Sequential Secret Sharing Scheme Based on Level Ordered Access Structure

Dileep Kumar Pattipati[1]*, Appala Naidu Tentu[2], V. Ch. Venkaiah[3], Allam Appa Rao[2]

(Corresponding author: Appala Naidu Tentu)

Computer Science and Engineering, IIT Madras, Chennai-600036, India[1]

CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science, University of Hyderabad Campus[2]
Hyderabad-500046, India

School of Computer and Information Sciences, University of Hyderabad, Hyderabad-500046, India[3]

(Email: naidunit@gmail.com)

(Received Dec. 26, 2014; revised and accepted Jan. 16 & Mar. 4, 2015)

Abstract

In Software Industry an application can be released to production only after it has gone through Unit testing, followed by Integration testing, then System testing and finally Acceptance testing. Note here that without the completion of unit testing, integration testing cannot be started and similarly without the completion of integration testing, system testing cannot be started and so on. That is the ordering is important. To realize this or similar kind of activity we need a hierarchial access structure that has in built ordering among the levels. Existing access structures fail to realize this scenario as they are short of enforcing the required ordering. The purpose of this paper is to propose an access structure that caters to this kind of scenarios and come up with schemes that realize this access structure. We call this new access structure as Level Ordered Access Structure(LOAS) and the schemes that realize this access structure as Level Ordered Secret Sharing(LOSS) schemes.

Keywords: Level ordered access structure, level ordered secret sharing, ordered hierarchial, threshold secret sharing

1 Introduction

Secret sharing is a cryptographic primitive which is used to distribute a secret among a group of players. It is simply a special form of key distribution [14]. The distribution is such that any group of authorized players can always reconstruct the secret, whereas an unauthorized group can never obtain any information about the secret. The first secret sharing scheme was designed independently by Shamir in [12] and Blakley in [4]. The approach in [12] relies on Lagrange polynomial interpolation, whereas the scheme in [4] is geometric and uses the concept of intersecting hyperplanes.

The Access Structure of a secret sharing scheme is the set of all groups which are allowed to reconstruct the secret. It is denoted by Γ. The elements of an access structure are referred to as the authorized sets and the rest are called unauthorized sets. The set of all unauthorized sets is called the Adversary structure. The adversary structure will be denoted by $\bar{\Gamma}$. An access structure is called monotone if it satisfies the following criteria.

1) $(A \in \Gamma) \wedge (A \subseteq B) \Longrightarrow B \in \Gamma$;

2) $(A \in \bar{\Gamma}) \wedge (B \subseteq A) \Longrightarrow B \in \bar{\Gamma}$.

We assume that Γ only contains the minimal allowed groups which can recover the secret. Similarly, $\bar{\Gamma}$ only contains maximal adversarial groups which cannot recover the secret.

Several access structures have been proposed in the literature. The primitive access structure is the (t, n)-threshold access structure. In a (t, n)-threshold access structure, there are n shareholders. An authorized group consists of any t or more participants and any group of at most $t - 1$ participants is an unauthorized group.

Threshold schemes are suitable for situations in which each player is assigned the same trust. In most practical situations, the degree of trust assigned to a player can differ based on the authority of the player. Simmons [13] introduced *multilevel* t_i-*out-of*-n_i and *compartmented* t_i-*out-of*-n_i secret sharing schemes to model secret sharing in some practical situations wherein the trust is not distributed uniformly over the set of all players

In Multilevel secret sharing, a set of players is partitioned into disjoint levels. Players at lower levels have more importance than players at higher levels. Each level i contains n_i players. So, the levels form a hierarchial structure. Hence multilevel secret sharing is also called hierarchial secret sharing. There are two types of multilevel

[*] Work done when the author was at University of Hyderabad

access structures: disjunctive multi-level access structure introduced by Simmons [13] and conjunctive multi-level access structure by Tassa [16].

In disjunctive multi-level access structure *any* t_i players of the i^{th} level can recover the secret. When the number of cooperating participants from the i^{th} level is smaller than t_i, say r_i, then $t_i - r_i$ participants can be taken from lower levels.

In conjunctive multi-level access structure *every* group of t_i players on the i^{th} level must cooperate to recover the secret. When the number of cooperating participants from the i^{th} level is smaller than t_i, say r_i, then $t_i - r_i$ participants can be taken from lower levels. A related signcryption scheme [18] for hierarchial groups is studied in [1].

In Compartmented secret sharing, a set of players is partitioned into disjoint compartments. The secret is distributed such that reconstruction of the secret requires cooperation of at least t_i players from the i^{th} compartment. In this context, let us recall the example presented by Simmons in [13]. Let two countries agree to control the recovery of the secret (which may initiate a common action) by a secret sharing scheme. The secret can be recreated only if at least two participants from both compartments pool their shares together.

Generalized access structure is the far reaching generalization of the access structures discussed above. Let U be a set of n participants and 2^U be its power set. Generalized access structure refers to the case when the collection of authorized subsets of U may be any collection $\Gamma \subseteq 2^U$ having the monotonicity property.

A secret sharing scheme is a perfect realization of Γ [15] if for all authorized sets $A \in \Gamma$, the users in A can always reconstruct the secret, and for all unauthorized sets B not in Γ, the users in B collectively cannot obtain any information about the secret. Schemes that satisfy this criteria is commonly referred to as unconditionally secure schemes.

The information rate, ρ_i, for participant i is defined as the ratio of the length of the secret, expressed in bits, to the length of the share, also expressed in bits i.e.

$$\rho_i = \frac{\log_2 |\text{secret}|}{\log_2 |\text{share}|}.$$

The information rate ρ of the scheme is defined as $\rho = \min\{\rho_i : i \text{ is a participant of the scheme}\}$.

A well known fact in secret sharing is that the size of a share is at least the size of the secret. Therefore, the information rate of the participant and hence the information rate of the scheme are both bounded between 0 and 1. Schemes with maximum information rate are desirable [15]. Schemes with information rate 1 are called ideal schemes [15]. The relationship between permutations and ideal secret schemes is studied in [10].

1.1 Our Contribution

Many applications require that secrets be reconstructed in a well-defined order. For example, in banks, a cheque has to be cleared first by the clerk, then by the cashier and finally by the manager. The order has to be strictly enforced. These applications require ordering theory to be introduced into an access structure. It may appear that this problem can be solved by using Multistage secret sharing, but in fact it is not. Refer Section 2.2 for details and Example 1 for a concrete example. To the best of our knowledge, this is the first paper to bring ordering theory into access structures.

A formal definition of proposed Level ordered Access structure (LOAS) is presented in the paper. Also, an ideal secret sharing scheme that realizes this access structure is presented. The scheme is similar in spirit to the compartmented secret sharing scheme proposed by Brickell [5], but differs in the way the partial secrets are combined to recover the secret. The way we combine ensures ordering among the levels, which is the main objective behind Level ordered secret sharing.

1.2 Outline of the Paper

Formal Definition of level ordered access structure is presented in Section 2. The difference between Level ordered secret sharing schemes (LOSS) and other extensions of Shamir secret sharing especially Hierarchial secret sharing are discussed in Section 2. An interesting relationship between generalized access structures and LOAS is discussed in Appendix 4. LOAS and its properties are discussed in Section 3. Section 3 also discusses the modification of LOAS to include a virtual player, which in turn enables to prove the existence of an ideal scheme for the LOAS. In addition, an ideal scheme and the properties of the LOSS scheme especially homomorphic properties are presented in Section 3. Finally we conclude the paper with possible directions for future work in Section 4.

2 Formal Definition of LOAS

In LOAS, a set of players are partitioned into different levels and each level is associated with a threshold. Also there is an ordering defined on the levels. During reconstruction, if the players submit shares according to the specified order, then the actual secret should get reconstructed. Formally the proposed Level ordered Access structure is as follows.

Definition 2.1 *Let U be a set of n participants and let $U_1, U_2, \cdots U_m$ be a partition of the set U. Also let b_i be a boolean variable, which we call the activation index associated with the i^{th} level U_i, $1 \leq i \leq m$. Define S_i, recursively, to be an authorized set corresponding to the i^{th} level if*

1) $S_i \subseteq U_i$ and $|S_i| \geq t_i$,

2) $\exists$ an authorized set (S_{i-1}) whose activation index (b_{i-1}) is True, where $b_0 = T$ and $S_0 = \emptyset$.

I.e., there is an authorized set S_{i-1} of $(i-1)^{th}$ level and the truth value of the corresponding activation index b_{i-1} is true.

A authorized sets of LOAS are the authorized sets of level m.

2.1 Relationship Between LOAS and Hierarchical and Compartmented Access Structures

There are a number of related definitions of access structures like Hierarchial and Compartmented access structures. Following arguments (discussion) explains that these access structures are different from the LOAS defined above.

Definition 2.2 *Disjunctive hierarchical access structure is a multipartite access structure in which each level L_i is assigned with a threshold t_i, $1 \leq i \leq m$, and the secret can be reconstructed when, for some i, there are at least t_i shareholders who all belong to levels smaller than or equal to L_i. Mathematically,*

$$\begin{aligned}\Gamma &= \{V \subseteq U : |V \cap (\cup_{j=1}^{i} U_j)| \geq t_i,\\ &\quad \textit{for some } i \in \{1, 2, \cdots, m\}\}.\end{aligned}$$

Definition 2.3 *Conjunctive hierarchical access structure is a multipartite access structure in which each level L_i is assigned with a threshold t_i for $1 \leq i \leq m$, and the secret can be reconstructed when, for every i, there are at least t_i shareholders who all belong to levels smaller than or equal to L_i. Mathematically,*

$$\begin{aligned}\Gamma &= \{V \subseteq U : |V \cap (\cup_{j=1}^{i} U_j)| \geq t_i,\\ &\quad \textit{for every } i \in \{1, 2, \cdots, m\}\}.\end{aligned}$$

Note that in Hierarchical secret sharing, players can be taken from lower levels and this is not permissible in LOAS. Also LOAS defines a sequence of levels where lower levels have to submit their shares before higher levels, whereas such requirement is absent in hierarchical secret sharing.

Definition 2.4 *Compartmented access structure is a multipartite access structure in which each compartment is assigned with a threshold t_i, $1 \leq i \leq m$, and the secret can be reconstructed when, for every i, there are at least t_i shareholders from U_i and a total of at least t_0 participants from all the compartments. Mathematically,*

$$\begin{aligned}\Gamma &= \{V \subseteq U : |V \cap U_i| \geq t_i,\\ &\quad \textit{for every } i \in \{1, 2, \cdots, m\} \textit{ and } |V| \geq t_0\}.\end{aligned}$$

where $t_0 \geq \sum_{i=1}^{m} t_i$. Compartmental secret sharing and LOAS bear a similarity. In fact, we'll see in Section 3 that the elementary access structure in Level ordered access structure is a Compartmented access structure. There is no concept of ordering among the compartments in a Compartmented access structure.

2.2 Relationship Between Multistage Secret Sharing and LOAS

In a Multistage secret sharing (MSS) scheme [8, 7, 20], shares are distributed to users so that k secrets can be reconstructed, one at each stage. Each participant receives a share known as master share. In each of the stages, a shadow share is computed for each user based on his master share. The shadow shares are used to reconstruct the secret at that stage. Also each stage uses some public values. Note that these methods reconstruct the secrets sequentially. Literature also offers methods that reconstruct all the secrets simultaneously [6, 20]. These methods are known as parallel secret reconstruction methods.

We would like to call the above traditional method of multistage secret sharing as "Loose sequential secret sharing" as a secret at level L_i may be computed without the knowledge of the secret at level L_{i-1}. Also this method supports parallel secret reconstruction.

The LOAS secret sharing scheme described in this paper can be called as "Strict sequential secret sharing" as the secret at level L_i requires the knowledge of secret at level L_{i-1} (See Section 2.3 for our idea of realizing LOAS). It is straightforward to infer that strict sequential secret sharing cannot support parallel secret reconstruction.

More formally, the distinction between loose and strict sequential secret sharing schemes(a scheme that involves a secret at each level) can be made as follows. Any sequential secret sharing scheme can be characterized by two parameters: the first parameter is a triple $(Id, \Gamma_{Id}, s_{Id})$, where Id is the stage or level identity, Γ_{Id} is the access structure for the stage and s_{Id} is the (partial) secret associated with the stage. The second parameter is a permutation on the stage Ids describing the valid order of secret reconstruction.

In traditional MSS Γ_{Id} is same for all stages and the permutation is often left unspecified to allow flexibility. The MSS schemes are flexible to allow the secret reconstruction of a random stage without reconstructing secrets in previous stages and also support parallel reconstruction. In LOAS schemes, there is no flexibility and the (partial) secrets need to be recovered in the specified order.

A simple modification to an existing MSS scheme, like addition of previous stage secret to current stage (t, n) Shamir secret, cannot accomplish the requirements of LOAS, as can be seen from Example 1.

There exists an interesting relationship between Generalized Access Structures and LOAS based on discrete mathematics concept, POSET. But, in order to continue the flow, we defer the discussion to Appendix 4.

The conclusion is that LOAS is different from Hierarchial secret sharing, Compartmental secret sharing, and Multistage secret sharing. LOAS is a recursive set of access structures.

2.3 Realization of LOAS: An Overview

This section proposes an overview on the realization of LOAS. Specific implementation of the scheme is given in Section 3.

In our implementation, a partial secret s_i is associated with each level L_i. The partial secret in the last level is the actual secret of the scheme i.e $s_m = s$. The players at level L_i are allowed to reconstruct the partial secret s_i only after the players at level L_{i-1} have reconstructed the partial secret s_{i-1}.

3 Realization of Level Ordered Access Structure

In this section, the properties of LOAS are examined and a scheme which realizes the Level ordered access structure is given.

3.1 Virtual Player

A way of realizing the level ordered access structure is by adding a virtual player at each level except the first level. The partial secret at each level acts as share of the virtual player in the next level. The virtual player along with the threshold access structure of that level forms the modified access structure at that level. The addition of virtual player ensures that the secrets are reconstructed in specified order.

We define an elementary access structure for a level L_i to be the conjunction of a virtual player(P_i') and a (t, n) threshold access structure. For example, if a level L_i is associated with a (2,3) threshold access structure for players $P = \{P_1, P_2, P_3\}$ and the virtual player of the level is P' then the modified elementary access structure is

$$\begin{aligned}\Gamma &= P'(P_1P_2 + P_1P_3 + P_2P_3)\\ &= P'P_1P_2 + P'P_1P_3 + P'P_2P_3.\end{aligned}$$

One of the widely studied properties of the access structures is whether an ideal scheme exists for a given access structure or not. The following Theorem 2, establishes that the elementary access structure is an ideal access structure. Proof of this theorem is based on the the following theorem, which talks about the existence of an ideal scheme of an access structure, is due to Stinson [15].

Theorem 1 *If the vector corresponding to the dealer can be expressed as a linear combination of the vectors in every authorized set, then there exists an ideal scheme for the corresponding access structure.*

Theorem 2 *An ideal scheme exists for the elementary access structure.*

Proof: Let $GF(q)^d$ denotes the vector space of all d-tuples over $GF(q)$, where q is a prime power and $d \geq 2$. Define $d = t + 1$, where t is the threshold of the (t, n) threshold access structure. Let

$$\phi(P_i) = (0, 1, x_i, x_i^2, \cdots, x_i^{t-1})$$

for $1 \leq i \leq n$, where x_i is the x-coordinate given to P_i. Also, let

$$\begin{aligned}\phi(D) &= (1, 1, 0, \cdots, 0)\\ \phi(P') &= (1, 0, 0, \cdots, 0).\end{aligned}$$

Without loss of generality, let $(P_{i_1}, P_{i_2}, \cdots, P_{i_t}, P')$ be an authorized set. Also let $a_1, \cdots, a_t, a'$ be the coefficients chosen from $GF(q)$. Hence,

$$\begin{aligned}\phi(D) &= a_1\phi(P_{i_1}) + a_2\phi(P_{i_2}) + \cdots + a_t\phi(P_{i_t})\\ &\quad + a'\phi(P') \qquad (1)\\ (1, 1, 0, \cdots, 0) &= \sum_{j=1}^{t} a_j(0, 1, x_{i_j}, x_{i_j}^2, \cdots, x_{i_j}^{t-1})\\ &\quad + a'(1, 0, 0, \cdots, 0). \qquad (2)\end{aligned}$$

It can be easily seen from that $a' = 1$. The remaining set of equations can be expressed in matrix form as follows:

$$\begin{pmatrix} 1 & 1 & \cdots & 1\\ x_{i_1} & x_{i_2} & \cdots & x_{i_t}\\ x_{i_1}^2 & x_{i_2}^2 & \cdots & x_{i_t}^2\\ \vdots & \vdots & & \vdots\\ x_{i_1}^{t-1} & x_{i_2}^{t-1} & \cdots & x_{i_t}^{t-1} \end{pmatrix} \times \begin{pmatrix} a_1\\ a_2\\ a_3\\ \vdots\\ a_t \end{pmatrix} = \begin{pmatrix} 1\\ 0\\ 0\\ \vdots\\ 0 \end{pmatrix}$$

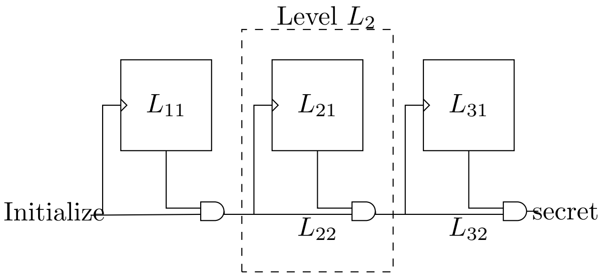
Since, the coefficient matrix is a Vandermonde matrix, its determinant is non-zero. So, the system has a unique solution. That is the vector $(0, 1, 0, \cdots, 0)$ can be expressed as a linear combination of the vectors of an authorized set.

3.2 Proposed Scheme

A look at virtual player concept reveals that each elementary access structure has two compartments. The first compartment is a (t, n) threshold access structure, and the second compartment has only a virtual player. We denote the j^{th} $(j = 1, 2)$ compartment of a level L_i with L_{ij}. So our scheme may be visualized as in the following block diagram.

3.3 Block Diagram

The LOAS can be shown in the form of a block diagram as shown below.



In the block diagram, the AND gate symbol is generic and it can be replaced with an XOR gate or an Adder (provides boolean addition of the two inputs) etc. In our algorithms below, we consider it to be an adder.

Let F_q be the ground field from which the shares and the secrets are chosen. Given the secret, the **Algorithm Share** assigns partial secrets to the levels of the access structure and subsequently to the players in the levels.

3.4 Algorithm Share

Let s be the secret, and i be the level index. Choose $s_1, \cdots, s_m$, so that $s_m = s$.

1) Initialize the partial secret of the last level s_m to s and level index i to m.

2) For each level $L_i (i > 1)$ with partial secret s_i do the following

   a. Assign s_{i-1} be the share of the virtual player at level i. Shares are assigned to the players in level L_{i1} based on Shamir's scheme [12] with $s_i - s_{i-1}$ as secret.

   b. Decrement the level index by 1 so that i becomes $i - 1$.

3) Assign shares to players in level L_1 based on Shamir's scheme [12] with s_1 as the secret.

3.5 Algorithm Reconstruct

1) The Shamir secret sharing scheme is used to generate partial secret, s_1 from the level L_1. The generated partial secret is the share of the virtual player in next level L_2. Initialize level index i to 2.

2) For each level L_i do the following

   a. The Shamir secret sharing scheme is used to generate secret from the first compartment L_{i1}, which is added with the share of the virtual player to generate the partial secret of level L_i. The generated partial secret is the share of the virtual player in the next level, i.e., the share of $L_{(i+1)2}$.

   b. Increment the level index i to become $i+1$, if $i < m$. Otherwise, return the partial secret of level L_m. This partial secret is the desired secret.

Remark: Note that there are two key operations in the proposed scheme. The first one is assigning the secret of stage $i (i < n)$ as the share of the virtual player in stage $i + 1$ and the other one is addition of partial secrets of stages i and $i + 1$ to provide the secret of stage $i + 1$. Both these operations are required to ensure ordering in the proposed scheme. Two examples are provided, each of which, tries to construct a scheme with only one of the above operations and fails to enforce the ordering.

Example 1 *(Considers only addition operation and excludes virtual player) Suppose that there are x stages and the order of secret reconstruction is $(s_1, \cdots, s_m)$ from left to right. The actual secret s is recovered only if the partial secrets are recovered in the specified order. Let $s_m = (t, n)$ Shamir $(s'_m) + s_{m-1}$, where s'_m is the partial secret recovered by stage m using Shamir secret sharing and $s_1 =$ Shamir (s'_1).*

From the definition of LOAS we have

$$\begin{aligned} s &= s_m \\ &= (t,n)Shamir(s'_m) + s_{m-1} \\ &= (t,n)Shamir(s'_m) + (t,n)Shamir(s'_{m-1}) + s_{m-2} \\ &= (t,n)Shamir(s'_m) + (t,n)Shamir(s'_{m-1}) + \cdots \\ &\qquad (t,n)Shamir(s'_1). \end{aligned}$$

Note that the final secret is simply the addition of the partial secrets of all the stages. So the actual secret can be constructed by any of the possible n! permutations with n stages. But according to the definition of LOAS, the secret should be recovered only if the partial secrets are reconstructed in the specified order.

Lemma 1 *The proposed scheme is perfect.*

Proof: It follows directly from the reconstruction algorithm that an authorized set can recover the secret. Any maximal unauthorized set B consists of $\sum_{i=1}^{m} t_i - 1$ players, where t_i is the threshold of the level L_i. So there exists a level L_j such that the number of corroborating players from that level fall below the threshold i.e., $B \cap L_j < t_j$. To find the partial secret of the level L_{j1}, we need t_j equations. But, the players from the level L_j provide a maximum of $t_j - 1$ shares. As the number of unknowns are less than the number of equations, there exists infinitely many solutions(i.e., $|F_q|$) for the secret value. Hence any maximal unauthorized set cannot obtain any information about the secret.

Theorem 3 *The proposed scheme is Level ordered. i.e., partial secrets are recovered in the specified order.*

Proof: We prove the theorem by the induction on levels. If there is only one level, the reconstruction algorithm returns the secret of the first level and terminates. Let the partial secret be recovered correctly for the k^{th} level (induction hypothesis). As per the construction, the first compartment of level $k+1$ implements Shamir secret sharing and provides the first input to the adder. As per the induction hypothesis, the second input is provided by the partial secret of the k^{th} level. Now the Adder can reconstruct the partial secret s_{k+1}. Hence, the partial secret in level L_{k+1} is reconstructed only after the partial secret in level L_k.

3.6 Properties of LOSS

3.6.1 Comparison with the Compartmental Access Structure

As can be seen from the virtual player concept that each elementary access structure other than the one at first level is a compartmental access structure with two compartments. The first compartment is a (t, n) threshold, the second compartment is a $(1, 1)$ threshold and the global threshold is $t + 1$. Note that sum of the individual thresholds is the global threshold. The elementary access structure in LOAS is a special case of the compartmental access structure in which sum of the individual thresholds is the global threshold.

3.6.2 LOSS is a Prepositioned Scheme

Prepositioned schemes [14] were introduced by Simmons and has two essential features:

Privacy. It should be possible to preposition all of the private information needed for the shared control subject to the condition that even if all of the participants were to violate the trust of their position and collaborate with each other, they would have no better chance of recovering the secret information than an outsider has of guessing it.

Activation. It should be possible to activate the shared control scheme once it is in place by communicating a single share of information, and for many applications, it should also be possible to reveal different secrets (using the same prepositioned private pieces of information) by communicating different activating shares of information.

LOSS is one of the best examples of prepositioned secret sharing schemes. The partial secret at level L_i is reconstructed only after the partial secret at level L_{i-1} is reconstructed. The partial secret at level L_{i-1} together with the activation index acts as activation information for the players at level L_i (Activation property). Without the partial secret at level L_{i-1}, the players at level L_i would have no better chance of recovering the secret information than an outsider has of guessing it (Privacy property).

3.6.3 Homomorphic Property of LOSS

The Homomorphic property of a secret sharing scheme allows to reconstruct the composition of secrets from the composition of corresponding shares without revealing anything about the individual secrets. Recovery of the partial secret at each level L_i in the reconstruction alogrithm of LOSS scheme comprises of two steps.

1) Shamir reconstruction algorithm to reconstruct the secret of the first compartment L_{i1};

2) Addition of secrets of levels L_{i-1} and L_{i2} to calculate the secret of the level L_i.

Shamir's scheme is homomorphic with respect to (+, +) [3] and the second operation is trivially homomorphic. Therefore, the proposed LOSS scheme is homomorphic with respect to (+, +).

4 Conclusion

This paper proposed an access structure that closely resembles the known access structures such as conjunctive hierarchial access structure and compartmental access structure. We call the proposed access structure as the Level Ordered Access Structure(LOAS). Unlike existing access structures; wherein there is no concept of ordering, LOAS enforces ordering and it is a sequence of threshold access structures.

It is easy to visualize applications of LOAS in variety of areas such as software testing, prepartion of cheques, drafts in banks etc. The paper presented a formal definition of LOAS and a model for realizing LOAS. The paper also analyzed the existence of an ideal scheme for the proposed LOAS and presented an ideal scheme for the same.

The side affects of cheating [17] by a player in the i^{th} level should be studied. Creating cheating models and analyzing the repercussions can be one direction for future work. To make the scheme secure against cheating, either a verification scheme [2] or a robust scheme [11] can be introduced. Designing such a scheme can be another direction for future work.

Acknowledgments

The authors gratefully acknowledge Prof.V.N.Sastry of IDRBT for his insights into the problem statement.

References

[1] A. Basu1, I. Sengupta1, and J. K. Sing, "Cryptosystem for secret sharing scheme with hierarchical groups," *International Journal of Network Security*, vol. 16, no. 6, pp. 455–464, 2013.

[2] M. Ben-Or, S. Goldwasser, A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC'88)*, pp. 1–10, New York, NY, USA, 1988.

[3] J. C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret (extended abstract)," in *Advances in Cryptology (CRYPTO'86)*, LNCS 263, pp. 251–260, Springer, 1987.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 AFIPS National Computer Conference*, vol. 48, pp. 313–317, June 1979.

[5] E. F. Brickell, "Some ideal secret sharing schemes," in *Advances in Cryptology (EUROCRYPT'89)*, LNCS 434, pp. 468–475, Springer, 1990.

[6] H. Y. Chien and J. K. Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics*, vol. 83, pp. 2762–2765, Sept. 2000.

[7] L. Harn, "Comment on "multistage secret sharing based on one-way function," *Electronics Letters*, vol. 31, pp. 262, Feb. 1995.

[8] J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30, pp. 1591–1592, Sept. 1994.

[9] K. M. Marin, *Discrete Structures in the Theory of Secret Sharing*, Ph.D. Thesis, University of London, 1991.

[10] J. Pieprzyk and X. M. Zhang, "Ideal secret sharing schemes from permutations," *International Journal of Network Security*, vol. 2, no. 3, pp. 238–244, 2006.

[11] P. Rogaway and M. Bellare, "Robust computational secret sharing and a unified account of classical secret-sharing goals," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07)*, pp. 172–184, New York, NY, USA, 2007.

[12] A. Shamir, "How to share a secret," *Communications of ACM*, vol. 22, pp. 612–613, Nov. 1979.

[13] G. J. Simmons, "How to (really) share a secret," in *Advances in Cryptology (CRYPTO'88)*, LNCS 403, pp. 390–448, Springer, 1990.

[14] G. J. Simmons, "Prepositioned shared secret and/or shared control schemes," in *Advances in Cryptology (EUROCRYPT'89)*, LNCS 434, pp. 436–467, Springer, 1990.

[15] D. R. Stinson, "An explication of secret sharing schemes," *Designs, Codes and Cryptography*, vol. 2, no. 4, pp. 357–390, 1992.

[16] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology*, vol. 20, pp. 237–264, Apr. 2007.

[17] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 2, pp. 133–138, 1988.

[18] M. Toorani and A. A. B. Shirazi, "Cryptanalysis of an ecient signcryption scheme with forward secrecy based on elliptic curve," *International Journal of Network Security*, vol. 10, no. 1, pp. 51–56, 2010.

[19] Wikipedia, *Partially Ordered Set*, The Free Encyclopedia, June 22, 2004. `http://http://en.wikipedia.org/wiki/Partially\_ordered\_set`

[20] T. Y. Yang, C. C. Chang and M. S. Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, pp. 483–490, 2004.

Appendix A.

Relationship Between Generalized Access Structures and LOAS

For mathematical background on POSET, Chains and Antichains the reader is referred to [19]. The following lemma, which is due to Martin[9] states an important relationship between the antichains of a POSET and generalized access structures.

Lemma 2 *Each of the antichain of a POSET P defines a generalized access strucutre.*

Example 2 *The antichains of the POSET* $P = \{\emptyset,\ \{x\},\ \{y\},\ \{z\},\ \{x,y\},\ \{y,z\},\ \{z,x\},\ \{x,y,z\}\}$ *are*
$\{\emptyset, \{\emptyset\}, \{\{x\}\}, \{\{y\}\}, \{\{z\}\},$
$\{\{x\},\{y\}\}, \{\{y\},\{z\}\}, \{\{z\},\{x\}\}, \{\{x\},\{y\},\{z\}\},$
$\{\{x,y\}\}, \{\{y,z\}\}, \{\{z,x\}\},$
$\{\{x\},\{y,z\}\}, \{\{y\},\{x,z\}\}, \{\{z\},\{x,y\}\},$
$\{\{x,y\},\{y,z\}\}, \{\{x,y\},\{z,x\}\}, \{\{y,z\},\{z,x\}\},$
$\{\{x,y\},\{y,z\},\{z,x\}\}, \{\{x,y,z\}\}\}$.

In the above example, excluding the empty set and the set containing empty set, the rest of the antichains define a generalized access structure. For example, the antichain $\{\{x\},\{y,z\}\}$ defines an access structure $\Gamma = x + yz$.

Define the operator RECONSTRUCT on the set of levels $U_1, U_2, \cdots, U_m$ as the one that permits the set U_i to reconstruct the secret only after the reconstruction of the secret by U_{i-1}. Now the set of levels with this RECONSTRUCT operator forms a chain. That is it is totally ordered set.

Example 3 *A set of three levels in LOAS* $U = \{U_1, U_2, U_3\}$ *is a strict POSET under the relationship operator RECONSTRUCT* $<$*. The set U forms a chain.* U_3 *is allowed to reconstruct the secret only after* U_2 *has reconstructed the partial secret; in turn* U_2 *is allowed to reconstruct the partial secret only after* U_1 *has reconstructed the partial secret.*

So the **Antichains of a POSET define generalized access structures; whereas the chains of a POSET define Level Ordered access structures**.

Dileep Kumar Pattipati received BTech from Jawaharlal Nehru Technological University, Hyderabad and M.Tech from University of Hyderabad, Hyderabad. Currently he is pursuing his PhD in Computer Science from IIT Madras, Chennai. He has software industry experience of 3 years. His research interests include Cryptography, Algorithms, and Semantic web.

Appala Naidu Tentu is a Research Scientist at CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science (AIMSCS), University of Hyderabad Campus, Hyderabad. He obtained his M.Tech in Computer Science from National Institute of Technology, Suratkal (NITK), Karnataka, in 2010 and M.Sc from Andhra University, Visakhapatnam, in 2007. Currently, he is pursuing his PhD in Computer Science from JNTU Hyderabad. His research interests are in the areas of cryptography, cryptanalysis and design of security protocols.

V. Ch. Venkaiah obtained his PhD in 1988 from the Indian Institute of Science (IISc), Bangalore in the area of scientific computing. He worked for several organisations including the Central Research Laboratory of Bharat Electronics, Tata Elxsi India Pvt. Ltd., Motorola India Electronics Limited, all in Bangalore. He then moved onto academics and served IIT, Delhi, IIIT, Hyderabad, and C R Rao Advanced Institute of Mathematics, Statistics, and Computer Science. He is currently serving the Hyderabad Central University. He is a avid researcher. He designed algorithms for linear programming, subspace rotation and direction of arrival estimation, graph colouring, matrix symmetriser, integer factorisation, cryptography, knapsack problem, etc.

Allam Appa Rao is a Director at CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science (AIMSCS), University of Hyderabad Campus, Hyderabad. He was the first to receive Ph.D from Andhra University in Computer Engineering in the year 1984. During his more than four decades of professional experience, such as First Vice Chancellor, JNTUK, Kakinada, A.P, Principal, College of Engineering (Autonomous), Andhra University. He shared his wisdom with fellow engineers and scientists across the globe through his innumerable research papers published in international journals and international conference proceedings. Indian Science Congress Association (ISCA) conferred him with "Srinivas Ramanujan Birth Centenary Award" Gold medal for his significant and life time contribution to the development of Science and Technology in the country specifically in the area of Computational Biology, Software Engineering and Network Security.