International Journal of Information Security and Privacy
Volume 17 • Issue 1

"Every Dog Has His Day": Competitive-Evolving-Committee Proactive Secret Sharing With Capability-Based Encryption

Chuyi Yan, Institute of Information Engineering, Chinese Academy of Sciences, China
Haixia Xu, Institute of Information Engineering, Chinese Academy of Sciences, China*
Peili Li, National Engineering Research Center for Cryptography, China

ABSTRACT

This article proposes a competitive-evolving-committee proactive secret sharing. Every participant in the system has the opportunity to become a member of the holding committee and have sufficient anonymity. During the life cycle of serving as the holding committee members, they only send one message in the protocol without excessive interaction, and achieve receiver strong anonymity with a capability-based encryption scheme different from most public-key encryption schemes, at present named RiddleEncryption, which is also proposed in this paper. In RiddleEncryption the sender does not need to pay attention to the specific identity of the receiver but focuses on what kind of capability the receiver should have. Nobody can determine this kind of capability at the beginning of the system establishment. This article aims at depositing a secret in a distributed manner (e.g., blockchain) without excessive trust and to emphasize more anonymity and capability. The scheme can be used in the dynamic groups, authentication management, rights abuse prevention, and so on.

KEYWORDS

Anonymity, Capability, Communication Protocol, Cryptography, Distributed System, Encryption, Information Theory, Secret Sharing

INTRODUCTION

Distributed systems pursue more rights for each node in the system. The supernodes in the distributed system which appear in some applications, such as the trusted third party, are contrary to the original intention of the distributed system which may cause excessive trust, single point of failure and be tracked.

Considering a scenario that a temporary group is required to do some downstream work depending on the group members capability. How can the dynamic groups be quickly formed? Generally, an authority may point out who the members are or finding some members who you already knew in the real world. But it may cause excessive trust of miss someone who do have such capability. It would

DOI: 10.4018/IJISP.318697 *Corresponding Author

be more secure and ideal if everyone had the opportunity to compete for the group members, which can also mitigate the burden of on single party. This article designed the scheme with the intention of depositing a secret (can be consider as the downstream work requirement) in a distributed manner (e.g., blockchain) without excessive trust and pursuing more anonymity and fairness. Firstly, every node has the opportunity to become the group member, and this group is not permanent, and it will change in the next round. Secondly, it is necessary to consider that people will not expect a single node that handle the downstream work because of the single point failure. So this article considers a group of participants to form groups, which can also be called as holding committee members, and each one holds a part of the secret (can be consider as the symbol of their capability), so put it together and they get the global secret. To resist the collusion attack, the holding committee members should not know who the other holding committee members are during the period of holding the part of the secret. Moreover, they only send one message when something needs to be done in a distributed manner (such as the center generate certificates for users, etc. In this scheme, center members only generate certificates in a distributed manner, and the master private key will not be reconstructed at any time). At the same time, from the attacker's perspective, they do not know who the current holding committee members are, so they cannot launch attacks such as *DDoS (Distributed Denial of Service)*.

To form a dynamic committee, this article use *SS (Secret Sharing)*, and the members of the previous round will send their share to the holding committee members of the next round. However, as long as a message has been sent, the node's identity will be exposed, and there is a risk of being attacked like DDoS. Then the node must complete the secret transmission when sending the message, and the sender needs to know the size of the holding committee in the next round and who they are in advance. Nevertheless, to ensure anonymity, the sender cannot know who they are in advance. So two problems need to consider: 1) How to determine the holding committee members' size to be shared in the next round? 2) How to re-share the secret to the holding committee member in the next round without knowing each other's identity?

In response to the first problem, this article modified the random number generation protocol in Ouroboros (Kiayias et al., 2017). The number of the holding committee members can be determined by all participants in the system together. For the second problem, it means, the sender needs to know the public keys of the holding committee members in the next round, but at this time, these public keys cannot correspond to any receivers like ordinary public-key encryption schemes because this will follow the public key to find the node of the specific receiver and then the adversary can launch a DDoS attack. So this article proposed a capability-based encryption scheme named **RiddleEncryption**. This scheme is similar to the process of guessing a riddle. The public key acts as the $clue$ of the riddle, and the private key acts as the $answer$ to the riddle. All participants can participate in the process of guessing the riddle. If someone guesses the private key correctly, then he will be a holding committee member in the next round. Of course, this will involve difficult problem-solving. The specific parameters set will meet the balance of feasibility and security. In this way, the sender only needs to know what capability the receiver should have without identifying the specific person at all.

Moreover, this article uses the **RiddleEncryption** to construct the **Competitive-Evolving-Committee Proactive Secret Sharing**, and the "authority" in our scheme is obtained by oneself (by solving difficult problems in a limited environment), rather than being granted by a higher-level person in advance. Therefore everyone in the system has the opportunity to be the holding committee member by their capability, which means "Every dog has his day."

Background and Motivation

This subsection compares the strengths and limitations of various popular SS schemes, illustrates the problems of existing schemes with applications that can benefit from SS, and the motivation of using RiddleEncryption to construct our secret sharing scheme.

SS schemes can be broadly classified into three categories: basic SS, roles rights limitation SS, and techniques-based SS. Among them, basic SS can be further subdivided according to the features