Analyzing Relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes

Sonali Patil[1] and Prashant Deshmukh[2]

[1]PhD student, Sant gadgebaba Amravati University, Amravati - 444 602, Maharashtra India

[2]Professor and Head, Sipna College of Engineering and Technology, Amravati – 444 701, Maharashtra India

Abstract

Secret Sharing Schemes (SSS) refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. Secret sharing has been an active research field for many years by mathematicians as object of intrinsic interest in their own right, cryptographers as important cryptographic primitives and security engineers as technique to employ in distributed security applications. In many circumstances, secret sharing has to provide more flexibility and functionality as per the need of an application. The intent of this paper is analyzing relation in application semantics and extended capabilities such as general access structure, verifiability of shares, cheater identification, enroll and dis-enroll of shareholders, recover lost or corrupted shares and periodically renew shares.

Keywords: *Secret Sharing, Network security, Multi functionality, Extended Capabilities, Cryptography*

1. Introduction

The effective and secure protections of sensitive information are primary concerns in commercial, medical and military systems. Needless to say, it is also important for any information process to ensure data is not being tampered. Encryption methods are one of the popular approaches to ensure the integrity and secrecy of the protected information. Public key encryption is a powerful mechanism for protecting the confidentiality of secure information. In those methods, secrets can be protected by more than one key. However, one of the critical vulnerabilities of encryption techniques is the single-point-failure. For example, the secret information cannot be recovered if the decryption key is lost or the encrypted content is corrupted during the transmission. Backup copies are created to protect cryptographic keys from loss or corruption. The problem is, the greater the number of copies made, the greater the risk of security exposure, and smaller the number of copies made, the greater the chance that all of them are lost. To address these reliability problems, a secret sharing scheme (SSS) is a good alternative to remedy these types of vulnerabilities. Secret sharing schemes allows improving the level of protection without increasing the risk of exposure.

There are circumstances where an action is required to be executed by a group of people. For example, to transfer money from a bank a manager and a clerk need to cooperate. A ballistic missile should only be launched if three officers authorize the action. In communications networks that require security, it is important that secrets be protected by more than one key. Furthermore, a system of several keys that can be combined in multiple ways may allow for the recovery of a unique secret regardless of how they are combined. Schemes that have a group of participants that can recover a secret are known as Secret Sharing Schemes.

The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst users by the dealer. Only certain groups (authorized subsets of participants) can reconstruct the original secret. More formally a Secret Sharing Scheme (SSS) is a method whereby n pieces of information called shares or shadows are assigned to a secret key K in such a way that: i)The secret key can be reconstructed from certain authorized groups of shares and ii) The secret key cannot be reconstructed from unauthorized groups of shares.

The rest of the paper is organized as follows. In Section 2 some definitions are discussed. Section 3 covers various secret sharing schemes as threshold schemes, secret sharing with general access structure, verifiable secret sharing schemes and proactive secret sharing schemes. In section 4 performances of these schemes based on various parameters like ideal, perfect, multi functionality and extended capabilities are analyzed. Also applications and required features of secret sharing schemes is discussed. Finally in section 5, we summarize this survey based on their comparative results.

2. Some Definitions

Formal foundation of secret sharing was formulated using the information theory. Two important concepts were defined based on information rate: ideal and perfect schemes.

Information Rate: The information rate was studied by Stinson [1]. It is a measure of the amount of information that the participants need to keep secret in a secret sharing scheme. The information rate for a particular shareholder is the bit-size ratio (size of the shared secret) / (size of that user's share). The information rate for a secret sharing scheme itself is the minimum such rate over all participants [2]. The efficiency of a secret sharing scheme is measured by its information rate.

Perfect: A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S whatsoever, in the information theoretic sense [2] [3].

Ideal Secret Sharing: Secret sharing schemes with information rate 1 are called ideal [4]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

3. Secret Sharing Schemes: A bird's eye view

3.1 Threshold Schemes:

First threshold schemes were independently invented by both Adi Shamir [5] and George Blackley [6] in 1979. The definition outlined in [1] to describe what a threshold secret sharing scheme is:

Definition: Let t and n be positive integers, $t \leq n$. A (t, n) - threshold scheme is a method of sharing a key K among a set of n players (denoted by P), in such a way that any t participants can compute the value of K, but no group of t-1 participants can do so.

The value of t is chosen by a special participant which is referred to by [1] as the dealer. When D wants to share the key K among the participants in P, gives each participant some partial information referred to earlier as a share. The shares should be distributed secretly, so no participant knows the share given to any other participant. At some later time, a subset of participants $B \subseteq P$ will pool their shares in an attempt to compute the key K. Alternatively they could give their shares to a trusted authority which will perform the computation on their behalf. If $|B| \geq k$, then they should be able to compute the value of K as a function of the shares they collectively hold. Furthermore if $|B| < t$, then they should determine nothing about the value of K.

Shamir's (t, n) threshold scheme is based on Lagrange's Interpolating polynomial. This scheme is information-theoretically secure scheme. By using Shamir's threshold scheme concept we can get a very robust key management scheme. [7] [8] [9] are some threshold schemes proposed in recent years.

In a traditional (t, n)-threshold secret sharing scheme, the secret key K can be shared only one time for this reason that one of participants, who participates in reconstruction of K, may be dishonest and probably leaks K. Chunming Tang and Zheng-an Yao [7] proposed a threshold scheme based on multi-prover zero-knowledge arguments and secure multi-party computation protocol. They construct a (t, n)-threshold secret sharing scheme in which the secret key K will be shared forever if at most $t-1$ participants are dishonest and discrete logarithm problem is hard. Chou, Lin and Li [8] proposed a threshold scheme using Sudoku. This method has an advantage to increase secret data delivery security, because the total number of possible solutions in Sudoku is extremely large.

Shi and Zong [9], pointed the problem of increasing the threshold value of the Shamir's (t, n)–threshold scheme without the dealer's helps. In this scheme, the dealer needs not to pre-compute or publish any information in advance, all participants cooperate to take on the dealer's role and to complete the share renewing, and each participant only stores one share as the same size of the secret. The results of analysis show that the proposed scheme is secure, and it is perfect and ideal. In this scheme all participants cooperate to take on the dealer's role and to complete the share renewing and each participant only stores one share as the same size of the secret. And it needs not the dealer's assistance to pre-compute the public information in advance. During the secret reconstruction phase, any t participants can reconstruct the secret *s* rightly and but no subset of less than participants can gain information on the secret. Thus, the proposed scheme is perfect and ideal. (t, n) threshold agreement certificate is introduced in [10].

Threshold schemes are ideally suited to situations where a group of mutually suspicious individuals with conflicting interests must cooperate.

Drawback: In novel (t, n) threshold schemes the

additional capabilities are not concerned.

3.2 Secret Sharing Schemes with General Access Structure:

In the outline of threshold schemes, we wanted k out of n participants to be able to determine the key. In practice, it is often needed that only certain specified subsets of the participants should be able to recover the secret. A more general situation is 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.

Let's denote Γ as being a set of subsets of P, and the subsets in Γ as being the subset of participants that should be able to compute the key. Then Γ is denoted as being the access structure and the subsets in Γ are called authorized subsets. Furthermore if we let K be the set of keys and S be the share set, we use the dealer D to share a key k Є K by giving each player a share S_i Є S. Sometime later a subset of players might attempt to determine K from the shares they collectively hold.

Definition (Stinson, [1]) A perfect secret sharing scheme using the general access structure Γ, is a method of sharing a key K among a set of n participants such that P is the set of all participants, in such a way that the following two properties are fulfilled:

- If an authorized subset of participants $B \subseteq P$ pool their shares, so that they can determine the value of K.
- If an unauthorized subset of participants $C \subseteq P$ pools their shares, then they can determine nothing about the value of K.

It is noticed that a (k, n)-threshold scheme creates the access structure $\{B \subseteq P \mid |B| \geq t\}$. This structure is referred to by Stinson [1] as the threshold access structure. It is possible to create a SSS for any access structure as long as this access structure satisfies monotone property:

- subset B Є Γ and $B \subseteq C \subseteq P$ then C Є Γ.

In other words a superset of an authorized set is again an authorized set.

For (t, n) threshold scheme design of access structures is difficult. Ito, Saito [11] provided a new methodology to design a secret sharing scheme realizing any given access structure. However the number of shadows used in the scheme might be quite large although it is bounded. K. Srinathan [12] describes non perfect general access structure. He considered the problem of non-perfect secret sharing (NSS) over general access structures, defined a more general notion of access hierarchies and studied their tolerability properties. Benaloh [13] presented a view that a threshold scheme is only a particular case of general access structure. For any given polynomial P, the number of n-variable monotone formulae of size no more than P(n) is exponential in P(n). However the total number of monotone functions on n variables is doubly exponential in n. Therefore, most monotone access structure cannot be realized with a large number of polynomial sized shares. Pang [14] proposed an efficient sharing scheme with general access structure. Sai-zhi [15] proposed a novel general access structure for multiple secret sharing, which is based on Shamir's secret sharing scheme and the discrete logarithm problem. In this scheme, the dealer need not send any secret information to participants. And the shared secret, the participant set and the access structure can be changed dynamically without updating any participant's secret shadow. The degree of the used Lagrange interpolation polynomial is only one, which makes the computational complexity of the proposed scheme very low.

Drawback: To add extra functionalities is difficult with general access structures.

3.3 Verifiable secret sharing schemes (VSS schemes) / Schemes with cheating detection and cheater identification:

In the previous scheme we assumed that the Dealer is reliable, however, a misbehaving dealer can deal inconsistent shares to the participants, from which they will not be able to reconstruct a secret. To prevent such malicious behavior of the dealer, one needs to implement a protocol through which a consistent dealing can be verified by the recipients of shares. The problem of verifiable secret sharing [15] is to convince shareholders that their shares (collectively) are, t-Consistent, meaning that every subset of *t* shares out of *n* (that the Dealer distributed) defines the same secret.

Of course if the shareholders would transfer their shares, they could easily confirm consistency, however this would contradict the purpose of the secret sharing scheme.

There are two versions of verifiable secret sharing

protocols: Interactive proofs and non Interactive proofs. Both versions allow the validity of secret shares to be verified without their being revealed; a shareholder can obtain high confidence that he/she holds a valid share of the secret rather than a useless random number.

VSS: Interactive Proof

There are two different interactive proofs for VSS as per Benaloh [13]. In the first protocol we assume that the shareholders do not cheat. In the second protocol we do not assume that.

- Dealer Cheating (Trusted Shareholders, Untrusted Dealer)
- Shareholders Cheating (Trusted Dealer, Untrusted Shareholders)

But the question that one may ask is what if a conflict occurs? We cannot determine who is cheating: the Dealer or one of the shareholders.

Drawbacks to interactive proofs:

Such an interactive proof asserts a proof only to the participants of this protocol, and only at the moment it is held. These proofs have no meaning for a person who is not online and does not participate in the random selections. As a result, these proofs are not valid to a third party, and in particular, they cannot be legal proofs in court.

VSS: Non Interactive Proof

Contrary to the previous protocols, in a Non Interactive Proof scheme [18], only the dealer is allowed to send messages, in particular the shareholders cannot talk with each other or with the dealer when verifying a share. The basic idea is that the dealer sends extra information to each participant during the distribution and each participant verifies that his/her secret share is consistent with this extra information.

The cheater problem is a serious obstacle for secret sharing schemes. A cheater is a qualified participant who possesses a true share, but releases a fake share or withholds a share during a reconstruction of the secret. If a cheater releases a fake share or withholds a share on secret reconstruction, then he/she can obtain the secret and exclude others. Thus, the cheater has an advantage over the other shareholders. Rabin et al. used an information checking protocol [18] to verify the validity of each share and thereby detect cheaters. VSS allows detecting cheating by secret participants and/or the secret dealer (e.g. [19] [20]). Verification capability is especially important, if secret consistency is crucial. Cheating can result not only in obstruction of the protocol, but also may allow dishonest parties to recover secret on their own [21]. Verification process requires presence of trusted third party or can be performed directly between parties of the protocol. When it takes place in public or uses publicly available data PVSS [22] is there.

Publicly Verifiable Secret Sharing: Publicly verifiable secret sharing plays an important role in escrow-cryptosystems, electronic voting and other applications. In this paradigm, not only the shareholder himself but also everybody can verify the correctness of his share. A Publicly Verifiable Dynamic Sharing Protocol is suggested by Jai Yu [23] for Data Secure Storage.

In order to prevent rational participants cheating during the secret sharing process, the extensive form game theory was introduced to the secret sharing scheme .The dealer distributed several sub-secret shadows instead of the secret shadows to each participant, from which a multi-round game model was constructed to simulate the secret sharing process. The designed game strategies made rational participants not distinguish which round was the last one of the game and have no incentive to cheat. It ensures all participants could receive the secret, realizing the fairness. Detecting Dealer Cheating [24] and Resistance against cheating [10] describes some methods for verifying cheating.

Yongquan CAI [25] proposed a cheat-proof rational secret sharing scheme applying the extensive form game to the secret sharing. Rational participants implement multi-round game to realize the rational secret sharing, which not only verifies whether the participants and dealer are cheater, but ensure the rational participants have no incentive to deviate from the protocol. (t, n) threshold agreement certificate is introduced in [10].

Detecting Dealer Cheating [24] proposed a method to handle the detection of that the dealer uses wrong degree of the polynomial which the dealer chooses to hide the key. The main idea of the proposed method is that they ask the dealer to generate a certificate polynomial and one-bit verifying keys to provide information when participants do the detection process.

Resistance against cheating [10] describes some methods for verifying cheating. In this paper they

proposed a notion, the (t, n)- threshold agreement certificate. The (t, n)-threshold agreement certificates of a secret are also shadows derived from the original secret using a different access structure. Based on these certificates, a (*t, n*)-threshold secret sharing scheme is presented which can resist participants cheating. That is, any participant's cheating would not work in the proposed scheme provided that the assumptions in the paper are true.

Drawback: Many of the proposed schemes are providing cheating verification but not cheater identification.

3.4 Proactive Secret Sharing:

The Secret Sharing scheme assumes long-lived shares; however the protection provided by this scheme may be insufficient. The security in a system that is exposed to attacks and break-ins might become exhausted; several faults might occur:

- Secrets can be revealed.
- Shares can gradually be corrupted / compromised.
- Hardware failure or damage, for example reboot, power failures etc.

The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it, in particular any group of *t* non-faulty shareholders should be able to reconstruct the secret whenever it is necessary.

Proactive secret sharing scheme (PSSS) was introduced to improve security through periodic executions. With no PSSS, using an (t, n)-threshold secret sharing scheme, SSS can tolerate up to t-1 compromised shares. Given enough time, a hacker may be able to compromise enough shares (t or more) to gain the secret. PSSS is a scheme that allows generating new set of shares for the same secret from the old shares without reconstructing the secret. Using PSSS, all the shares are refreshed so that old shares become useless. Thus, an adversary has to gather at least t shares between two executions of PSSS. The secret remains confidential if fewer than t shares were compromised from the start of one PSSS to the end of the next PSSS. The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it; In particular any group of t non-faulty shareholders should be able to reconstruct the secret whenever it is necessary.

The term pro-active refers to the fact that it's not necessary for a breach of security to occur before secrets are refreshed, the refreshment is done periodically (and hence, proactively).

Several PSSS have been proposed. Bai [26] has proposed a PSSS based on Shamir [5] secret sharing scheme based on matrix projection method. Optimum secret sharing is described by Zhengjun [27]. They extend the secret *s* in the Shamir's scheme to an array of three elements, *(s, e0, e1)*, and construct two equations for checking validity. Each item in the equations should be reconstructed using Lagrange's interpolation. In this paper, the schemes are revisited by introducing a public hash function to construct equations for checking validity. The revisited scheme is more efficient because they only extend the secret to an array of two elements.

Jia Yu [28] proposed a publicly verifiable secret sharing with enrollment ability. The scheme can provide a share to an enrolling member without exposing the secret and other shares. What's more, because the dishonest behavior of old shareholders can be detected, the new player can verify whether his share is right or not. The scheme can provide a share to an enrolling member without exposing the secret and other shares. The new player can verify whether his share is right or not.

Drawback: The scheme should more secure and efficient. This should be performed without, of course, any information-leak or any secret change. Unfortunately, in a normal publicly verifiable secret sharing, new members can't enroll the system according to the need of actual circumstance because the normal publicly verifiable secret sharing has no this ability.

After this little survey it can be thought that many kinds of secret sharing techniques have been developed to secure data, but none is with all augmented capabilities like robustness against cheating shareholders, verifiability of the shares, proactive redistribution of shares, share generation and set-up of the scheme, protecting against cheating, and dealing with un-trusted parity, etc. These extra functionalities attract our attention, and we are also eager to know their specific implementation methods.

Following section gives performance analysis of few schemes.

4. Performance analysis of schemes

Table I shows application type and the required additional feature of secret sharing schemes. Few secret sharing schemes are considered for comparative study based on some parameters. Table II summarizes that:

Table I. Application Type and Required Features of Secret Sharing Schemes

Application Type	***Required feature of secret sharing***
Transfer money from a bank	Threshold schemes
Launching of a ballistic missile	Threshold, General Access Structure
Communications networks	Ideal, Perfect, Low complexity
Trusted Shareholders, Untrusted Dealer	Verifiable Secret Sharing
Trusted Dealer, Untrusted Shareholders	Verifiable Secret Sharing, Periodically Renew Share
Electronic voting	Publicly Verifiable Secret Sharing
Private querying of database	Low Complexity, Threshold
Collective Control	Periodically renew shares, Enroll/dis-enroll shareholders, Recover lost share
escrow-cryptosystems	Publicly Verifiable Secret Sharing
Secure Storage	Ideal, Reliable, General Access Structure

Table II. Comparison of secret sharing schemes on various extended capabilities

Authors	***Perfect***	***Ideal***	***Flexibility***	***Security***	***Multi functionality***		***Extended Capabilities***			
			Threshold Scheme (k, n)	***Computation Time Complexity***	***General Access Structure***	***Periodically Renew Shares***	***Enroll / Disenroll Shareholders***	***Verifiability of Shares***	***Cheater Identification***	***Recover lost shares***
G. Blakely [6]	No	No	Yes	Low	No	No	No	No	No	No
Tang, Yao [7]	Yes	Yes	Yes	Low	No	No	No	Yes	No	No
Chou, Lin, Li [8]	Yes	Yes	Yes	Very Low	Yes	No	Yes	No	No	No
Shi, Zhong [9]	Yes	Yes	Yes	Low	No	Yes	No	No	No	No
K. Srinathan [12]	No	Yes	Yes	High	Yes	No	No	No	No	No
Staddler [22]	Yes	Yes	Yes	High	No	No	No	No	No	No
Bai [26]	Yes	Yes	Yes	High	No	No	No	No	No	No
Jai Yu [28]	Yes	Yes	Yes	High	No	No	Yes	No	No	No
Chan, Chang, Wang [10]	Yes	No	Yes	High	No	No	No	Yes	No	No

5. Conclusion:

In this paper several extended capabilities of secret sharing schemes like general access structure, verifiability of shares, cheater identification, enroll and dis-enroll of shareholders, recover lost or corrupted shares and periodically renew shares are discussed. Table I gives comparison of some secret sharing schemes based on some parameters like complexity measure, perfect, ideal and extended capabilities. Table II summarizes application semantic and required extended capability feature of secret sharing schemes. There is a lot advancing (steadily but surely) in secret sharing. Applications for secret sharing schemes seem to be getting more important. There is a need to extend the research for analysis for finding relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes. We can expect more rationalization of secret sharing schemes in the near future.

6. References

[1] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.
[2] Menezes, A., P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 524-528
[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
[4] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp. 207–216.
[5] Shamir, A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.
[6] G. Blakely, "Safeguarding cryptographic keys", presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1997, pp. 313–317.
[7] Chunming Tang, Zheng-an Yao, "A New (*t*, *n*)-Threshold Secret Sharing Scheme", International Conference on Advanced Computer Theory and Engineering, IEEE 2008 p. 920-924.
[8] Yung-Chen Chou, Chih-Hung Lin, Pao-Ching Li, Yu-Chiang Li, "A (2, 3) Threshold Secret Sharing Scheme Using Sudoku", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE 2010.
[9] Runhua Shi, Hong Zhong, "A Secret Sharing Scheme with the Changeable Threshold Value", International Symposium on Information Engineering and Electronic Commerce, IEEE 2009 p. 233-236.
[10] Chao-Wen Chan, Chin-Chen Chang, Zhi-Hui Wang, "Cheating Resistance for Secret Sharing", International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009 IEEE p. 840-846.
[11] Mitsuru Ito, Akira Saito, Takao Nishizeki, "Secret Sharing Scheme: Realizing General Access Structure", GLOBECOM IEEE 1987.
[12] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan, "Non-perfect secret sharing over general access structures," in INDOCRYPT, 2002, pp. 409–421.
[13] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27-35.
[14] Pang, L.-J., Li, H.-X., Wang, Y.-M., "A secure and efficient secret sharing scheme with general access structures", Lecture Notes in Computer Science v 4223 LNAI, Fuzzy Systems and Knowledge Discovery - Third International Conference, FSKD 2006, Proceeding 2006, p. 646-649.
[15] Sai-zhi Ye, Guo-xiang Yao, Quan-long Guan, "A multiple secret sharing scheme with general access structure, International Symposium on Intelligent Ubiquitous Computing and Education, 2009 IEEE.
[16] Stadler, M., "Publicly verifiable secret sharing", Lecture notes in Computer Science, 1997, 190-199.
[17] P. Feldman, A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427--437. IEEE, 1987
[18] Rabin, T., and M. Ben-Or, Verifiable secret sharing and multiparty protocols with honestmajority, Proceedings of the 21st ACM Symposium on the Theory of Computing, 1989, pp.73-85.
[19] T. P. Pedersan, "Non-Intractive and Information-Theoretic Secure Verifiable Secret Sharing", Lecture notes in Comuter Science, 1992, pp.129-140 (Advances in Cryptology – CRYPTO' 91).
[20] C. Dwork, "On verification in Secret Sharing", Lecture notes in Comuter Science, 1992, pp.114-128 (Advances in Cryptology – CRYPTO' 91).
[21] Tompa, M., and Woll, H. "How to share a secret with cheaters", Journal of Cryptology, Vol.1, No.2, 1998, pp.133-138.
[22] M. Stadler, "Publicly Verifiable Secret Sharing", Lecture notes in Computer Science, 1997, 190-199 (Advances in Crptology – EUROCRYPT'96).
[23] Jia Yu, Fanyu Kong, Rong Hao, Zhen Cheng, "A Publicly Verifiable Dynamic Sharing Protocol for Data Secure Storage", Ninth International Conference on Web-Age Information Management 2008 IEEE.
[24] Chin-Chen Chang, Chao-Wen Chan, "Detecting Dealer Cheating in Secret Sharing Systems", Proceedings of the Twenty-Fourth Annual International Computer Software & Applications Conference (COMPSAC'00), IEEE 2000.
[25] Yongquan CAI, Xiaofeng REN, "A Cheat-proof Rational Secret Sharing Scheme", Journal of Computational Information Systems, (2011) p. 88-96, January 2011.
[26] Bai, L. and Zou, X. (2009) 'A Proactive Secret Sharing Scheme in matrix projection method', *Int. J. Security and Networks*, Vol. 4, No. 4, pp.201–209.
[27] Zhengjun Cao, Olivier Markowitch, "Two Optimum

Secret Sharing Schemes Revisited", International Seminar on Future Information Technology and Management Engineering, 2008 IEEE, p. 157-160.

[28] Jia Yu, Fanyu Kong, Rong Hao, "Publicly Verifiable Secret Sharing with Enrollment Ability", ACIS, IEEE 2007.