Study of Secret Sharing Schemes Using Access Structure

Ashwini Satpute[1], Reshma Batule[2], Shweta Wakalkar[3], Pooja Shelar[4]

[1,2,3,4] Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Abstract: ***Secret sharing schemes (SSS) are used to distribute a highly sensitive secret among a group of individuals so that only when an authorized group of them come together can the secret be reconstructed. The set of these authorized groups is called the access structure. In the outline of threshold schemes, we wanted out of n participants to be able to determine the key. In practice, it is often needed to specify exactly which subset of participants should be able to determine the key and those that should not. The access structure describes all the authorized subsets to design the access structure with required capabilities. In this paper, we have proposed a novel secret sharing scheme with General access structures that is based on the Key-Lock-Pair mechanism. In this paper, associated with each access or is only a key , and associated with each resource is only a lock, and through simple operations on the keys and locks, privacy decisions of the protection system can be revealed. The different qualified subset of participants can cooperate to reconstruct the shared secret, and no unqualified participants can reconstruct the corresponding shared secret.***

Keyword: General Access Structure, Secret sharing, Threshold Scheme, KeLock Pair Mechanism, Qualified subset, Forbidden subset.

1. Introduction

Security is an important issue in information technology. In today's reduced trust world, how to keep the secret information so that it does not depend only on one authority is major problem. While keeping the secret we want to ensure that no single entity is entrusted with too much knowledge or power, the question is how to ensure that secret will not be exploited by the authority holding it.SSS provide solution to such kind of problems.SSS is a method whereby a secret is assigned in n pieces of information called shares or shadows in a such way that1)the secret can be reconstructed from certain authorized groups of shares and 2)The secret key cannot be reconstructed from unauthorized groups of shares. This problem and the first solutions to it were given by Shamir and Blakley in 1979. Shamir's solution to the secret sharing problem is based on polynomial interpolation over a finite field. Many researchers have been proposed threshold secret sharing schemes for number But very few researchers have proposed the general access structure for number secret sharing as it is difficult to add the extended capabilities in general access structure schemes.

In the outline of threshold schemes, we wanted out of n participants to be able to determine the key. But in practice, it is often needed to specify exactly which subsets of participants should be able to determine the key and those that should not. The Access structure describes all the authorized subsets to design the access structure with required capabilities. In this paper we have proposed a general access structure for construction of secret sharing scheme for numbers. Let $P = \{p1, p2, , , pn\}$ be the set of participants. An access structure, denoted by Γ, is a collection of qualified subsets of p. The access structure of a secret sharing scheme satisfies the monotone ascending property, i.e., for any $A \in \Gamma$, $B \subseteq A$ implies $B \in \Gamma$. The traditional (t, n) threshold secret sharing is a special case of general secret sharing.

2. Literature Survey

2.1 Shamir's secret sharing scheme [1979]

Secret image sharing has drawn considerable attention in recent years. A (k, n) threshold secret image sharing scheme, abbreviated as (k, n)-TSISS, encrypts a secret image into n shadow images (also referred to be shadows) in such a way that any k shadows can be used to reconstruct the secret image exactly, but any less than k shadows should provide no information about the secret image. The secret pixel can be hidden in the constant term of a (k - 1)-degree polynomial using Shamir's (k,n) secret sharing scheme, abbreviated as Shamir's (k, n)-SSS , and the secret image can be perfectly reconstructed from any k shadows by Lagrange's interpolation. In Such a case, each shadow is the same size as the secret image. For example, to encrypt a 10GB satellite image by a (5, 10)-TSISS, and get 10 shadows, each with size 10GB; and to reconstruct the 10GB satellite image, and then have to collect 5 shadows, which sum up to 50GB. The larger the amount of information grows, the severer the above problem suffers from. To solve this large shadow size problem in secret image sharing, Thien and Lin embed the secret pixels in all coefficients of a (k-1)-degree polynomial and reduce the shadow size to 1/k of the secret image **[1]**.

2.2 T. Tassa, Hierarchical threshold secret sharing [2007]

Contemplate the matter of threshold secret sharing in groups with hierarchical data structure. In such settings, the key is shared among a bunch of participants that's partitioned into levels. The access structure is then determined by a sequence of threshold requirements: a set of participants is permitted if it's a minimum of k0 members from the best level, additionally as a minimum of k1 > k0 members from the 2 highest levels so forth. Such issues might occur in settings where the participants disagree in their authority or level of confidence and also the presence of upper level participants is imperative to permit the recovery of the common secret. Although secret sharing in hierarchical teams has been studied extensively within the past, none of the prevailing solutions addresses the simple setting wherever, say, a bank

transfer ought to be signed by 3 staff, a minimum of one amongst whom must be a department manager. Tendency to gift an ideal secret sharing scheme for this drawback that, in contrast to most secret sharing schemes that are appropriate for stratified structures, is ideal. As in Shamir's scheme, the key is pictured because the free constant of some polynomial. The novelty of this scheme is that the usage of polynomial derivatives so as to come up with lesser shares for participants of lowers levels. Consequently, this scheme uses Birkhoff interpolation, i.e., the development of a polynomial in keeping with AN unstructured set of purpose and spinoff values. a considerable a part of this discussion is devoted to the question of the way to assign identities to the participants from the underlying finite field so the ensuing Birkhoff interpolation drawback are going to be well expose. In addition, Tendency to devise a perfect and economical secret sharing scheme for the closely connected stratified threshold access structures that were studied by Simmons and Brickell[2].

2.3 C. F. Hsu, Q. Cheng, X. M. Tang, and B. Zeng, An ideal multi-secret sharing scheme based on MSP [2011]

An ideal secret sharing scheme could be a technique of sharing a secret key in some key area among a finite set of participants in such the simplest way that solely the licensed subsets of participants will reconstruct the secret key from their shares that are of identical length as that of the key key. The set of all licensed subsets of participants is that the access structure of the key sharing scheme. In this scheme, tendency to derive many properties and repeat the combinatorial characterization of a perfect secret sharing scheme in Brickell-Stinson model in terms of orthogonality of its representative array. This scheme has two sensible models, particularly the parallel and hierarchical models, for access structures, and then, by the restated characterization, many series of ideal secret sharing schemes realizing special parallel or hierarchical access structure model are made from finite projective planes **[3]**.

2.4 Secret Sharing for General Access Structures ˙Ilker Nadi Bozkurt, Kamer Kaya, and Ali Aydın Selc¸uk

Secret sharing schemes (SSS) are used to distribute a highly sensitive secret among a group of individuals so that only when an authorized group of them come together can the secret be reconstructed. The set of these authorized groups is called the access structure. If the access structure only contains all groups of size larger than a threshold value, the problem is called threshold secret sharing. There exist several efficient solutions in the literature proposed for threshold secret sharing and some methods adapt threshold SSSs to general secret sharing problems where the access structures can be more complex. In this paper, we are interested in the adaptation of threshold SSSs based on the Chinese Remainder Theorem (CRT) for general access structures. Galibus and Matveev (2007) proposed a solution for the same problem. We first modify their algorithm to work over integers rather than polynomials. Then we show that this modified algorithm is impractical and propose another one based on splitting the secret into multiple parts. Experimental results show that the proposed solution is better than the former in terms of the information rate.

2.5 A dynamic key lock pair access control scheme vol 10, issue to April 1991

Based on the concept of an access control matrix, a new dynamic access control scheme for frequently inserted or deleted users and files is proposed. The main idea of this paper is inspired by the mechanism of key-lock-pair proposed by Chang and Jan in which we replace the representation in modulo and the product of different primes with the representation in basis *t*, where *t* is the number of access control privileges. Our scheme associates each user with a user key and each file with a file lock. Through a simple operation on keys and locks, the corresponding privilege can easily be revealed. Moreover, by applying our scheme, whenever a new user or file is joined to the file system, the corresponding key values and lock values will be determined immediately without changing any previously defined keys and locks. Our scheme may be the first attempt for processing frequently deleted users or files. Whenever a user or a file is deleted from the protection information system, only some relevant keys or locks need to be modified. In addition, any updating of privilege values can also be implemented easily

3. Comparison Table

Schemes Parameters	*Shamir's Scheme [1]*	*Hierarchical threshold SS Scheme [2]*	*Ideal multi secret sharing[3]*	*Secret sharing with general access structure*	*General Access structure scheme*
Threshold	'k' number of participants should be present out of total 'n' participants to reconstruct the secret (k,n)	'k' number of participants should be present out of total 'n' participants to reconstruct the secret (k,n)	All participants should be present out of total n participants to reconstruct the secret (2,2)	'k' number of participants should be present out of total 'n' participants to reconstruct the secret (k,n)	Specific 'k' number of participants in Access Structure should be present to reconstruct the secret (k,n)
Ideal	Yes	No	Yes	Yes	Yes
Security of Scheme	Security is Less, as if value of k is known ,then secret can be found by any unauthorized third party	Security is of not guarantee	Security is of not guarantee	Security is provided due to construction of Access Structure	Security is more as the Access Structure cannot be found by any unauthorized third party
Multiple secret sharing	Only a single secret can be shared and reconstruct	Only a single secret can be shared and reconstruct	More then one secret can be shared and reconstruct	Only a single secret can be shared and reconstruct	Only a single secret can be shared and reconstruct
Secure channel required	Yes	yes	yes	yes	yes

4. Some Definition

- **Secret**: Something that is kept or meant to be kept unknown or unseen by others.
- **Shadow**: Shadow is also known as shares. Shadow is a part of the secret which is to be shared among qualified participants of subset
- **General Access Structure**: The Access structure describes all the authorized subsets to design the access structure with required capabilities.
- **Qualified Subset**: The participants in a qualified set can collaboratively recover the secret. It is denoted by Γ Qual.
- **Forbidden Subset**: The participants in a forbidden set cannot recover the secret. It is denoted by Γ Forb.

5. Conclusion and Future Scope

In this paper we have tried to analyze mapping of different secret sharing schemes in Shamir secret sharing scheme, general access structure is not use instead threshold value is used to reconstruct the secret thus security is not much achieved in these scheme .In Hierarchical threshold secret sharing ,the secret is shared among a group of participants that is partitioned into some levels and the corresponding access structure is determined by a sequence of threshold requirements therefore access structures can easily be determined if value of threshold is already known . Hence the improved scheme for secret sharing with general access structure is more secured and more efficient then previous schemes as access structure is constructed based on real time situation

6. Appendix: SSS

Secret sharing scheme in which a secret known to only dealer is to divided among n others participants .This is done in such a way that a certain number k of these participants is necessary to reconstruct the secret

7. SSS with General Access Structure

Secret sharing scheme is a system for the protection of a secret among a number of participants in such a way that only certain subsets of these participants (access structure) can reconstruct the secret, and the remaining subsets can obtain no additional information about the secret**.**

References

[1] Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.
[2] T. Tassa, Hierarchical threshold secret sharing, Journal of Cryptology , vol. 20, no. 2, pp. 237-264
[3] F. Hsu, Q. Cheng, X. M. Tang, and B. Zeng, An ideal multi-secret sharing scheme based on MSP Journal of Information Sciences, vol. 181, no. 7, pp. 1403-1409, 2011.
[4] An explication of secret sharing schemes with general access structure Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande Pimpri Chinchwad College of Engineering, Nigdi, Pune, India
[5] A Novel (t, n) Threshold Secret Sharing Using Dot Product of Linearly Independent Vectors International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013
[6] Analyzing Relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes IJCSI International Journal of Computer Science Issues Vol. 9, Issue 3, No 1, May 2012