on the chain, including potentially sensitive information. Therefore, it is especially important to improve the privacy of the blockchain [10]. In the regulatory-focused blockchain, privacy protection is the top priority. Blockchain privacy includes transaction privacy and user privacy. In the supervision-oriented blockchain, the protection of transaction privacy and user privacy is the top priority.

3 HIBBE

3.1 Current Status of HIBBE Research

We will give several common HIBBE schemes in this section, which can be divided into bilinear pair-based and lattice based schemes.

3.1.1 Bilinear Pair-based Scheme

Bilinear pairs are introduced in many papers as one of the important tools for constructing modern cryptographic schemes. HIBBE can be considered as a combination of HIBE and broadcast encryption scheme (BE). As early as 2004, Yao [11] et al. started to study the application of HIBE in broadcast encryption. In 2008, Boneh [12] et al. proposed the first short ciphertext Broadcast HIBE system, which is an early prototype of our current HIBBE system, but Boneh did not give a specific HIBBE scheme.

Subsequently, Liu [7] et al. proposed a method to construct the HIBBE scheme using the composite-order bilinear pairs and in 2016 proposed an improvement to the previous scheme by constructing a new HIBBE scheme using prime-order linear pairs [8]. The new scheme, in which the group operations are more efficient in prime-order bilinear groups, makes the newly proposed HIBBE scheme more practical.

In 2016, Ameri [13] et al. proposed an efficient and provably secure anonymous HIBBE scheme. This scheme constructs an identity-based hierarchical broadcast encryption scheme that protects the privacy of a specific recipient using composite-order bilinear pairs. While with the advantage of HIBBE, we can sign a specified set of verifiers using an identity-based hierarchical signature (HIBS) scheme. This paper also presents a generic construction of a new concept of hierarchical identity based multi-designated verifiable signature (HIB-MDVS).

In 2019, Li [14] et al. proposed a HIBBE scheme using prime-order bilinear pair construction, which supports efficient revocation. The scheme uses a subset-covering revocation framework that divides the key into two parts related to identity and time. This reduces the workload and bandwidth of the Public Key Generator (PKG) and eliminates the need to issue keys to all unrevoked users one at a time using a highly secure key transport channel in normal HIBBE. The PKG shares its burden with high-level users, who can delegate keys and update keys for the corresponding underlying users. The number of update keys that can be publicly broadcast is the logarithm of the number of non-revoked users.

3.1.2 Lattice-based Scheme

Zhang [15] et al. first proposed to construct the HIBBE scheme based on the learning with errors (LWE), in which each user's identity is associated with a lattice matrix, so the relationship between the lattice and its sub-lattices can easily represent the hierarchical identity structure. The short bases of the lattice can be used as the user's private key, so the private keys of users at all levels can be derived based on the SampleBasis algorithm. In addition, the scheme proposed in this paper has higher efficiency in encryption and decryption compared with the broadcast encryption scheme based on bilinear mapping.

Yang [16] et al. proposed a new HIBBE scheme based on learning with errors (LWE) construction in 2014, which achieves random indistinguishability under adaptive choice of plaintext and choice of identity and random prediction model.

3.2 Formal Definition

This section gives the formal definition of HIBBE.

A HIBBE scheme consists of five algorithms, which can be expressed as:

$$\mathcal{T} = (Setup, Extract, Delegate, Encrypt, Decrypt).$$

Each step of the algorithm has a corresponding input, and the output of the image should be obtained. The following is a detailed explanation.

Setup: Input security parameter κ, the maximum depth $\mathcal{D}$ and the size of the receiver set $\mathcal{S}$. Output master key msk and public parameters pp.

Extract: Input master key msk and identity $ID_{|s}$ with depth $\iota(\iota \leq \mathcal{D})$. Output corresponding secret key sk' for the $ID_{|s}$.

Delegate: Input public parameters pp, secret key sk' and a parent identity $ID_{|s}$. Output secret key sk' for the $ID_{|s}$.

Encrypt: Input the public parameters pp, a set of recipients $Set = \{ID_1, ID_2, \dots, ID_n\}_{n \leq \mathcal{S}}$. Output a two-tuple (Hdr, K), where Hdr is the header of the ciphertext, and K is a symmetric key.

Decrypt: Input the public parameters pp, a set of recipients $Set = \{ID_1, ID_2, \dots, ID_n\}_{n \leq \mathcal{S}}$, an identity ID_i and corresponding secret key sk_{ID_i}, and a header hdr. If $ID_i \in Set$ is satisfied, the symmetric key K used to decrypt the message is output.

4 HIBBE-based blockchain

The existing combination scheme is mainly based on the HIBE structure, with a structure similar to the Merkle tree [17-19]. Taking Wan [17] et al.'s scheme as an example, they constructed a decentralized hierarchical identity-based signature scheme (DHIBS) to sign data. Compared with general HIBS, DHIBS uses a verifiable secret share scheme to distribute keys. Figure one shows the principle of this scheme can be described as follows.

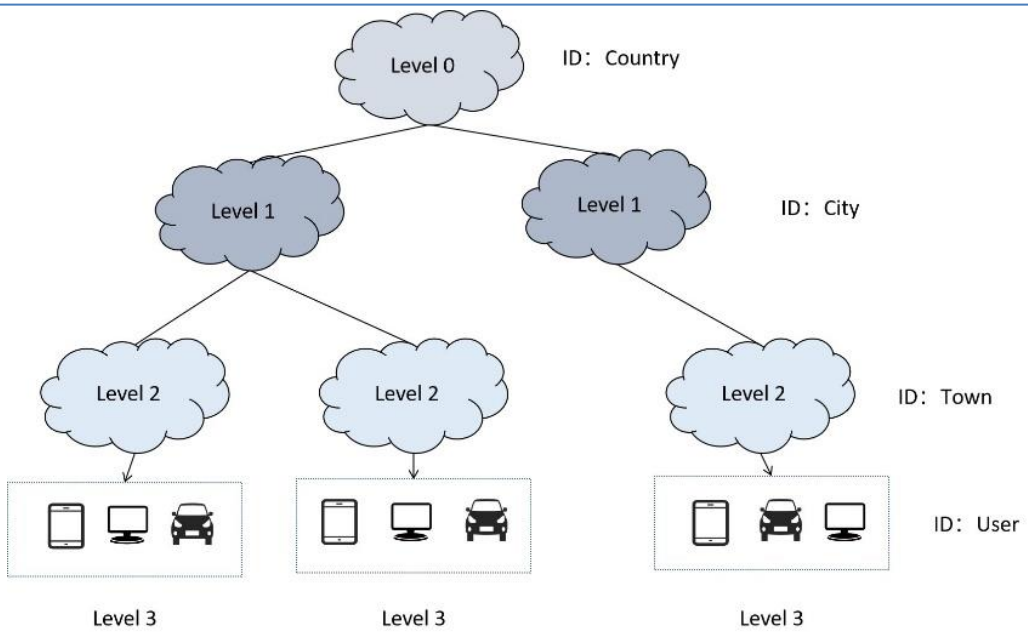

Figure 1: HIBE-based Blockchain

Levels 0-3 successively represent a set of different permissions, of which level 0 has the highest authority. For example, assume that the country is Level 0, and the cities and towns are Level 1 and Level 2, respectively. Level 3 is composed of users.Level 0 is responsible for distributing corresponding keys to lower levels. Level 3 can be composed of a variety of devices, and they have the lowest authority. Their keys need to be distributed by superiors. One of the benefits of the decentralized HIBE solution is that if one of the users of a partial set is attacked, it will not affect the users of the other set.

With reference to above proposals, we propose here two possibilities for the construction of a HIBBE-based blockchain.

- Decentralized HIBBE. Considering large-scale applications such as the Internet of Things, we can also construct an improved decentralized HIBBS scheme and assign permissions to nodes on each layer.
- Block data encryption. The paper [20, 21] gives another possibility. We can directly encrypt the data that needs to be stored in the blockchain, and then perform storage operations. Such a method can improve data security and privacy.

Of course, the existing HIBBE scheme may not be functionally able to meet the needs of the blockchain. Therefore, further improving the HIBBE program is also one of our future research directions. Specific examples include constructing anonymous HIBBE, traceable HIBBE scheme and revocable HIBBE scheme. There is still a lack of work in this area.

5 Conclusions

As a branch of modern cryptography, HIBE has received extensive attention from researchers and has been used to construct improved blockchain mechanisms. HIBBE is a practical variant of HIBE, which also has potential. This paper first analyzes the existing security problems of the existing blockchain, and then proposes to use HIBBE to solve it. Then the formal definition of HIBBE and several existing schemes

are given. Finally, it analyzes the possibility of constructing a blockchain based on HIBBE and possible future research directions.

6 Declarations

6.1 Acknowledgements

Thank you for Advanced Machinery Research Institute's support for this paper.

6.2 Competing Interests

The author declared that no conflict of interest exists in this work

References

[1] Belchior, Rafael, et al. "A survey on blockchain interoperability: Past, present, and future trends." ACM Computing Surveys (CSUR) 54.8 (2021): 1-41.

[2] Imbugwa, Gerald, Mazara Manuel, and Salvatore Distefano. "Developing a Mobile Application Using Open Source Parking Management System on Etherium Smart Contracts." Journal of Physics: Conference Series. Vol. 1694. No. 1. IOP Publishing, 2020.

[3] Yang, Xiaohui, and Wenjie Li. "A zero-knowledge-proof-based digital identity management scheme in blockchain." Computers & Security 99 (2020): 102050.

[4] Li, Wanxin, et al. "Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach." IEEE Access 8 (2020): 181733-181743.

[5] Mundhe, Pravin, et al. "Ring signature-based conditional privacy-preserving authentication in VANETs." Wireless Personal Communications 114.1 (2020): 853-881.

[6] Langrehr, Roman, and Jiaxin Pan. "Tightly secure hierarchical identity-based encryption." Journal of Cryptology 33.4 (2020): 1787-1821.

[7] Liu, Weiran, et al. "Hierarchical identity-based broadcast encryption." Australasian Conference on Information Security and Privacy. Springer, Cham, 2014.

[8] Liu, Weiran, et al. "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption." International journal of information security 15.1 (2016): 35-50.

[9] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375.

[10] Shi, Shuyun, et al. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." Computers & Security (2020): 101966.

[11] Yao, Danfeng, et al. "ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption." Proceedings of the 11th ACM conference on Computer and communications security. 2004.

[12] Boneh, Dan, and Michael Hamburg. "Generalized identity based and broadcast encryption schemes." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2008.

[13] Ameri, Mohammmad Hassan, Javad Mohajeri, and Mahmoud Salmasizadeh. "Efficient and provable secure anonymous hierarchical identity-based broadcast encryption (hibbe) scheme without random oracle." Cryptology ePrint Archive (2016).

[14] Li, Dawei, et al. "Revocable hierarchical identity-based broadcast encryption." Tsinghua Science and Technology 23.5 (2018): 539-549.

[15] Jinman, Zhang, and Chen Qin. "Hierarchical identity-based broadcast encryption scheme on lattices." 2011 Seventh International Conference on Computational Intelligence and Security. IEEE, 2011.

[16] Yang, Chunli, et al. "Hierarchical identity-based broadcast encryption scheme from LWE." Journal of Communications and Networks 16.3 (2014): 258-263.

[17] Wan, Zhiguo, Wei Liu, and Hui Cui. "HIBEChain: A Hierarchical Identity-based Blockchain System for Large-Scale IoT." IACR Cryptol. ePrint Arch. 2019 (2019): 1425.

[18] Pavithran, Deepa, Jamal N. Al-Karaki, and Khaled Shaalan. "Edge-Based Blockchain Architecture for Event-Driven IoT using Hierarchical Identity Based Encryption." Information Processing & Management 58.3 (2021): 102528.

[19] Khan, Saifullah, et al. "Blockchain and the Identity based Encryption Scheme for High Data Security." 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2020.

[20] Khan, Saifullah, et al. "Blockchain and the Identity based Encryption Scheme for High Data Security." 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2020.

[21] Zhang, Meng, et al. "Protecting data privacy for permissioned blockchains using identity-based encryption." 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019.