Evolving Secret Sharing with Essential Participants

Jyotirmoy Pramanik* and Avishek Adhikari

Abstract Komargodski et.al. introduced *Evolving Secret Sharing* which allows an imaprtial participant, called *dealer*, to share a secret among unbounded number of participants over any given access structure. In their construction for evolving secret sharing over general access structure, the size of share of the i^{th} participant happens to be exponential $(\mathscr{O}(2^{i-1}))$. They also provided constructions for (k,∞) threshold secret sharing. We consider the problem of evolving secret sharing with t essential participants, namely, over t-(k,∞) access structure, a generalization of (k,∞) secret sharing $(t=0)$. We further generalize this access structure to a possible case of unbounded number of essential participants and provide a construction for secret sharing on it. Both the constructions are information theoretically secure and reduce the share size of the construction due to Komargodski et.al. over general access structure, exponentially. Moreover, the essential participants receive ideal (and hence, optimal) shares in the first construction.

Key words: Evolving Access Structure, Secret Sharing, Essential Participants, Information Theoretic

Jyotirmoy Pramanik
Department of Pure Mathematics, University of Calcutta,
35, Ballygunge Circular Road, Kolkata 700019, India
e-mail: jyotirmoy.pramanik2@gmail.com

Avishek Adhikari
Department of Mathematics, Presidency University,
86/1, College Street Rd, Kolkata 700073, India
e-mail: avishek.adh@gmail.com

1 Introduction

In *secret sharing* one can so share an information (usually a field element) among n (fixed and pre-decided) participants that certain subsets are able to reconstruct it back while others are not [18]. Given any access structure on a set of participants, there exists a secret sharing scheme realizing it. *Evolving secret sharing* generalizes the notion of usual secret sharing where the participants' set was to be known beforehand. It allows participants to join one by one and the dealer hands them their shares without refreshing shares already distributed. Komargodski et.al. introduced evolving secret sharing in [8]. We discuss few of these notions in details in *Section* 2. In *Section* 3 we introduce t-(k,∞) and (t,∞,k,∞) secret sharing and provide two constructions. In *Section* 4 we summarize our results and suggest further research directions.

Our Contribution: In this paper, we provide a construction for secret sharing realizing t-(k,∞) access structure where fixed t participants are essential. Essential participants in this scheme receive a share of size $\mathscr{O}(1)$ whereas i^{th} of the other participants receives a share of the size $(k-1)\cdot\log i + poly(k,\ell)\cdot\mathscr{O}(\log i)$ for an ℓ-bit secret being shared. We further generalize this access structure to (t,∞,k,∞) access structure and provide a construction for secret sharing realizing it. In the latter construction, the i^{th} participant receives a share of size $\mathscr{O}((k-1)\cdot\log i + poly(k,\ell)\cdot\mathscr{O}(\log i))$. Share sizes in both the schemes are a huge (exponential) improvement compared to the scheme for general access structure having share size $\mathscr{O}(2^{i-1})$ in [8]. We compare our results with [8] for a single bit secret in Table 1.

Construction	**Share Size of the i^{th} party**
[8] General Access Structure	2^{i-1}
[8] (k,∞)	$(k-1)\cdot\log i + poly(k)\cdot\mathscr{O}(\log i)$
1. This paper t-(k,∞)	
(i) Essential	$\mathscr{O}(1)$
(i) Other	$(k-1)\cdot\log i + poly(k)\cdot\mathscr{O}(\log i)$
2. This paper (t,∞,k,∞)	
(i) Essential	$\mathscr{O}((k-1)\cdot\log i + poly(k)\cdot\mathscr{O}(\log i))$
(i) Other	$(k-1)\cdot\log i + poly(k)\cdot\mathscr{O}(\log i)$

Table 1 Comparison of Size of Shares for a single bit secret

2 Preliminaries

For a given access structure $\Gamma \subset 2^{\mathscr{P}}$ on a participants' set $\mathscr{P}$, a subset $\mathscr{A}$ of participants is called *qualified* if and only if $\mathscr{A} \in \Gamma$; otherwise $\mathscr{A}$ is *forbidden*. A (t,n) threshold access structure on n participants consists of qualified sets which are precisely of size t or more. For secret sharing on any given access structure,

an impartial participant $\mathscr{D} \notin \mathscr{P}$ (called the *Dealer*) invokes the *share generation* protocol ShareGen and generates n shares, one for each participant. In the hour of need for reconstruction of the secret, certain participants pool their shares in the *reconstruction* protocol Reconst. The secret sharing scheme is denoted by $\Pi = (\mathsf{ShareGen}, \mathsf{Reconst})$. The *correctness* property in a secret sharing scheme ensures that any qualified set of participants is able to reconstruct the secrets with certainty, i.e. $Pr[s' = s | s' \leftarrow \mathsf{Reconst}(\mathscr{A}) \text{ and } \mathscr{A} \in \Gamma] = 1$. On the other hand, due to *perfect secrecy*, Reconst outputs for the correct secret from a forbidden set's share with probability no more than that derived from the probability distribution of the secret space $\mathscr{S}$, i.e. $Pr[s' = s | s' \leftarrow \mathsf{Reconst}(\mathscr{A}) \text{ and } \mathscr{A} \in 2^{\mathscr{P}} \setminus \Gamma] = Pr[s \leftarrow \mathscr{S}]$. *Share size* of a participant P_i is size of collection of all possible shares for him; this collection (called the *share space* V_i of P_i) is generated due to different values of randomness of the share generation algorithm. In an *ideal* secret sharing scheme, the share size and secret size are same.

Secret sharing with essential participants was initiated in a work by Arumugam et.al. in [2]. They denoted this type of access structure as $(k,n)^*$ *access structure* where a secret image was shared into n *shadow* images where presence of the shadow corresponding to *one* particular participant was *essential*. Later this notion was generalized to access structures containing t essential participants as t-(k,n) secret sharing in [14, 7, 5]. A further generalization (t,s,k,n) secret sharing was considered in [10] by Li et.al. where at least t essential shadows (among s of those) were necessary to reconstruct the secret, along with the threshold condition being satisfied.

Evolving secret sharing was introduced by Komargodski et.al. in [8]. As opposed to usual secret sharing with n participants, they considered a far more practical variant where there is no upper bound on number of participants. Participants join one by one and they are handed over a share based on shares distributed to previous participants but without interacting with the previous participants. In other words, shares are not refreshed. Most of the secret sharing schemes are linear [18] in nature and requires the underlying field of be of size at least $\log(\text{field size})$, where $(\text{field size}) > \#(\text{participants})$. This creates a problem for the *evolving* setup where the number of participants in not known beforehand. Komargodski et.al. provided a beautiful solution for this problem in [8] on general access structure where the i^{th} participant receives a share of size $\ell \cdot 2^{i-1}$ for an ℓ bit secret. They also provided a (k,∞) secret sharing scheme sharing an ℓ bit string with share size of the i^{th} participant being $(k-1) \cdot \log i + poly(k,\ell) \cdot \mathscr{O}(\log i)$. A few more follow up works in evolving setup can be found in [11, 9, 4, 3, 6].

3 Evolving Secret Sharing with Essential Participants

Secret sharing with essential participants is a generalized case of usual threshold secret sharing. Though being well studied in traditional secret sharing, this notion is yet unexplored in evolving setup except for a work by Dutta et.al. [6]. In the

following sections, we introduce secret sharing on t-(k,∞) and (t,∞,k,∞) access structures.

3.1 A Construction for t-(k,∞) Secret Sharing Scheme

In a t-(k,∞) secret sharing, qualified subsets are those which are of at least size k and contain t special participants, called the *essential participants*. The essential participants are predefined and fixed, and are free to join as and when they wish to, just like other non-essential participants. Of course, until the last essential participant has joined, no subset of participants is qualified. We define an attribute function $f : \mathscr{P} \to \{0,1\}$ for each participant P_i as : $f(P_i) = 1$ if and only if P_i is an essential participant. The function f can also be interpreted as the characteristic function of the subset of essential participants. Let us demonstrate the simple case of $1-(2,\infty)$ secret sharing: To share a secret $s \in \{0,1\}^\ell = \mathscr{S}$, give the essential participant P_α a random number $r \leftarrow \mathscr{S}$ and every other participant $r \oplus s$. Reconstruction is done by XORing two shares. Every participant receives a share of constant size and this scheme is ideal. This example portrays a somewhat extremal case of evolving secret sharing with essential participants. Another such extremal case of consideration would be $k-(k,\infty)$ secret sharing. In this case all but the essential participants would receive *dummy shares* which might play no role whatsoever in secret reconstruction. For the rest of this paper, we shall assume that $t < k$. Now that we are warmed up with how two simplest instances of t-(k,∞) secret sharing schemes work, let us move on to a more general construction. We assume the availability of (k,∞) - secret sharing schemes Π_k due to Komargodski et.al. [8] for every $k \geq 2$. We shall use this scheme as a black-box to generically produce a t-(k,∞) secret sharing scheme.

Theorem 1. *For positive integers $t, (<)k$ and ℓ, there exists a t-(k,∞) secret sharing scheme sharing an ℓ bit secret, meeting the correctness and perfect secrecy conditions. Moreover, the scheme is ideal for essential participants and for the i^{th} non-essential participant, share size is given by $(k-1)\cdot\log i + poly(k,\ell)\cdot\mathscr{O}(\log i)$.*

Proof. For $k > t$, we demonstrate the following secret sharing scheme (ShareGen, Reconst) attaining the said conditions.

ShareGen : For a secret $s \in \{0,1\}^\ell = \mathscr{S}$, we describe the share generation protocol below :

1. Generate $t+1$ random numbers $r_1, r_2, \ldots, r_t, r_{t+1} \xleftarrow{\$} \{0,1\}^\ell$ such that $s = \bigoplus_{i=1}^{t+1} r_i$.
2. Initialize $c = 0$.
3. On arrival of the i^{th} participant P_i ($i = 1,2,3,\ldots$), if P_i is an essential participant, i.e. if $f(P_i) = 1$, then update c by adding 1 to it and give r_c to P_i as his share; else run the share generation algorithm of Π_{k-t} to generate a share w_i of r_{t+1} and give it to P_i. If at any point of share generation $c > t$, then ShareGen aborts.

Reconst : k participants including the t essential participants pool their shares; the $k-t$ non-essential participants reconstruct r_{t+1} using reconstruction algorithm of Π_{k-t}. Further, they find s by bit wise XORing $r_1, r_2, \ldots, r_t, r_{t+1}$. If a forbidden set submits shares for reconstruction, FAIL is output.

Proof of Correctness: Every qualified set of participants $\mathscr{A} \in \Gamma$ contains the t essential participants and at least $k-t$ other participants. Due to correctness property of reconstruction algorithm of Π_{k-t}, these $k-t$ or more participants can uniquely reconstruct r_{t+1}. The secret s is found by XORing r_i's for $i \in [t+1]$.

Proof of Perfect Secrecy: In t-(k,∞) access structure there are two kind of forbidden sets possible, namely, (i) *Type 1* forbidden sets which contain k or more participants but do not contain at least one essential participant; (ii) *Type 2* forbidden sets which contain at most $k-1$ participants in total. For a Type 1 forbidden set $\mathscr{A}$, members of $\mathscr{A}$ possess the following set of information $info^{(1)} = \{r_i : \text{ for } \leq t-1 \text{ values of } i \text{ from } [t]\} \sqcup \{\text{shares of } r_{t+1}\}$, where $\sqcup$ denotes disjoint union. Using $info^{(1)}$ $\mathscr{A}$ can reconstruct r_{t+1}, since there are at least $k-(t-1) = k-t+1$ shares of r_{t+1} present. Without loss of generality, let us assume that the 1^{st} essential participant is not present in $\mathscr{A}$, then participants of $\mathscr{A}$ can reconstruct with a probability $Pr[\text{Finding } s = r_1 \oplus r_2 \oplus \cdots \oplus r_{t+1} | r_2, r_3, \ldots, r_t, r_{t+1}] = Pr[r_1 \xleftarrow{\$} \{0,1\}^\ell] = Pr[s \xleftarrow{\$} \mathscr{S}]$, i.e. the best that a Type 1 forbidden set can do with their shares is guess the secret s (without looking at any share, like any person not present in $\mathscr{P}$). A Type 2 forbidden set either consists of all the essential participants but $k-t-1$ non-essential participants; or, $t-1$ or lesser essential participants. The proof of perfect secrecy for the latter of these two cases can be done in a manner similar to Type 1. We only prove perfect secrecy for the former case now. $\mathscr{A}$ possesses the following set of information: $info^{(2)} = \{r_1, r_2, \ldots, r_t\} \sqcup \{k-t-1 \text{ shares of } r_{t+1}\}$. Due to perfect secrecy of Π_{k-t} used, it follows that $Pr[\text{Finding } s = r_1 \oplus r_2 \oplus \cdots \oplus r_{t+1} | info^{(2)}] = Pr[r_{t+1} \xleftarrow{\$} \{0,1\}^\ell] = Pr[s \xleftarrow{\$} \mathscr{S}]$.

Share Size Analysis: The scheme described above is ideal for essential participants. For the i^{th} non-essential participant, share size is given by $(k-1)\cdot \log i + poly(k,\ell) \cdot \mathscr{O}(\log i)$. It is convenient to assume $k \geq 3$ as for $k = 2$, the access structure reduces to two trivial sub-cases of $1-(2,\infty)$ and $2-(2,\infty)$ access structures, where secret sharing can be done trivially, as shown in the beginning of this section. Due to our construction, share size of the i^{th} non-essential participant preserves the share size of the i^{th} participant in (k,∞) secret sharing scheme of [8] by Komargodski et.al. sharing ℓ bit strings. ■

We further generalize t-(k,∞) secret sharing in the following section. Specifically, we give rise to a new access structure called (t,∞,k,∞) access structure in Section 3.2 in which qualified subsets are those which contain any t of the possibly infinite collection of *pseudo-essential* participants and also k participants in total. We call these participants pseudo-essential because essentiality of these participants doesn't depend on their individuality but on their grouping with other similar par-

ticipants in sufficient number. It can be noted that, unlike t-(k,∞) access structure, in this access structure one may find qualified subsets consisting of only pseudo-essential participants. As a particular case, if no new pseudo-essential participant arrives after the t-th one, it is nothing but a t-(k,∞) access structure, establishing the fact that (t,∞,k,∞) access structure is indeed a generalization of t-(k,∞) access structure. Moreover, (t,∞,k,∞) access structure can be seen as a generalization of another access structure, namely (t,s,k,n) access structure. Secret sharing was done on the latter access structure by Li et.al. in [10].

3.2 A Construction for (t,∞,k,∞) Secret Sharing Scheme

We define a new access structure called (t,∞,k,∞) access structure in this section where a qualified subset of participants contains at least k participants in total including at least t participants from a subset $\mathscr{P}_{ps}$ of special participants called *pseudo-essential participants*. The subset may not be known in the beginning but this subset can be characterized by defining an attribute function as in Section 3.1. To summarize, $f : \mathscr{P} \to \{0,1\}$ is a function defined on the collection of participants $\mathscr{P}$ [which is also unknown in the beginning but f can be identified with a function with similar properties being defined on the set $\mathbb{N}$ of natural numbers and, hence, is convenient] as : $f(P_i) = 1$ if and only if P_i is a pseudo-essential participant. In the beginning of the scheme, we set $\mathscr{P}_{ps} = \emptyset$ and whenever a new pseudo-essential party joins, we add him to the set $\mathscr{P}_{ps}$. We assume availability of (k,∞) - secret sharing schemes Π_k [8] for every $k \geq 2$. In this construction, every pseudo essential participant receives share which is *heavier* than the size of every other participant, the convenience of which we describe in proof of Theorem 2.

Theorem 2. *For positive integers $t, (<)k$ and ℓ, there exists a (t,∞,k,∞) secret sharing scheme sharing an ℓ bit secret, satisfying correctness and perfect secrecy conditions. Moreover, the share of size of the i^{th} participant is $\mathscr{O}((k-1)\cdot\log i + poly(k,\ell)\cdot\mathscr{O}(\log i))$ if he is pseudo-essential; otherwise share size is $(k-1)\cdot\log i + poly(k,\ell)\cdot\mathscr{O}(\log i)$.*

Proof. For $k > t$, we demonstrate the following secret sharing scheme (ShareGen, Reconst) attaining the said conditions.

ShareGen : For a secret $s \in \{0,1\}^\ell = \mathscr{S}$, we describe the share generation protocol below :

1. Generate a random number $r \xleftarrow{\$} \mathscr{S}$.
2. On arrival of the i^{th} participant P_i, if $f(P_i) = 1$ then run the share generation algorithms of Π_t and Π_{k-t} to generate a new shares $w_{1,i}$ and $w_{2,i}$ of r and $r \oplus s$ respectively and give $(w_{1,i}, w_{2,i})$ to P_i as his share; else run the share generation algorithm of Π_{k-t} to generate a new share $w_{2,i}$ of $r \oplus s$ and give it to P_i.

Reconst : Suppose, k parties $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$ pool their shares.

1. Set $\mathscr{P}_{ps,t} = \emptyset$ and $L = \{i_1, i_2, \ldots, i_k\}$.
2. Adjoin the first t pseudo essential participants present for reconstruction to $\mathscr{P}_{ps,t}$ and delete their corresponding indices from L. In other words:
   $c = 0$
   for (i in L) :
   if ($f(P_i) = 1$) :
   $\mathscr{P}_{ps,t} = \mathscr{P}_{ps,t} \cup \{P_i\}$
   $L = L \setminus \{i\}$.
   $c \mathrel{+}= 1$
   if ($c = t$):
   break.
3. Run the reconstruction algorithm of Π_t on $\left\{w_{1,i} : P_i \in \mathscr{P}_{ps,t}\right\}$ to reconstruct r. Run the reconstruction algorithm of Π_{k-t} on $\{w_{2,i} : i \in L\}$ to reconstruct $r \oplus s$. XOR r and $r \oplus s$ to reconstruct s. If a forbidden set submits shares, Reconst outputs FAIL.

Proof of Correctness: Every qualified set $\mathscr{A}$ in this access structure is of size $\geq k$ and contains t pseudo-essential participants. If $\mathscr{A}$ contains more than t pseudo-essential participants, we 'treat' the first t of them as pseudo-essential and the others ordinarily. The (first) t pseudo-essential participants reconstruct r and the remaining participants reconstruct $r \oplus s$ using respective reconstruction algorithms of Π_t and Π_{k-t}. Since both the algorithms possess correctness, the property is preserved for our construction as well.

Proof of Perfect Secrecy: The proof for perfect secrecy is similar to Theorem 1.

Share Size Analysis: The i^{th} participant receives a share of size of size $\mathscr{O}((k-1) \cdot \log i + poly(k,\ell) \cdot \mathscr{O}(\log i))$ if he is pseudo-essential; otherwise share size is $(k-1) \cdot \log i + poly(k,\ell) \cdot \mathscr{O}(\log i)$. It can be noted that pseudo-essential participants receive shares which are *heavier* compared to other participants. This is convenient as there are qualified sets consisting of only pseudo-essential participants, and hence, they should possess shares corresponding to both r and $r \oplus s$. ■

4 Conclusion and Future Research

To sum up, we provide a secret sharing scheme realizing t-(k,∞) access structure where t (fixed) participants are essential. Essential participants in this construction receive a share of size $\mathscr{O}(1)$ whereas i^{th} of the other participants receives a share of the size $(k-1) \cdot \log i + poly(k,\ell) \cdot \mathscr{O}(\log i)$ for an ℓ-bit secret being shared. We further generalize this access structure to a new access structure called (t,∞,k,∞) access structure and provide a secret sharing scheme realizing it. In the latter construction, the i^{th} participant receives a share of size

$\mathcal{O}((k-1)\cdot\log i + poly(k,\ell)\cdot\mathcal{O}(\log i))$. Share sizes in both the schemes are a huge (exponential) improvement compared to the scheme for general access structure having share size $\mathcal{O}(2^{i-1})$ in [8].

A further research direction could be considering dynamic thresholds (both in t and k) like [9] in both the access structures demonstrated. Another interesting follow up work would be to introduce secret sharing with cheaters [19, 13, 12, 15, 16, 1, 17] in evolving setup.

References

1. Adhikari, A., Morozov, K., Obana, S., Roy, P.S., Sakurai, K., Xu, R.: Efficient threshold secret sharing schemes secure against rushing cheaters. In: ICITS 2016, Revised Selected Papers, pp. 3–23 (2016)
2. Arumugam, S., Lakshmanan, R., Nagar, A.K.: On (k, n)*-visual cryptography scheme. Des. Codes Cryptogr. **71**(1), 153–162 (2014)
3. Beimel, A., Othman, H.: Evolving ramp secret-sharing schemes. In: SCN 2018, Proceedings, pp. 313–332 (2018)
4. D'Arco, P., Prisco, R.D., Santis, A.D., del Pozo, A.L.P., Vaccaro, U.: Probabilistic secret sharing. In: MFCS 2018, pp. 64:1–64:16 (2018)
5. Dutta, S., Adhikari, A.: XOR based non-monotone t- (k, n)^* -visual cryptographic schemes using linear algebra. In: ICICS 2014, pp. 230–242 (2014)
6. Dutta, S., Roy, P.S., Fukushima, K., Kiyomoto, S., Sakurai, K.: Secret sharing on evolving multi-level access structure. In: WISA 2019, Proceedings (To appear)
7. Guo, T., Liu, F., Wu, C.K., Ren, Y., Wang, W.: On (k, n) visual cryptography scheme with t essential parties. In: ICITS 2013, Proceedings, pp. 56–68 (2013)
8. Komargodski, I., Naor, M., Yogev, E.: How to share a secret, infinitely. In: TCC 2016-B, Proceedings, Part II, pp. 485–514 (2016)
9. Komargodski, I., Paskin-Cherniavsky, A.: Evolving secret sharing: Dynamic thresholds and robustness. In: TCC 2017, Proceedings, Part II, pp. 379–393 (2017)
10. Li, P., Yang, C., Wu, C., Kong, Q., Ma, Y.: Essential secret image sharing scheme with different importance of shadows. J. Vis. Comm. and Im. Rep. **24**(7), 1106–1114 (2013)
11. Paskin-Cherniavsky, A.: How to infinitely share a secret more efficiently. IACR Cryptology ePrint Archive **2016**, 1088 (2016)
12. Pramanik, J., Adhikari, A.: Ramp secret sharing with cheater identification in presence of rushing cheaters. Groups Complexity Cryptology **11**(2), 103–113 (2019)
13. Pramanik, J., Roy, P.S., Dutta, S., Adhikari, A., Sakurai, K.: Secret sharing schemes on compartmental access structure in presence of cheaters. In: ICISS 2018, Proceedings, pp. 171–188 (2018)
14. Praveen, K., Rajeev, K., Sethumadhavan, M.: On the extensions of (k, n)*-visual cryptographic schemes. In: SNDS 2014, Proceedings, pp. 231–238 (2014)
15. Roy, P.S., Adhikari, A., Xu, R., Morozov, K., Sakurai, K.: An efficient robust secret sharing scheme with optimal cheater resiliency. In: SPACE 2014, pp. 47–58 (2014)
16. Roy, P.S., Adhikari, A., Xu, R., Morozov, K., Sakurai, K.: An efficient t-cheater identifiable secret sharing scheme with optimal cheater resiliency. IACR Cryptology ePrint Archive **2014**, 628 (2014)
17. Roy, P.S., Dutta, S., Morozov, K., Adhikari, A., Fukushima, K., Kiyomoto, S., Sakurai, K.: Hierarchical secret sharing schemes secure against rushing adversary: Cheater identification and robustness. In: ISPEC 2018, Proceedings, pp. 578–594 (2018)
18. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
19. Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptology **1**(2), 133–138 (1988)