International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9
Website	www.iciems.in
Received	10 - July - 2015
Article ID	ICIEMS044

VOL	01
eMail	iciems@asdf.res.in
Accepted	31- July - 2015
eAID	ICIEMS.2015.044

A Novel Proactive Secret Sharing

Sayantan Mandal[1], Prof.V. Ch. Venkaiah[2]
[1,2] School of Computer and Information
Sciences, University of Hyderabad, Hyderabad-500046, India

Abstract: *A (t, n) secret sharing scheme that divides a secret into n shares in such a way that any t or more than t shares can reconstruct the secret; but fewer than t shares cannot reconstruct the secret. A share renewal protocol is to protect a secret in long-lived system by distributing it to a group of n participants and refreshing their shares periodically in this fixed group. In this paper we propose a share renewal protocol without the presence of a trusted party. Shareholders renew their shares among themselves using old shares without disclosing their shares at any stage of the protocol and able to reconstruct the secret without changing it. The protocol is robust and maintain privacy of shares.*

I. INTRODUCTION

In Cryptography, a secret sharing scheme refers to any method for distributing a secret among a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when an authorized subset of participants combine their shares.In a secret sharing scheme, a secret s is divided into n shares by a dealer and shared among n shareholders in such a way that any t or more than t shares can reconstruct this secret; but fewer than t shares cannot reconstruct the secret s. Such a scheme is called a (t, n) secret sharing scheme.

Some of the Secret Sharing schemes assume long-lived shares; however the protection provided by these schemes may be insufficient after some time. Several faults might occur, shares can gradually be corrupted/compromised, hardware failure or damage may take place . One way to overcome this problem is to refresh the shares periodically. Thus the concept of proactive secret sharing was introduced.The goal of the proactive 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.

The core property of pro-active secret sharing is to renew the existing shares without changing the secret, so that previous exposures of shares will not damage the secret. This should be performed without, of course, any information-leak or any secret change. Proactive security for secret sharing was first suggested by Herzberg et al. [6] where they presented, among other things, a proactive polynomial secret sharing scheme. Proactive security refers to security and availability of secret in the presence of a mobile adversary. Herzberg et al. [6] further specialized this notion to robust secret sharing schemes and gave a detailed efficient proactive secret sharing scheme. Robust means that in any time period, the shareholders can reconstruct the secret value correctly.

A. Related Work

Secret sharing schemes were introduced by both Blakley [2] and Shamir [4] independently in 1979. Shamir's (t,n) secret sharing scheme is a threshold scheme based on polynomial interpolation. It allows a dealer D to distribute a secret s to n players, such that at least t less than n players are required to reconstruct the secret. The protocol is information theoretically secure, i.e., any fewer than t

Cite this article as: Sayantan Mandal, V. Ch. Venkaiah. "A Novel Proactive Secret Sharing." *International Conference on Information Engineering, Management and Security (2015)*:260-265. Print.

players cannot gain any information about the secret by themselves. In 1985, Chor et al. [5] extended the notion of the original secret sharing and presented the concept of verifiable secret sharing (VSS). The property of verifiability allows the shareholders to verify their shares for consistency. The proactive secret sharing(PSS) has been studied extensively in the literature [6], [7], [3],[8]. All these PSS schemes initiate the secret using a trusted party.Proactive secret sharing scheme based on Verifiable Secret Sharing (VSS) provides strong security against an active attacker. It combines the secret sharing scheme with a periodical share update process to ensure the overall security of a system.Through update mechanism, old shares become useless. Even to steal a secret; however, an attacker needs to intrude on at least t participants during the same time period if security is maintained in a (t; n) threshold secret sharing scheme.

1) Motivation: Trusted Party is required to create and renew the shares. Also these schemes make use of polynomial generation in both the share distribution and share renewal phases; thereby increasing the computational complexity. Our motivation is to design of an proactive secret sharing without a trusted party. The scheme proposed in this report is independent of trusted party and uses the polynomial generation only for share distribution and not for share renewal phase. Thus our scheme has the advantage that shares will be renewed without Dealers involvement. And polynomial is generated once in share distribution phase, share renewal phase make use of old share to generate new share without changing the secret.

2) Overview: Section II, introduces the basic security model and definitions. Section III presents our share renewal scheme without a trusted party. Section IV looks at the security issues and discusses the complexity of the proposed scheme. Conclusion remarks are in Section V.

II. MODEL AND DEFINITION

A. Model

1) Existing System: In all the existing proactive secret sharing scheme found in the literature are based on the presence of the trusted party.

[Initialization]

Dealer generates a polynomial of degree t-1.

f(x) = s + d1x + : : : + dt□1xt□1

where di, 1 _ i _ t □ 1 are the random elements of the field Fq: Then, the dealer sends the share si = f(i) mod q to the server i. Since this is Shamir's secret-sharing scheme [4], any t servers can reconstruct the secret by using Lagrange interpolation, while t □ 1 cannot get any information.

[Share Updation]

Each server i generates a polynomial of degree t-1 by using random numbers di1 : : : dit□1. where f(x) = S + di1x + : : : + dit□1xt□1 This satisfies fi(0) = 0. Server i then sends the value sij= fi(j) mod q to server j, which updates its new share s(new) J as follows :

$$s_j^{(new)} = s_j^{(old)} + s_{1j} + \ldots + s_{nj} \bmod \mathrm{q}$$

Since the new shares lie on the polynomial

f(new)(x) =f(old)(x) + f1(x) + ::: + fn(x)

The new polynomial still maintains the secret value S at x = 0 , because f(new)(0) = S + 0 + ::: + 0 = S.

Observations:

•In both the [Initialization] and [Share Updation] phases, the dealer and the participants generate polynomials satisfying constraints f(0) = S and fi(0) = 0, 1 _ i _ n.

• Dealer control and coordinates all the activities like generation, distribution and updation of shares, the scheme is heavily dependent upon dealer.

B. Definition

A share renewal protocol is secure if following properties hold:

•Privacy : No information about the secret S is revealed.

•Robust : Correct re- constructibility is possible at any time when k shares are present.

III. PROPOSED SHARE RENEWAL PROTOCOL WITHOUT TRUSTED PARTY AGAINST PASSIVE ADVERSARY

A. Overview of the Scheme

In this section we construct our own share renewal scheme without the presence of a Dealer. Every participant Pi chooses a random value si and distributes it among all n participants the secret S is a function as

$$S = \sum_{i=1}^{n} s_i \delta_L^i, \text{ where n is the set}$$

of participants and _Il is the Lagrange coefficient according to L. Then each shareholder uses its old share values to obtain new shares without changing the secret S. The difference from previous schemes is that no participant uses the Shamir's scheme to distribute

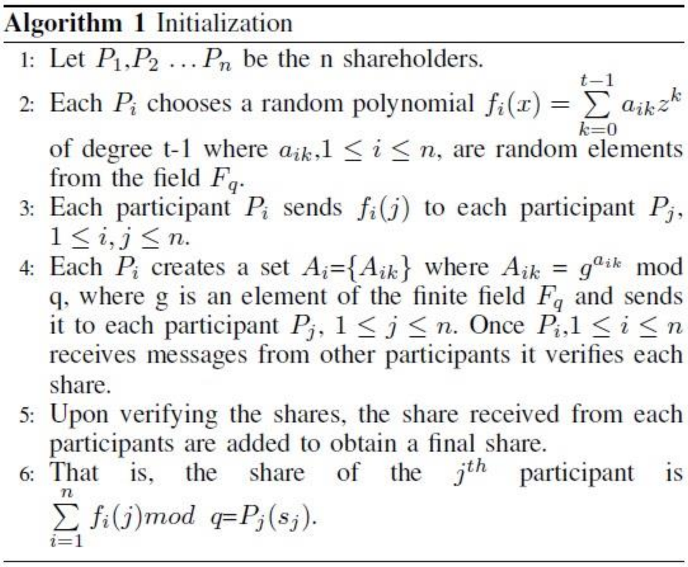
Cite this article as: Sayantan Mandal, V. Ch. Venkaiah. "A Novel Proactive Secret Sharing." *International Conference on Information Engineering, Management and Security (2015)*:260-265. Print.

share. Each participant uses its old share to create new shares without disclosing his original share. The scheme consists of three phases. We have basically divided our proposed scheme into three
phases:

•Initialization phase
•Distribution phase
•Updation phase

Each phase of our scheme is discussed below in detail. It may be noted that the Dealer is not involved in any phase of the proposed scheme. All the computation such as secret generation, share distribution and share renewal are done by the shareholders without revealing any information about the secret or their share. In addition to that its implementation is less complicated compared to other existing schemes.

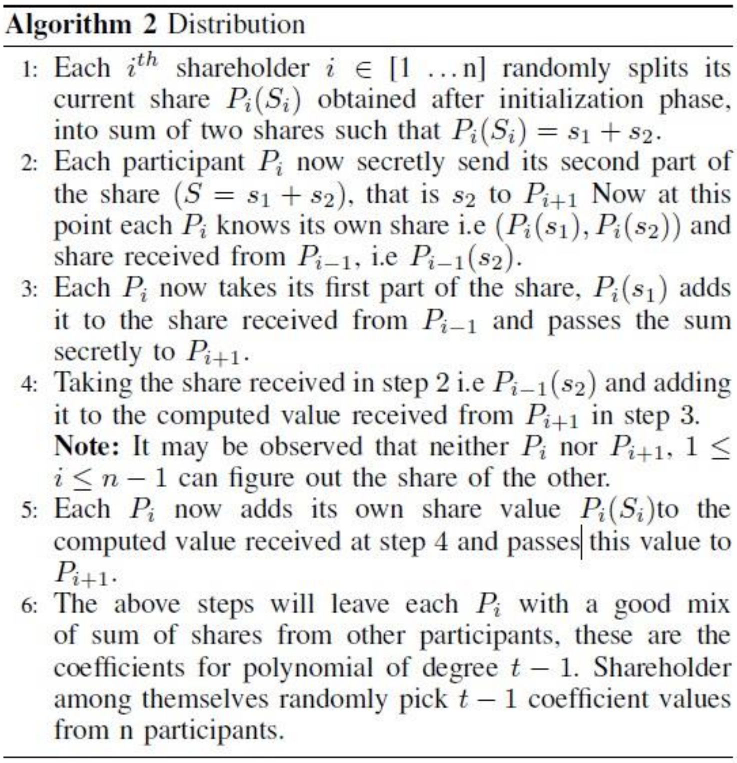
1) [Initialization]: In this phase each participant creates share value to distribute shares to other participants.



Algorithm 1 Initialization

```
Let $P_1$,$P_2 \dots P_n$ be the n shareholders.
Each $P_i$ chooses a random polynomial $f_i(x) = \sum_{k=0}^{t-1} a_{ik}z^k$ of degree t-1 where $a_{ik}$,$1 \leq i \leq n$, are random elements from the field $F_q$.
Each participant $P_i$ sends $f_i(j)$ to each participant $P_j$, $1 \leq i, j \leq n$.
Each $P_i$ creates a set $A_i$=$\{A_{ik}\}$ where $A_{ik}$ = $g^{a_{ik}}$ mod q, where g is an element of the finite field $F_q$ and sends it to each participant $P_j$, $1 \leq j \leq n$. Once $P_i$,$1 \leq i \leq n$ receives messages from other participants it verifies each share.
Upon verifying the shares, the share received from each participants are added to obtain a final share.
That is, the share of the $j^{th}$ participant is $\sum_{i=1}^{n} f_i(j) mod\ q$=$P_j(s_j)$.
```

2) [Distribution]: In this section distribution of share takes place among the participants.

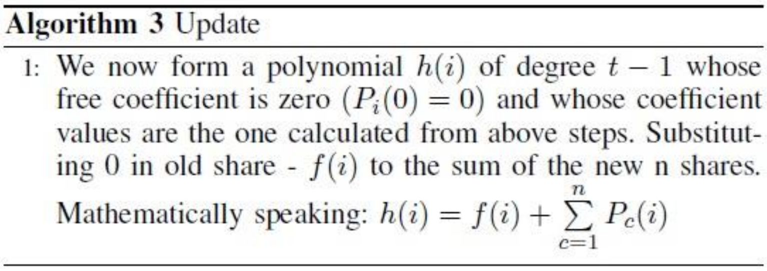


Algorithm 2 Distribution

```
1: Each $i^{th}$ shareholder $i \in [1 \dots$n] randomly splits its current share $P_i(S_i)$ obtained after initialization phase, into sum of two shares such that $P_i(S_i) = s_1 + s_2$.
2: Each participant $P_i$ now secretly send its second part of the share $(S = s_1 + s_2)$, that is $s_2$ to $P_{i+1}$ Now at this point each $P_i$ knows its own share i.e $(P_i(s_1), P_i(s_2))$ and share received from $P_{i-1}$, i.e $P_{i-1}(s_2)$.
3: Each $P_i$ now takes its first part of the share, $P_i(s_1)$ adds it to the share received from $P_{i-1}$ and passes the sum secretly to $P_{i+1}$.
4: Taking the share received in step 2 i.e $P_{i-1}(s_2)$ and adding it to the computed value received from $P_{i+1}$ in step 3.
   **Note:** It may be observed that neither $P_i$ nor $P_{i+1}$, $1 \leq i \leq n-1$ can figure out the share of the other.
5: Each $P_i$ now adds its own share value $P_i(S_i)$to the computed value received at step 4 and passes this value to $P_{i+1}$.
6: The above steps will leave each $P_i$ with a good mix of sum of shares from other participants, these are the coefficients for polynomial of degree $t-1$. Shareholder among themselves randomly pick $t-1$ coefficient values from n participants.
```

Cite this article as: Sayantan Mandal, V. Ch. Venkaiah. "A Novel Proactive Secret Sharing." *International Conference on Information Engineering, Management and Security (2015)*:260-265. Print.

3) [Update]: Now we have the new coefficient values required to create a new polynomial to update the old polynomial without changing the secret.



```
Algorithm 3 Update
1: We now form a polynomial $h(i)$ of degree $t-1$ whose
   free coefficient is zero ($P_i(0) = 0$) and whose coefficient
   values are the one calculated from above steps. Substituting
   0 in old share - $f(i)$ to the sum of the new n shares.
   Mathematically speaking: $h(i) = f(i) + \sum_{c=1}^{n} P_c(i)$
```

B. Example

[Initialization Phase]

We hereby give an example of working of the Protocols

- Let n = 4, p = 11
- Each participant chooses a random polynomial of degree t □ 1 with fi(0) = si, where si is a random value chosen by each participant.
- Four participant A,B,C and D chooses the following polynomial and create shares.

fa(x) = 5 + 7x + 2x2 mod 11
fb(x) = 4 + 2x + 5x2 mod 11
fc(x) = 10 + 7x + 2x2 mod 11
fd(x) = 2 + 3x + 2x2 mod 11

- Each participant now create n shares and distribute to each participant Pj , 1 _ j _ n
- Using the Lagrange0s interpolation the shares created are:
- participant A creates f(1) = 3 , f(2) = 5 ,f(3) = 0, f(4) = 10
- participant B creates f(1) = 0 , f(2) = 6 ,f(3) = 0 , f(4) = 4
- participant C creates f(1) = 8 , f(2) = 10 ,f(3) = 5, f(4) = 4
- participant D creates f(1) = 7 , f(2) = 5 ,f(3) = 7, f(4) = 2
- Each participant Pi sends _ij = fi(j) to each participant Pj , 1 _ i; j _ n, where _ij is the corresponding share w.r.t to the participant .

[Verifying shares using VSS]

Before proceeding to the share renewal protocol. each participant can verify whether the shares given to him by the other participant is correct or not.

From the above example, polynomial f(x) generates four shares which are distributed among four participants A,B,C and D respectively. Now say A wants to verify his share received from C then it initiates the following steps: Verification of shares : Let the encrypted values of the coefficients of the
polynomial be :

E(a0) = g10mod 11 , E(a1) = g7mod 11 , E(a2) = g2mod 11, where g is an element of the finite field Fp: Using Feldmen verifiable secret sharing scheme, we have for the first shareholder (i = 1): E(f(1)) = g8mod 11 is equal to:

E(f(i)) = E(a0)(E(a1)E(i1))_: : :_(E(at□1)E(it□1))
= E(a0 _ (a1 _ (11)) + (a2 _ (12)))
= g10+7+2 mod 11
= g8 (share verified for i = 1)

Similarly other shareholders can also verify their share values. Once share are verified we proceed to share renewal scheme. Computing Final Shares After verification of shares the share received by each Pi from other Pj are added to form
final shares.

- A computes (3 + 0 + 8 + 7) mod 11 = 7
- B computes (5 + 6 + 10 + 5) mod 11 = 4
- C computes (0 + 0 + 5 + 7) mod 11 = 1
- D computes (10 + 4 + 4 + 2) mod 11 = 9

Note: As said above secret

$$S = \sum_{i=1}^{n} s_i \delta_L^i,$$

of participants and S^{i}_{L} is the Lagrange coefficient according to L. Thus each Pi now sends its si also t - 1 coefficients
are randomly picked from above computed shares and a new polynomial is formed.

- Adding si gives 5 + 4 + 10 + 2 = 21 mod 11 = 10
- New polynomial becomes f(x) = 10 + 4x + 9x2

[Distribution]

Let the random partition of the shares A,B,C and D be

•A = 4 + 3 (A1 + A2)
•B = 2 + 2 (B1 + B2)
•C = 0 + 1 (C1 + C2)
• D = 6 + 3 (D1 + D2)

Step 2 Secretly, After exchanging second parts of their shares with the other participants we have the following scenario
•A knows A1;A2;D2
B knows B1;B2;A2
C knows C1;C2;B2
D knows D1;D2;C2
Step 3 After adding the first part of the share with the second part of the received share from the other participant, we have
• A calculates A1 + D2 and gives to B
B calculates B1 + A2 and gives to C
C calculates C1 + B2 and gives to D
D calculates D1 + C2 and gives to A
That is
A computes 4 + 3 = 7 and gives to B
B computes 2 + 3 = 5 and gives to C
C computes 0 + 2 = 2 and gives to D
D computes 6 + 3 = 9 and gives to A
Step 4 Now each participant takes the share value received in step 2 and add it to value received in step 3. That is,
• A adds D2 to (D1+C2) getting (D2+D1+C2) = (D+C2), since A does not know C2, he cannot derive D.
• Similarly B adds A2 to (A1+D2) getting (A+D2)
• Similarly C adds B2 to (B1+A2) getting (B +A2)
• Finally D adds C2 to (C1 + B2) getting (C + B2)
That is
A computes 9 + 1 = 10
B computes 7 + 3 = 10
C computes 4 + 3 = 7
D computes 1 + 2 = 3
Step 5 The participant then adds their own share to the sum arrived in the above step and passes the sum to the next participant.
That is
•A adds A to (D + C2) getting (A + D + C2) and passes to B.
• B adds B to (A + D2) getting (B + A + D2) and passes to C.
• C adds C to (B + A2) getting (C + B + A2) and passes to D.
• D adds D to (C + B2) getting (D + C + B2) and passes to A.
That is,
A computes 7 + 10 = 17 passes to B
B computes 4 + 10 = 14 passes to C
C computes 1 + 7 = 8 passes to D
D computes 9 + 3 = 12 passes to A

Privacy check : At this stage of Algorithm
• A knows A1, A2, D2, (D1 + C2), (D + C + B2), A knows D2 however he cannot derive D, since D1 and C2 are not known individually to A.
• B knows B1, B2, A2, (A1 + D2),(A + D + C2), B knows A2, however he cannot derive A, since A1 and D2 are not known individually to B.
• C knows C1, C2, B2, (B1 + A2), (A + B + D2) C knows C2, however he cannot derive B, since B1 and A2 are not known individually to C.
• D knows D1, D2, C2, (C1 + B2), (C + B + A2) D knows C2, however he cannot derive C, since C1 and B2 are not known individually to D.
C. Update
•With the arrival of new shares old shares are erased and new shares are kept. Thus new shares are
A:12 , B:17 , C:14 , D:8
• Above steps generate coefficients for new polynomial, Now we want to form polynomial of degree two, any two coefficients. Old polynomial was

f(x) = 10 + 4x + 9x2

f(0) = 10 + 4(0) + 9(02) = 10

•Now we form new polynomial from above coefficient

g(x) = 0 + 12x + 14x2

• we add above two polynomials

h(x) = f(0) + g(x)

h(x) = 10 + 12x + 14x2

• Thus h(x) is our new polynomial, we can repeat the above Distribution Algorithm with new shares to renew the shares.

IV. SECURITY CHECK

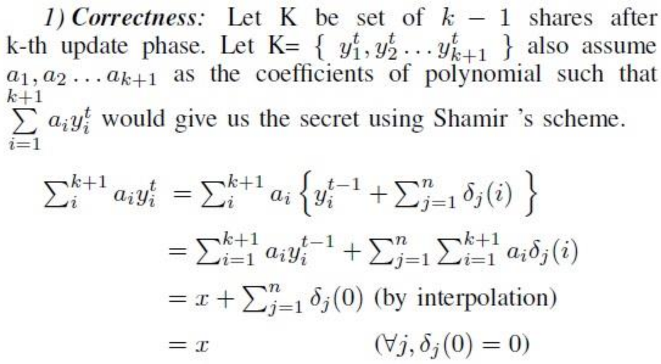
As per the Definition we can call a share renewal protocol secure if it satisfies properties :Privacy, Robustness.

A. Privacy Check

As seen in the Distribution phase of proposed share renewal protocol at no stage any shareholder gets any information about share value of any other shareholder. As each shareholder randomly splits its share value into sum of two share and throughout the Distribution phase only part of share value is used to communicate among shareholder.Thus our proposed protocol complies with privacy constraint.

B. Robustness Check

The new shares computed at the end of Update phase corresponds to secret S.The algorithm allows to re-construct the original secret whenever t - 1 shares are present.In other words any subset of t - 1 share will give us secret S.



1) Correctness: Let K be set of $k-1$ shares after k-th update phase. Let K= { $y_1^t, y_2^t \dots y_{k+1}^t$ } also assume $a_1, a_2 \dots a_{k+1}$ as the coefficients of polynomial such that $\sum_{i=1}^{k+1} a_i y_i^t$ would give us the secret using Shamir 's scheme.

$$\begin{aligned} \textstyle\sum_i^{k+1} a_i y_i^t &= \textstyle\sum_i^{k+1} a_i \left\{ y_i^{t-1} + \sum_{j=1}^{n} \delta_j(i) \right\} \\ &= \textstyle\sum_{i=1}^{k+1} a_i y_i^{t-1} + \sum_{j=1}^{n} \sum_{i=1}^{k+1} a_i \delta_j(i) \\ &= x + \textstyle\sum_{j=1}^{n} \delta_j(0) \text{ (by interpolation)} \\ &= x \qquad\qquad (\forall j, \delta_j(0) = 0) \end{aligned}$$

V. CONCLUSION

In this paper, we have designed a share renewal protocol where shares can be renewed without a trusted party against passive attacker.The scheme is both robust and maintain privacy. shareholder can verify their share before beginning of the share renewal scheme.We assume secure channel exist among the shareholder to exchange share value.The correctness of the properties of the scheme is also discussed The proposed scheme is secure and practical.

REFERENCES

[1] Dahlia Malkhi,:An advance course in computer and network security.The Hebrew University of Jerusalem, Lecture Notes

[2] Blakley, G. R.: Safeguarding cryptographic keys. In: Proc. of AFIPS National Computer Conference. vol. 48, pp. 313317 (1979)

[3] Cachin, C., Kursawe, K., Lysyanskaya, A., Strobl, R: Asynchronous verifiable secret sharing and proactive cryptosystem. In: Proc. 9th ACM Conference on Computer and Communications Security, pp. 8897 (2002)

[4] A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612613.

[5] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, 2123 October, Oregon, Portland, IEEE Computer Society, 1985, pp. 383395.

[6] Herzberg, A., Jarecki, S., Krawczyk, H., Yung, M.: Proactive secret sharing or: How to cope with perpetual leakage. In: Proceedings of CRYPTO 95. LNCS, vol. 963, pp. 339352. Springer, Heidelberg (1995)

[7] Zhou, L., Schneider, F. B., Ranesse, R. V.: APSS: Proactive secret sharing in asynchronous systems. ACM Transaction on Information and System Security 8 (3), 259286 (2005)

[8] Choudhury, A., Patra, A.: Brief announcement: efficient optimally resilient statistical AVSS and its applications. In: Proceedings of PODC 12, pp. 103104 (2012)

[9] Pedersen, T.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Proceedings of CRYPTO 91. LNCS, vol. 576, pp. 129140. Springer, Heidelberg (1992)

Cite this article as: Sayantan Mandal, V. Ch. Venkaiah. “A Novel Proactive Secret Sharing.” *International Conference on Information Engineering, Management and Security (2015)*:260-265. Print.