Overview of Anonymous Authentication in Mobile Communication

Chengzhi Shangguan *

School of North China Electric Power University, Baoding, China

* 424386598@qq.com

Abstract. With the development of mobile communication, while users enjoy higher-value services, they are always concerned about whether their privacy is leaked. Therefore, it is very important to ensure anonymity in the service process. This paper briefly introduces the importance of anonymous authentication, summarizes the commonly used techniques of anonymous authentication such as group signature and ring signature, summarizes the typical anonymous authentication schemes and some existing problems, and points out that anonymous authentication will become the focus of research.

Keywords: Anonymity; Authentication; Privacy Protection; Mobile Communications.

1. Introduction

In the rapid development of mobile communication service, traffic and mobile network optimization at the same time, many new businesses also constantly emerging, such as: multimedia, e-commerce, Internet banking, mobile payment, etc., these business requirements for the user's identity and personal information authentication and verification, but the resulting personal information confidentiality issues. In addition, mobile networks form a vast complex network consisting not only of multiple operators but also of interconnections with networks in other countries around the world. At the same time, the large scale of mobile communication network users and the complex composition of personnel will also bring great threats to our personal information security. There are both authentication and security threats in mobile networks, as well as confidentiality requirements. Therefore, an anonymous authentication service is needed to verify the validity without exposing the identity to meet the above security requirements.

2. Introduction to Anonymous Authentication

Anonymous authentication technology is an important means to realize privacy protection. While providing services for users, it verifies the legitimacy of user identity, but it cannot obtain users' personal information. In order to protect user privacy and provide anonymous services, some applications, such as E_Voting, E_Banldng and E-COMMERCE, have taken anonymity as a measure index. Most schemes of anonymous authentication technology are implemented from the application layer, namely software. This kind of scheme is characterized by both identity verification and anonymity. On the premise of verifying the validity of user identity, anonymous authentication schemes can be roughly divided into two categories according to tracking ability. - Class is an anonymous authentication scheme that can trace the identity of the signer. In this case, the anonymity of the signer's identity is controllable, that is, the administrator can calculate the signer's identity through the threshold information and part of the information provided by the verifier. The second type is anonymous authentication scheme which cannot trace the identity of the signer. The anonymity of signers in such schemes is absolutely secure and there is no way to calculate the identity of signers. The first scheme can be implemented by proxy signature or group signature, while the second scheme can be implemented by ring signature.[1]

To realize information security, identity authentication is an important key link, and the identity authentication requires users to expose their real identities, which precisely reveal the secrets of the user, so the reality presents a problem to us, requires us hand in hand with the identity authentication,

can't reveal personal information of users. And it's almost impossible to actually do that, because in order to verify someone's identity, we have to know who they are, otherwise it's almost impossible. So, there is a workaround, the authentication of identity and the use of the identity to carry out business or use services separate, after the authentication of identity, when customers use services, we will no longer verify their real identity, but use information security technology to verify, in the authentication to ensure that the user's information is not leaked.[2]

3. Common Techniques to Implement Anonymous Authentication Schemes

3.1 Basic Encryption and Decryption Algorithms

Mainly symmetric encryption and decryption and asymmetric encryption and decryption algorithm.

3.2 Message Digest Algorithm and Digital Signature Technology

3.3 Bit Commitment Scheme

Alice wants to promise Bob a bit B (b can also be a sequence of bits), but she does not tell Bob her promise information for the time being, that is, she does not reveal her promised bit value B to Bob, and does not disclose her promise or b until a certain time later. In addition, Bob can confirm that Alice did not change her promise between the time she promised and the time she disclosed B. To put it simply, Alice, the prover, wants to promise a prediction (i.e., 1 bit or sequence of bits) to Bob, the prover, but does not reveal his prediction until a certain time later. On the other hand, Bob wants to make sure that he hasn't changed his mind after Alice has committed to his prediction. In cryptography, this commitment method is commonly called bit-commitment scheme, or bit-commitment for short.

3.4 Cut-and-Choose

With cut-and-choose, Bob, the signer, knows what he's signing, but he doesn't know what he's signing or to whom.

3.5 Blind Digital Signature

The basic idea is that the signer uses the plaintext M as a blind transformation B (m), and B (m) hides the content of M; Then b(m) is given to the signer (arbitrator) to obtain S [b(m)], and the signer obtains s [B (m)] through reverse blind transformation.

3.6 Group Signature

Any member of a group can sign messages anonymously on behalf of the entire group.

3.7 Ring Signature

Ring signature, like group signature, is a signer - fuzzy signature scheme. In ring signature, there is no need to create rings, change or delete rings, assign assigned keys, and revoke the anonymity of signers unless the signers themselves wish to reveal their identities. In the ring signature scheme, the signer first selects a temporary signer set, which includes the signer. Then the signer can use his private key and the public key of others in the signature set to generate the signature independently without the help of others. Members of the signer collection may not be aware that they are included. Ring signature has no trust center, no group establishment process, and the signer is completely correct and anonymous for the verifier. Ring signatures provide an ingenious way to reveal secrets anonymously. This unconditional anonymity of ring signatures is useful in special environments where information needs to be protected for a long time. For example, anonymity must be protected even when RSA is breached.

3.8 Certificate Authority

A Digital Certificate Authority (DCA), also known as a Digital Certificate Authority (DCA), is an organization that issues and manages digital certificates that meet common standards for e-commerce transactions. It often appears as a trusted third party in e-commerce transactions.

4. Research Status of Anonymous Authentication

Anonymous authentication technology is an important means to realize privacy protection. While providing services for users, it verifies the legitimacy of user identity, but it cannot obtain users' personal information. At present, with the development of mobile communication, in order to protect users' privacy while enjoying various services, anonymous authentication technology of mobile communication has been paid more and more attention. Several typical anonymous authentication schemes are summarized below.

Reference [3] proposed a controllable anonymous authentication scheme based on blockchain and decentralized traceable attribute signature. Based on the existing traceable attribute signature scheme, decentralized attribute authorization authority was realized, which enhanced the security of the system and was more in line with the decentralized characteristics of blockchain. Compared with the over-exposure of user identity and attribute information in traditional authentication schemes and the inability of existing anonymous authentication schemes to meet the requirements of supervision audit services, this scheme can ensure that users can implement anonymous authentication and supervise user identity information through the regulatory authorities to prevent the abuse of anonymity. However, there is room for further optimization in computing and storage costs.

The controllable anonymous authentication scheme based on blockchain and decentralized traceable attribute signature includes four roles: decentralized Application (DAPP), attribute authorization authority, regulatory authority and user. The solution flow is shown in Figure 1.

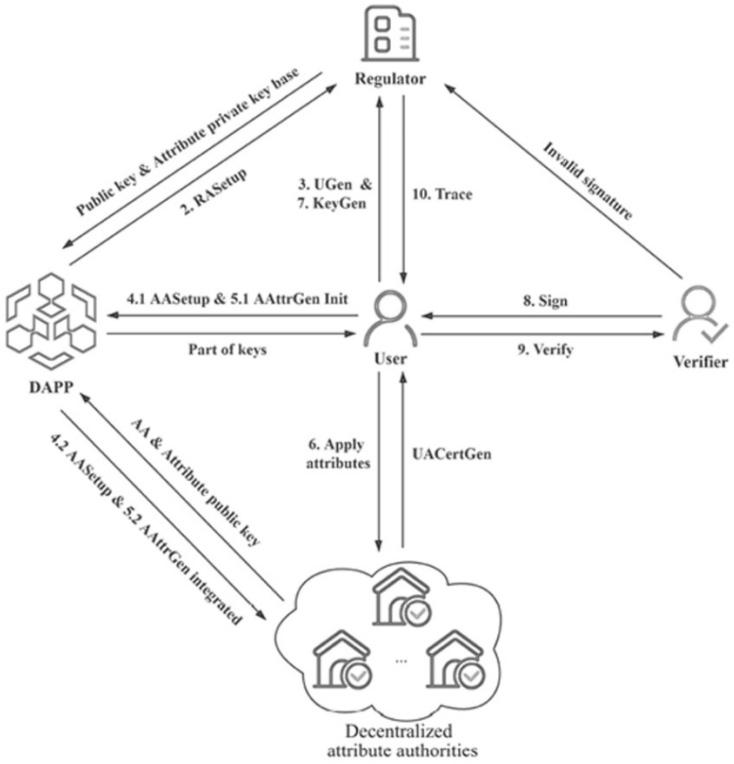

Figure 1. Solution process

The scheme proposed in reference [4] is a typical anonymous authentication scheme involving third-party certification bodies. In the anonymous authentication scheme involving third-party certification bodies:

1) the anonymity of any user can be revoked, and there is no need to embed duplicate payment information during payment;

2) The agreement to identify overpayment and track phone bill holders is the same, the system is simpler;

3) The trusted third party does not need to be online and does not participate in the execution of any other agreement except to track the call fee, track the call fee applicant, and check the overpayment agreement when necessary.

The protocol model is shown in Figure 2.

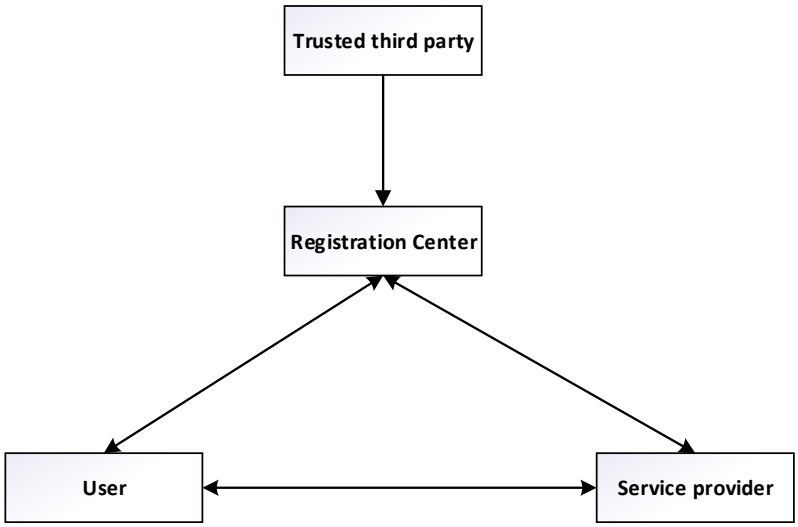

Figure 2. Protocol model

In the anonymous authentication scheme involving third-party authentication bodies, under the circumstance of judicial authorization, the use of third-party authentication bodies can revoke the anonymity of users, reveal the identity of relevant users, so as to achieve the purpose of deterring crimes. However, if in the case of not getting judicial authorization, the registration management center and the third party certification body malicious collusion, in the case of users do not know, but also can view users' privacy, so there is the risk of information leakage. In addition, the scheme involving third-party certification bodies has a complex structure and many participants. Therefore, how to establish a simpler system is an urgent problem to be studied.

Reference [5] To improve network scalability, an effective certificateless aggregate signature scheme without bilinear pairings is proposed. Thus, the key escrow problem in traditional authentication schemes is solved. This scheme is often used in the Internet of vehicles. The combination of the long-term pseudo identity generated by RTA and the short-term pseudo identity generated by the vehicle itself ensures the strong anonymity of the vehicle and the freshness of the signature. The aggregation non-bilinear pairings are used for signature and verification. With the increase of the number of nodes, the verification time of RSUs is greatly reduced and the network scalability is improved. And in the event of malicious events, RTA can track the real identity of the vehicle and revoke the user by TA. The scheme is secure in integrity, privacy, non-repudiation, traceability, anonymity and revocation.

Reference [6] proposed two anonymous authentication schemes using ring signature:

1) Proposed an anonymous authentication protocol based on ring signature and block chain. In a protocol, conditional ring signatures hide the true identity of ring members and do not require the assistance of other members. To reveal the identity of the real signer, the signer can perform the recognition algorithm to prove that it is the real signer, and other ring members can perform the denial

algorithm to find out the real signer. Blockchain has the characteristics of decentralization, tamper-proof and transparency. It uses conditional ring signature to sign user pseudonyms or temporary public keys, and stores signature information in blockchain in the form of Merkle tree. In order to construct a weakly centralized traceable authentication protocol, the authenticity of signature messages can be determined through the consensus protocol of blockchain. When users communicate, they can use the pseudonym after ring signature or temporary public key to communicate, so as to protect user identity privacy. When users do evil things, the real identity of the perpetrator can be revealed through the disclosure algorithm.

2) Proposed an identity privacy protection scheme for Internet of vehicles based on weak centralized authentication protocol. In this scheme, users use ring signature to hide their identity and store it on the blockchain. The consensus nodes on the chain verify the message to ensure the validity and authenticity of signature information and weaken the third party's manipulation of user privacy. The real identity of the user is hidden in the ring members of the ring signature on the blockchain, and the user only needs to carry out hash verification to prove that the user's identity exists on the blockchain during communication, which ensures the privacy of the vehicle's identity and the high efficiency of verification. At the same time, based on the characteristics of conditional ring signature, the scheme is also traceable.

5. Conclusion

With the development of ubiquitous computing and the progress of mobile communication, its openness provides users with great convenience, but also brings greater security threats. Therefore, information security is very important, authentication mechanism is the basis of information security, in the process of identity authentication, not only to ensure the privacy of users, but also to achieve the effect of authentication. It can be seen that the research of anonymous authentication technology will become a hot spot in today's development.

References

[1] Huo Shiwei, Liu Xugang, Chen Quanjin. A review of anonymous authentication research in ubiquitous Environment [J]. Telecom Express,2017(10):30-33.

[2] Liu Jinye. Research on anonymous authentication in Mobile Communication Environment [D]. Beijing University of Posts and Telecommunications, 2013.

[3] Fang Ning, Liu Baixiang, KAN Haibin. A controllable anonymous authentication scheme based on blockchain and decentralized traceable attribute signature [J]. Science China Information Science, 2021, 51 (10):1706-1720.

[4] Zhang Lin-juan, WANG Li-li, JIN Lu, GAO De-yun. Design of Safety Certification Mechanism for Electric Vehicle Charging and Changing Network System [J]. Computer Applications and Software, 2021, 38 (11):338-343.

[5] Liu Xueyan, Wang Li, Huan Lijuan, Du Xiaoni, Niu Shufen. Journal of Electronics & Information Technology, 2022,44(01):295-304. (In Chinese).

[6] Jiang Yuzhang. Based on the ring signature and chain blocks car network privacy protection scheme [D]. Xihua university, 2021. The DOI: 10.27411 /, dc nki. GSCGC. 2021.000243.