International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Variable Member Group Authentication Protocol using Bivariate Polynomials

Suresh Grandhi, P. S. Avadhani

Abstract: Group authentication is required for secure group communication, which ensures that users in the group are valid. When a group user count is not fixed, group authentication has to handle the entry of new users and exit of current users from the group, if necessary. The challenges to group communication are Security, Integrity and Confidentiality. Currently, available group authentication schemes are complex that require heavy computation and communication overheads. Whenever the group membership is changed, the rekeying of group key process is a challenging task. Thus, in this paper, we propose a variable number group authentication mechanism based on the Lagrange interpolation using bi-variate polynomials. Our proposed scheme handles the generation of the group key and validation effectively. The proposed model shares secret keys to the group user and authenticates all users participated in the group using a single computation and individual users when required. The proposed scheme has a group manager (GM) authenticating all group users and also generates a group key for validating member authenticity. GM is responsible for authenticating and validating each user in the group. GM takes care of members entry and exit from the group. During the changes to the group membership, rekeying is necessary. Our proposed scheme efficiently handles the rekeying process. The proposed scheme also handles backward and forward confidentiality during the group conversation. The security analysis of our scheme guarantees Forward Secrecy, Backward Secrecy, Integrity, Confidentiality and Availability. Our proposed method works effectively for dynamic group communications, where the group membership changes quite frequently.

Keywords: Group Authentication, Variable Group Members, Lagrange Interpolation, Bi-variate Polynomials, Group communication.

I. INTRODUCTION

In group communication, all the users must be authenticated and verified. Secure communication applications must provide user authentication and group key creation as essential services. User authentication process helps in identifying the participating members. Group key is used by the group for securing the group conversations. There are two common authentication approaches, 1) Knowledge based [1,2] and 2) key based authentication schemes. [3,4] Knowledge based approach has security concerns [5]. User tendency is to use easy and familiar passwords. Simple and familiar passwords are easily decoded by hackers. Public key and Private Key based authentication require a valid certificate authority to provide authenticated public keys. Also, the key exchange process is complex and process intensive approach. Performance is the most critical factor of key based authentication. A better and easy scheme is to be developed for securing Group Communication. User validation and securing the group communication are the two important aspects of any group conversation. A group communication is secure only if it validates all the users and protect entire group conversation. All the members of the group must be authenticated in a secure group communication. George Thomas et al. [6] proposed a method that uses a one-time session key for each group along with individual security. USB based key is used by individual users to increase the security further. This process uses Shamir's [12] famous secret sharing method to create individual shares for all the group users, and Lagrange Interpolation method to construct individual member key share. Distribution of shared secret keys for all the group users is called as Key establishment process [14]. Secret keys are used to secure the messages transmitted during the communication and keeping the integrity of them. Key Agreement and Key Transfer protocols are the two prominent key establishment protocols.

Key Generation Center (KGC) plays an important role in Key transfer protocols. KGC chooses a group key for communication among the group members during the group initialization process. Key agreement protocol uses public keys to create group key. Group key works as a session key for the communication among the group members. Our proposed scheme addresses the establishment of a session key for group communication. During registration process, KGC uses another secret key to encrypt session keys. [7] Vijaya Lakshmi et al. proposed a key transfer protocol that uses secret sharing scheme for authentication. Group key is transmitted by KGC to authorized group members. Group key cannot be accessed by unauthorized users. They claim that their scheme is information-theoretically secure. Transportation of group key is done based on authentication.

KGC acts as a trusted party in Group key transfer protocol. Also, it creates and transfers the group key to all the members in a secure manner. KGC registers all the users and subscribes them for key distribution. KGC is responsible for keeping track of all the registered users and delete inactive users. KGC sends a secret key to all the users during registration process.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Suresh Grandhi, Research Scholar, Department of Computer Science and Systems Engineering (CSSE), A. U. College of Engineering, Andhra University, Vizag (Andhra Pradesh), India. Email: suresh.grandhi@gmail.com.
Dr P S Avadhani*, Professor, Department of Computer Science and Systems Engineering (CSSE), A. U. College of Engineering, Andhra University, Vizag (Andhra Pradesh), India. Email: psavadhani@yahoo.com.

KGC uses encrypting methods to send the secret keys to all the users. Message checksum is also calculated and shared during the group authentication. A computationally secure encryption algorithm is used for group key transmission. Harn [8] proposed a secret sharing protocol in place of encryption algorithm. Designing a Group key scheme to securely deliver messages to the group users is required for group communication. Any group communication protocol should handle registering users, keeping track of them, adding new users, exiting current users and securing the communication among the group users. The proposed mechanism is an extension to the Group Authentication Scheme defined by Shi et al. [9]. In their scheme, they defined Group authentication method that works for fixed group size. Our scheme is extended to a variable number of users. Also, our method is extended to handle issues with Lagrange Interpolation errors. As part of the proposed scheme, Lagrange Interpolation and bivariate polynomials are used to generate key shares to be distributed among the users and these shares along with Lagrange Interpolation basis values are used to verify the group users.

II. METHODOLOGY

In this section, an authentication scheme is proposed for handling groups with variable number of users using Lagrange interpolation and bivariate polynomials.

A. Lagrange Interpolation

Lagrange Interpolation polynomials are used for polynomial interpolation. It is a method for finding the equation corresponding to a curve having some data points.

Given $(n+1)$ points, with distinct x – coordinates $\{(x_i, y_i)\}_{i=0}^{n}$, find a polynomial $L(x)$ of degree n, which passes through all points. The following is the Lagrange Interpolation function $L(x)$.

$$L(x) = \sum_{i=0}^{n} y_i l_i(x)$$

Where $l_j(x)$ is given by:

$$l_j(x) = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_n)}{(x_j - x_n)}$$

When $x = x_j$, $l_j(x) = 1$.

When $x = x_i$ $(i \neq j)$, $l_j(x) = 0$.

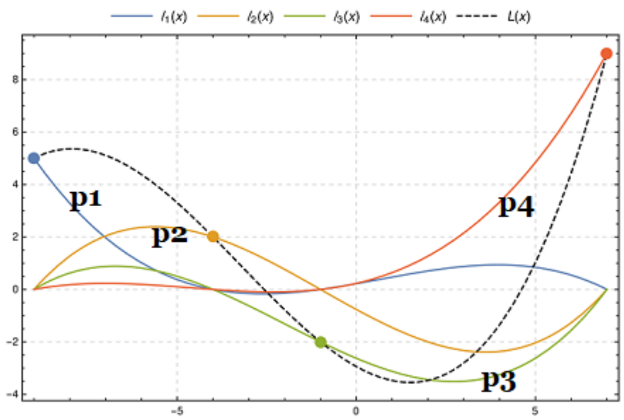

Fig. 1. Polynomial Passing through all points.[10]

Consider (x_i, y_i) $(i = 0,1,2,3)$ indicate four points $(-9,5), (-4,2), (-1,-2), (7,9)$ respectively. The four lines p1, p2, p3 and p4 denote the scaled basis polynomials $y_i l_i(x)$ $(i = 0,1,2,3)$respectively. A black dotted line passes through all four points, that combines all the four basis polynomials.

B. Polynomial of two variables (Bivariate)

A Bivariate Polynomial of degree n is a polynomial in two variables x, y and has the following form.[13]

$$f(x, y) = \sum_{i,j} a_{i,j} x^i y^j \qquad (1)$$

It is often represented in binary form as $< a_0, a_1, a_2, \ldots a_n >$.

The process assumes that GM is secure which is presented as a reasonable assumption. The following is the matrix form of bivariate polynomial.

$$\mathbf{f(x, y)} = (x^0 \ \ldots \ x^n) \begin{vmatrix} a_0 & \cdot\cdot & a_p \\ \cdot\cdot & \cdot\cdot & \cdot\cdot \\ a_q & \cdot\cdot & a_n \end{vmatrix} \begin{vmatrix} y^0 \\ \cdot\cdot \\ y^n \end{vmatrix} \qquad (2)$$

$$a_i \in \mathbb{R} \ (0 \leq i \leq n)$$

Equation (2) can be also be expressed as follows.

$$f(x, y) = a_0 + a_1 x^{\alpha 1} y^{\beta 1} + a_2 x^{\alpha 2} y^{\beta 2} + .. + a_n x^{\alpha n} y^{\beta n} \qquad (3)$$

$$\alpha_i, \beta_i \in \mathbb{N} \ and \ \alpha_i \neq \beta_i \ (0 \leq i \leq n)$$

When x = 1, equation (3) becomes a polynomial of y as given below.

$$f(1, y) = a_0 + a_1 y^{\beta 1} + a_2 y^{\beta 2} + .. + a_n y^{\beta n} \qquad (4)$$

And when y = 1, equation (3) becomes a polynomial of x as given below.

$$f(x, 1) = a_0 + a_1 x^{\alpha 1} + a_2 x^{\alpha 2} + .. + a_n x^{\alpha n} \qquad (5)$$

Thus, in equations (4) and (5) the degree of polynomials $f(x, 1)$ and $f(1, y)$ are between 1 and n.

When x = y, the polynomial in equation (3) is transformed as.

$$f(x, x) = a_0 + a_1 x^{\alpha 1 + \beta 1} + a_2 x^{\alpha 2 + \beta 2} + .. + a_n x^{\alpha n + \beta n}$$

$$f(y, y) = a_0 + a_1 y^{\alpha 1 + \beta 1} + a_2 y^{\alpha 2 + \beta 2} + .. + a_n y^{\alpha n + \beta n}$$

$$f(x, y) = f(x, x) = f(y, y) \qquad (6)$$

When x = y = 1, the polynomial is the sum of all coefficients.

$$f(1, 1) = a_0 + a_1 + \cdots + a_n = \sum_{i=0}^{n} a_i \qquad (7)$$

Retrieval Number: B7101129219/2020©BEIESP
DOI: 10.35940/ijitee.B7101.039520
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C. Generation of Key Pair and Sharing

A *key pair* is generated by GM for each and every participating member in the group. All the *n* users in the system share a public value W with the remaining group users and the GM. During the group initialization process, each user ***j*** is registered by GM to include into the group. GM generates a key pair $f(w_j,1)f(1,w_j)$ for the user ***j*** using its public value w_j and equations (4) and (5). *Key pair* for user ***j*** is designated as:

$$\boldsymbol{KP_j = \{KP_j^1, KP_j^2\} = \{f(w_j,1), f(1,w_j)\}} \quad (8)$$

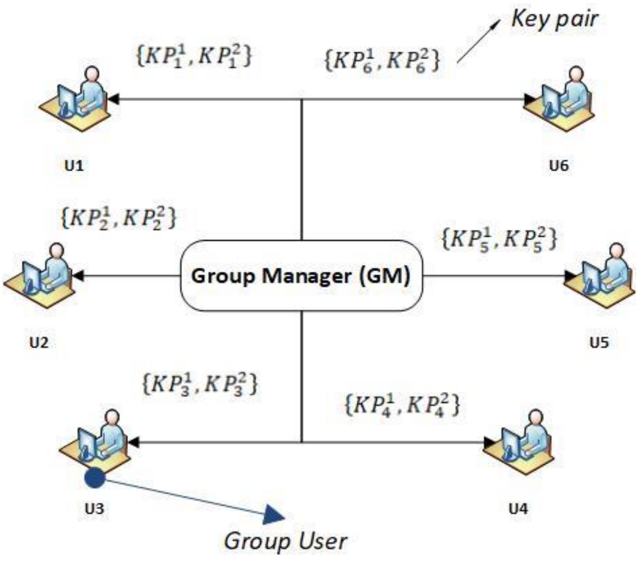

Fig. 2. Key pair distribution from GM

All the participating *m* users go through a registration process with GM. Generated *key pairs* $\{\boldsymbol{KP_i^1, KP_i^2}\}$ $(\boldsymbol{0 \le i \le m})$ are distributed by GM to the group members in a secured manner. KP_i is a secure private value which is only known to the group member ***i*** itself. Fig. 2 shows the sharing of *key pairs* from GM to group users.

The algorithm for generating key pairs is given below.

Step #1: GM generates a Bivariate Polynomial
Step #2: Each user share $\boldsymbol{W_i}$ value with GM
Step #3: GM Calculate Key Pairs $\boldsymbol{f(W_i,1)}$ and $\boldsymbol{f(1,W_i)}$ for each user and shares them respectively
Step #4: Group Manager chooses $\boldsymbol{W_{GM}}$ value
Step #5: GM Calculates Key pair $\boldsymbol{f(W_{GM},1)}$,$\boldsymbol{f(1,W_{GM})}$

D. Variable number group user authentication scheme

A group started with an initial number of $\boldsymbol{n}$ $(\boldsymbol{2 \le n \le m})$ users. Each user authenticates with GM using their identities. Using equation (2), GM choses a polynomial. Here, $f(x,1)$ and $f(1,y)$ degrees should be equal to the number of users.

During the registration phase, GM generates *m key pairs* $\{KP_i\}$ $(1 \le i \le m)$ with all the user selected public values w_i. Each *key pair* $\{KP_i\}$ generated is delivered to the corresponding member ***i***. The public value w_{GM} of GM is shared to all the users similar to any other user's public value. GM calculates its own private key pair $\{KP_{GM}\}$.

Each participating group member ***i*** calculates Lagrange basis polynomial with its key pair and the public value w_i. The Lagrange basis polynomial for group member *j* is calculated as:

$$\boldsymbol{l_j(x) = \frac{(x - w_{GM})}{(w_j - w_{GM})} \prod_{i=1, i \ne j}^{n} \frac{(x - w_i)}{(w_j - w_i)}} \quad (9)$$

GM calculate $l_{GM}(x)$ using w_{GM} as given below.

$$\boldsymbol{l_{GM}(x) = \prod_{i=1}^{n} \frac{(x - w_i)}{(w_{GM} - w_i)}} \quad (10)$$

All *n* group members calculate the interpolating value $l_j(1)$ when $x = 1$.

Each calculated user values of Lagrange basis polynomial $l_j(1)$ $(1 \le j \le n)$ along with the *key pair* received from GM are transmitted back to GM $\{\boldsymbol{KP_j^1, KP_j^2, l_j(1)}\}$

GM validates each user by checking user-submitted *key pair* and Lagrange basis polynomial values $\{\boldsymbol{KP_j^1, KP_j^2, l_j(1)}\}$ against the generated key pairs by GM. Checking of key pairs satisfies minimum security requirements for user verification.

GM uses the following formula to calculate its two values of interpolation polynomial $\{KP_{GM}^1 l_j(1), KP_{GM}^2 l_{GM}(1)\}$.

$$\boldsymbol{KP_{GM}^1 l_{GM}(1) = f(w_{GM},1) \prod_{i=1}^{n} \frac{(1 - w_i)}{(w_{GM} - w_i)}} \quad (11)$$

$$\boldsymbol{KP_{GM}^2 l_{GM}(1) = f(1,w_{GM}) \prod_{i=1}^{n} \frac{(1 - w_i)}{(w_{GM} - w_i)}} \quad (12)$$

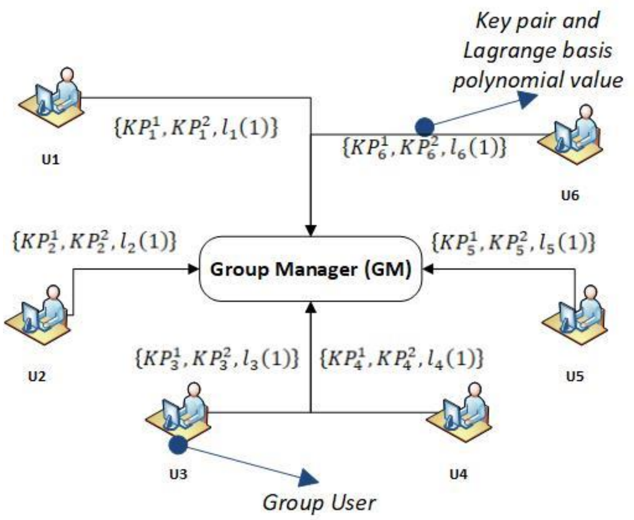

Fig. 3. Key pair and Lagrange basis polynomial value deliver to GM

After receiving all the values $\{\boldsymbol{KP_j^1, KP_j^2, l_j(1)}\}$ from *n* users of the group, GM calculates the sum of all the interpolating values at x = 1 and y = 1 as:

$$\sum \boldsymbol{para_{f(x,1)}} = \sum_{i=0}^{n} \boldsymbol{KP_j^1 l_j(1) + KP_{GM}^1 l_{GM}(1)} \quad (13)$$

$$\sum para_{f(1,y)} = \sum_{i=0}^{n} KP_j^2 l_j(1) + KP_{GM}^2 l_{GM}(1) \quad (14)$$

When all users are authenticated members of the group, GM can check the values of equations (13), (14) and (2). The sum of all the interpolating values $\sum par\, a_{f(1,x)}$ when x= 1 and $\sum par\, a_{f(x,1)}$ when y = 1 must be equal to the total value of all the parameters as in equation (2).

If the two sum results calculated by GM satisfy the following condition, then all the participated $\boldsymbol{n}$ users are valid group members [9].

$$\sum para_{f(x,1)} = \sum par\, a_{f(1,x)} = \sum_{i=0}^{n} a_i \quad (15)$$

The algorithm for group authentication is given below.

Step #1: Each user calculates the Lagrange basis polynomial value at 1 using $\boldsymbol{W_i}$ values and $\boldsymbol{W_{GM}}$.

Step #2: All the user Key values, and Lagrange values are summed up by GM.

Step #3: The total values calculated in step #2 must be equal to the sum of all the coefficients

With the selection of the bivariate polynomial along with degrees of x and y, it is observed that the calculated key pairs and Lagrange basis polynomial values are not satisfying the condition in equation (15). Also, the selection of higher values for W by each individual user is causing errors in the Lagrange Interpolation values thus, invalidating the condition in equation (15). A work around for this issue is to compare the user-submitted values $\{KP_j^1, KP_j^2, l_j(1)\}$ by GM for checking the authenticity of group users.

This extended verification process involves checking the sum of all the *key pairs* generated by GM and sent by the users. In addition to this, GM verify each user submitted Lagrange basis polynomial value.

The only caveat in this method is that the group authentication is done by each user instead of doing the validation for the entire group at once.

E. Inclusion of a new user

A new user $\boldsymbol{x}$ must be registered with GM to get included into the group. The intended user $\boldsymbol{x}$ requests inclusion into the Group. User *x* must send $w_x$value to GM. GM generates a *key pair*$\{KP_x\}$ and shares it with the new user $\boldsymbol{x}$. GM makes w_x value available to all the existing users and informs the remaining users in the group about the inclusion of user $\boldsymbol{x}$. In addition to this, GM calculates revised *key pairs* of all the users by including user $\boldsymbol{x}$ and distribute respective shares of the users to the corresponding member in a secured manner. All the users must recalculate their two values of Lagrange basis polynomial by including $w_x$the value of the new user *x* as mentioned in equation (9). Also, GM must recalculate its Lagrange basis polynomial values using equation (10).

Recalculation of key pairs ensures backward secrecy as the newly added user would not be able to access the previous key pairs.

F. Exclusion a user

There are two cases of excluding a user from the group. 1) When a user $\boldsymbol{x}$ exits from the group by informing to GM and 2) When a user $\boldsymbol{x}$ is inactive for a specific interval of time. In these two cases, GM initiates the following exit process

GM broadcasts user $\boldsymbol{x}$ as inactive, informing all the group users about user exit. GM calculates new *key pairs* for all the users, excluding the exited user and shares corresponding values with them in a secured manner. All the users must recalculate their Lagrange basis polynomial values, as mentioned in equation (9) to send them back to GM. Also, GM has to recalculate its Lagrange basis polynomial as per equation (10).

In order to maintain forward secrecy when a group user is exited, all the remaining active users along with GM should recalculate their Lagrange basis polynomial values. As the new key pairs are delivered by the GM, the exited user would not be able to access group communication any more as the exited user keys do not work anymore.

G. Example Calculation of Key Pairs and Validation

The following example shows the calculation of Key pairs and validating the group key method using a sample set of data elements.

Consider a sample Bivariate Polynomial:

$\boldsymbol{6y^3 + 5x^3y^2 + 4xy^3 + 2x^2y + 3xy^2 + 6}$

Polynomial Degree: 3

Total Number of Users: 20

Consider the following User $\boldsymbol{W_i}$ Values for all 20 users: (81, 12, 98, 92, 80, 55, 50, 85, 20, 24, 32, 48, 56, 97, 45, 30, 44, 73, 86, 67)

GM selected $\boldsymbol{W_{GM}}$ Value: 23

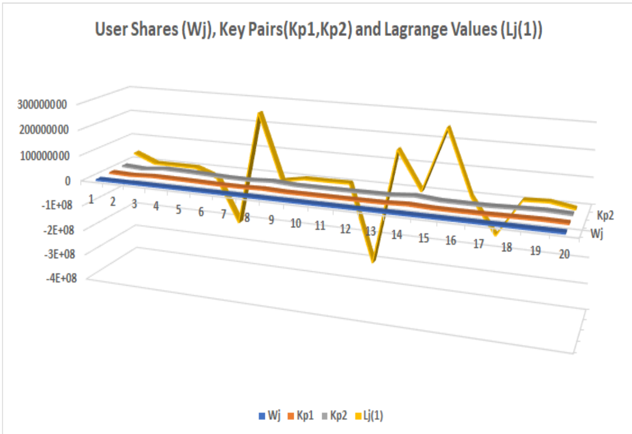

Fig.4. User Shares, Key Pairs and Lagrange Values graph

The graph in Fig. 4 shows the variations of the user calculated values $\boldsymbol{l_j(1)}$ and GM generated key pairs $\boldsymbol{KP_j^1, KP_j^2}$ for the user selected shares $\boldsymbol{w_j}$.

The User Selected Shares, GM Calculated Key Pairs and Lagrange Values calculated by the users are given in Table 1. It can be observed that the values are so randomly distributed, implying that the security is strengthened.

Retrieval Number: B7101129219/2020©BEIESP
DOI: 10.35940/ijitee.B7101.039520
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It is computationally intensive for any intruder to compromise the security of group key. Every time, there is a change in the group membership, all these keys are recomputed resulting randomly distributed values. So, when the group is dynamic, it ensures security as it is hard to compute the keys by any intruder.

Table 1. User Shares w_i, Key Pairs KP_i^1,KP_i^2 and Lagrange Values $l_i(1)$.

U#	W_i	KP_i^1	KP_i^2	$l_i(1)$
1	81	2670906	5367066	35691809.61
2	12	9024	18462	196.6669472
3	98	4725866	9488954	-17077.8999
4	92	3911024	7854782	-174695.74
5	80	2573372	5171366	-32243081.7
6	55	838322	1688066	-208829265
7	50	630362	1270106	248721594.3
8	85	3085682	6199226	-16449710.7
9	20	40952	83246	-12967.7783
10	24	70452	142902	78942.9073
11	32	166124	335942	1384411
12	48	557916	1124454	-3E+08
13	56	884756	1781366	1.52E+08
14	97	4582874	9202202	36011.22
15	45	460002	927546	2.51E+08
16	30	137022	277266	-935315
17	44	430112	867422	-1.4E+08
18	73	1956266	3932954	5919442
19	86	3195686	6419906	10154716
20	67	1513274	3043682	-5710052

As per equation (15) All the three calculated total values are equal to 26.

$$\sum par\, a_{f(x,1)} = 26$$

$$\sum par\, a_{f(1,x)} = 26$$

$$\sum_{i=0}^{n} a_i \ = 26$$

The group key correctness is validated by checking the values sent by the users and comparing them with the sum of all coefficients using equations 13, 14 and 15. This example works for 20 users with a lesser degree (3) polynomial. Although a significantly small degree bivariate polynomial (in this example, it is 3) is taken, the security is maintained even the number of users is 20.

III. SECURITY ANALYSIS

Security Analysis focuses on different criteria to verify the security of the proposed scheme.

A. Confidentiality

GM distributes individual key pairs securely to all the group members during the registration process. Key pair is private information specific to each user, and it must be protected by each user. They should not share it with other users in the group. Even if any user compromises on the key pair, the proposed model can identify the leak and the culprit user. This is done by the GM while verifying the individual key pairs during the validation process.

Also, GM has its own key pairs which are essential in determining the group key. It is a significant information in generating group key. Group key cannot be inferred by anyone as the GM key pair is private and confidential information. GM is responsible for keeping the confidentiality of the communication

B. Integrity

If there are some attackers who modify/forge transmitted key pairs, it cannot pass the GM authentication as it won't satisfy the condition laid in formula (15). If any two members share the same key pairs to GM, then the culprit can be easily identified. GM knows the initial registration value of each user so the culprit can be identified. The proposed scheme ensures the Integrity of the system.

C. Availability

The proposed method works for any n users when a bivariate polynomial of degree n is used. This ensures availability.

D. Forward Secrecy

Forward Confidentiality ensures that the user who exits the group would not be able to access the future keys. The proposed scheme effectively maintains forward secrecy as the user who exits from the group cannot be able to communicate with the group any longer after the exit process is completed by GM and key pairs are re-calculated. The earlier key-pairs are not valid any more. GM excludes the user from the key pair calculation as well as all the users would do the same by excluding the exited user.

E. Backward Secrecy

Backward Confidentiality ensures that whenever an additional user is entered to the group, the new user would not have access to the previous communication details. The proposed scheme effectively maintains backward secrecy as the user who enters into the group won't be able to gather previous communications as the user is allowed access only after GM generates new user key pairs and all the rest of the users generate the same. User entry timestamp would be used to provide access to the communication to conceal any previous communication available if any.

IV. PERFORMANCE ANALYSIS

The time complexity of each user communication is $O(n)$ where n is the number of users in the group. In the proposed method, each user is communicating with the GM and do not involve in any communication with the other group users. The users are required to perform calculation of their Lagrange basis polynomial value whenever users are added or exited from the group.

This is required for changes in group membership and ensuring security in keeping backward secrecy and forward secrecy.

V. CONCLUSION

In this paper, a variable number of group member authentication scheme is proposed ensuring security. Lagrange Interpolation and Bivariate polynomials are used to compute user keys and the group key. Bivariate polynomials are used to generate a pair of keys for each participating user, making the security two-fold. Validation of user keys and group keys are checked by using Interpolation. Whenever group membership is changed, rekeying of group key can be computed as the proposed method is computationally efficient. Intrusion into the group communication can be identified by the proposed validation method. Malicious users can be identified and tracked. As our proposed scheme is designed to be flexible with the number of users, users can be added to the group or exit from the group without compromising the security of the communication involved.

VI. FUTURE SCOPE

During the execution tests, it is observed that the proposed scheme works with a greater number of users and with fewer degree polynomials. Another mechanism can be devised by creating a random W values for each user by GM itself. This allows, GM to have a set of pre-defined and verified polynomials of lesser degrees than the user count. It increases the performance as the computations as lower degree polynomial computations are used.

REFERENCES

1. Yan J., Blackwell A., Anderson R., and Grant A., “Password memorability and security: Empirical results”, IEEE Security & Privacy Magazine, 2(5), (2004): 25-31
2. Ku W. C., “Weaknesses and drawbacks of a password authentication scheme using neural networks for multi-server architecture”, IEEE Transactions on Neural Networks, 16(4), (2005): 1002-1005
3. Downnard I., “Public-key cryptography extensions into Kerberos, IEEE Potentials, 21(5, (2002)): 30-34
4. Ren K., Yu S., Lou W., and Zhang Y., “Multi-user broadcast authentication in wireless sensor networks”, IEEE Transactions on Vehicular Technology, 58(8) (2009): 4554-4564
5. Lein Harn and Changlu Lin, “AN EFFICIENT GROUP AUTHENTICATION FOR GROUP COMMUNICATIONS’, International Journal of Network Security & Its Applications, Vol.5, No.3, May 2013
6. George Thomas, lashim lamaludheen K, Levin Sibi, Maneesh P and Mufeedh, “A Novel Mathematical Model for Group Communication with Trusted Key Generation and Distribution Using Shamir's Secret Key and USB Security”, IEEE ICCSP 2015 conference
7. Vijaya Lakshmi Pandranki, N. Krishna, “Secure Group Key Transfer Protocol Based on Secret Sharing”, International Journal of Computer Science and Information Technologies, Vol. 3 (4), 2012:4712 - 4717
8. Lein Harn and Changlu Lin, “Authenticated Group Key Transfer Protocol Based on Secret Sharing”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 6, JUNE-2010: 842-846
9. Shi Li, Inshil Doh, Kijoon Chae, “A Group Authentication Scheme based on Lagrange Interpolation Polynomial”, 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2016: 386:389
10. https://en.wikipedia.org/wiki/Lagrange_polynomial
11. L. Harn, “Group Authentication,” IEEE Trans. Computers, vol. 62, no. 9, Sep-2013:1893-1898
12. A. Shamir, “How to Share a Secret”, Communication ACM 22,11, Nov. 1979:612-613.
13. https://www.sciencedirect.com/topics/computer-science/bivariate-polynomial
14. Lein Harn, “Group Authentication”, IEEE Transaction on Computers, Vol. 62, No. 9, Sep-2013:1893-1898
15. Chin-Chen Chang, Lein Harn, and Ting-Fang Cheng, “Polynomial-based Key Management for Secure Intra-Group and Inter-Group Communication”, International Journal of Network Security, Vol.16, No.2, Mar-2014:143-148

AUTHORS PROFILE

Suresh Grandhi has received M.Tech. from Andhra University, Vishakhapatnam. The author is currently pursuing his Ph.D. from the Department of CSSE - Computer Science and Systems Engineering in Andhra University College of Engineering, Vishakhapatnam. His main research work focus on Group Authentication in fixed as well as variable settings. The author has 23 years of experience in software design and development in India, Austria and USA. The author is also having 12 years of teaching experience and dealt with various subjects in Computer Science like Database Management, Computer Networks, Cloud Computing, Python Programming, Data Structures, Machine Learning etc. The author had trained various M.Tech. & B.Tech. Engineering students during his 12 years of teaching career.

Prof. P S Avadhani pursued M.Tech. and also Ph.D. from IIT Kanpur. He is working as a Professor in the Department of CSSE (Computer Science and Systems Engineering) in Andhra University College of Engineering, Vishakhapatnam. His areas of interest are Cyber Security, Fuzzy Logic, Cyber Forensics, Computer Algorithms, Public Cryptography, Data and Network Security. The author has written 6 books in Computer Science Engineering on various subjects. The author has published 58 papers in International Journals, 8 papers in National Journals, 38 research papers in Conferences at International level and 9 research papers in National level conferences. Several awards have been awarded for his excellence in Teaching, Research and Administration like “State Best Teacher Award”, “Best Researcher Award”, “Distinguished Principal Award” from Andhra Pradesh state government. The author had trained various PhD., M.Tech. & B.Tech. Engineering students during his 35 years of long teaching career.