e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

GROUP AUTHENTICATION USING MULTI-VARIATE POLYNOMIALS

Swathi A Grandhi[*1], Suresh Grandhi [*2],

[*1] M.Tech. Student, Department of CSE, Grandhi Varalakshmi Venkata Rao Institute of Technology, Bhimavaram, Andhra Pradesh, India

[*2] Associate Professor, Department of CSE, Grandhi Varalakshmi Venkata Rao Institute of Technology, Bhimavaram, Andhra Pradesh, India

ABSTRACT

Group authentication helps keep the group communication secured by checking the authenticity of the users involved in the group. Present group authentication methods involve heavy computation and also uses private and public key infrastructure which requires more resources and effort. In this paper, we propose a group authentication mechanism using Multi-variate polynomials and Lagrange Interpolation. The proposed model uses a group manager who controls the group communication and all the participant members shared their private secret keys with the Group Manager. A method of verifying the group authentication for tri-variate polynomials is provided. Similar methodology can be adopted for bi-variate and polynomials with a greater number of variables. The proposed scheme also complies with backward and forward confidentiality throughout the group communication process. The proposed algorithm guarantees Confidentiality, Integrity and Availability.

KEYWORDS: Group Communication; Bi-variate Polynomials; Tri-variate Polynomials; Multi-variate Polynomials; Group Authentication; Lagrange Interpolation.

I. INTRODUCTION

Group communication helps collaborate teams to work together. Keeping the group communication secure is essential and plays an important role in increasing the group collaborated activities over the Internet and Intranets. User authentication helps in identifying the participating group members. Group Key is used by all the group members for securing the group communication. Knowledge based [1,2] and Key based authentication schemes are two prominent authentication approaches. [3,4] Knowledge based approach has security concerns.

In Group communication, a group key scheme must be designed to share messages among the group members in a secured manner. Group communication protocol must provide ways to enroll users, tracking them, adding new users, removal of users from an existing group. The proposed schemes are extensions to the Group Authentication Scheme presented by Shi et al. [4] They defined Group authentication method which works for constant group membership.

The proposed scheme is extended to a variable number of users and using multi-variate polynomials. The proposed scheme uses Lagrange Interpolation and Multi-variate polynomials to generate key shares to be shared among the group users, and these shares along with Lagrange Interpolation basis values are used to verify the group users.

II. METHODOLOGY

a) Lagrange Interpolation:

Lagrange Interpolation formula provides a method to construct a polynomial with certain values at arbitrary points.

For $(n+1)$ points, with different x – values $\{(x_i, y_i)\}_{i=0}^{n}$, identify a polynomial $L(x)$ of degree n, which

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

passes through all data points. The following formula is the Lagrange Interpolation function $L(x)$.

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

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

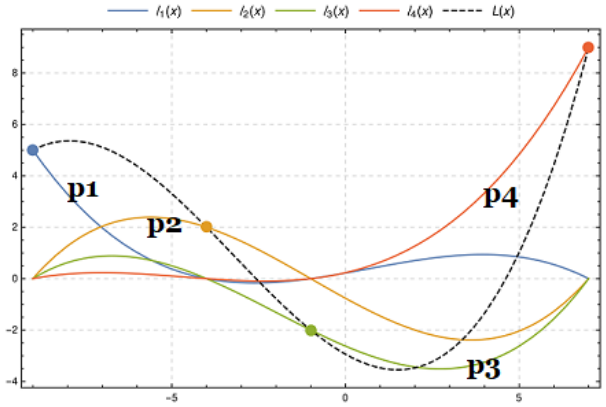

Fig-1: Polynomial with four points.[1]

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

b) Polynomial of two variables (Bi-variate):

A Bivariate Polynomial of degree *n* is a polynomial with two variables x, y and can be denoted as given below.[14]

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

The above Equation can be expressed as:

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

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

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

In the equation (2) if x value is substituted with 1 then the equation (2) would be a polynomial of y.

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

In the equation (2) if y value is substituted with 1 then the equation (2) would be a polynomial of x.

$$f(x,1) = a_0 + a_1 x^{\alpha 1} + a_2 x^{\alpha 2} + .. + a_n x^{\alpha n} \quad (4)$$

Equation $f(x,1)$ and $f(1,y)$ have the degree of polynomials between 1 to n.

If x = y, the polynomial in equation (2) is represented as.

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

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

$$f(x,y) = f(x,x) = f(y,y) \quad (5)$$

If x = y = 1, the polynomial is the total of all the constants.

$$f(1,1) = a_0 + a_1 + \cdots + a_n = \sum_{i=0}^{n} a_i \quad (6)$$

c) Tri-variate Polynomial:

A three variable polynomial which is also called as tri-variate polynomial can be denoted as given below. [5]

$$f(x,y,z) = \sum_{i,j,k} a_{i,j} x^i y^j z^k \quad (7)$$

Equation (8) expanded form is as follows.

$$f(x,y,z) = a_0 + a_1 x^{\alpha 1} y^{\beta 1} z^{\gamma 1} + a_2 x^{\alpha 2} y^{\beta 2} z^{\gamma 2} + .. + a_1 x^{\alpha n} y^{\beta n} z^{\gamma n} \quad (8)$$

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

Polynomial of y can be obtained when value 1 is substituted in place of x and z.

$$f(1,y,1) = a_0 + a_1 y^{\beta 1} + a_2 y^{\beta 2} + .. + a_n y^{\beta n} \quad (9)$$

Polynomial of x can be obtained when value 1 is substituted in place of y and z.

$$f(x,1,1) = a_0 + a_1 x^{\alpha 1} + a_2 x^{\alpha 2} + .. + a_n x^{\alpha n} \quad (10)$$

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

Polynomial of z can be obtained when value 1 is substituted in place of x and y.

$$f(1,1,z) = a_0 + a_1 z^{\gamma 1} + a_2 z^{\gamma 2} + .. + a_n z^{\gamma n} \quad (11)$$

When x, y and z have the same values then equation (8) can be represented as:

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

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

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

$$f(x,y,z) = f(x,x,x) = f(y,y,y) = f(z,z,z) \quad (12)$$

When all the variables x, y and z are equal to 1 then the polynomial is the sum of all constants.

$$f(1,1,1) = a_0 + a_1 + \cdots + a_n = \sum_{i=0}^{n} a_i \quad (13)$$

III. MODELING AND ANALYSIS

Here, we considered tri-variate polynomial for verifying the group authentication. The method proposed can be used for bi-variate polynomials as well as polynomials with a greater number of variables.

Calculation of User Key Triplets

All the members in the group share their corresponding W values which are publicly available to all the users. Users calculate their corresponding key triplet and share them with the Group Manager. When the group is initialized, each user gets registered with the Group Manager. Key triplet for user j is represented as:

$$KP_j = \{KP_j^1, KP_j^2, KP_j^3\} = \{f(w_j,1,1), f(1,w_j,1), f(1,1,w_j)\} \quad (14)$$

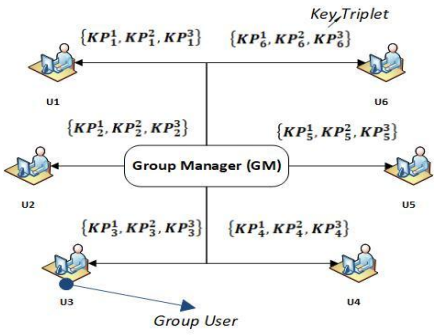

Fig-2: Key Triplet Distribution From GM

Every group member i computes Lagrange basis polynomial value with its key triplet and their corresponding public value. The Lagrange basis polynomial value for group member j is calculated as:

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

$$l_j(x) = \frac{(x-w_{GM})}{(w_j-w_{GM})}\prod_{i=1,i\neq j}^{n}\frac{(x-w_i)}{(w_j-w_i)} \quad (15)$$

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

$$l_{GM}(x) = \prod_{i=1}^{n}\frac{(x-w_i)}{(w_{GM}-w_i)} \quad (16)$$

All participating group users calculate their corresponding interpolating value $l_j(1)$ when $x = 1$.

The Key triplets and Lagrange basis polynomial values $l_j(1)\ (1 \le j \le n)$ of all the users are computed and are shared back to GM

$$\{KP_j^1, KP_j^2, KP_j^3, l_j(1)\}$$

Group Manager checks all the user submitted *key triplets* and Lagrange basis polynomial values$\{KP_j^1, KP_j^2, KP_j^3, l_j(1)\}$ with the generated key triplets by Group Manger. Verifying the key triplets meets the minimum-security requirements for user membership.

Group Manager uses the following formula to compute its two values of interpolation polynomial

$\{KP_j^1, KP_j^2, KP_j^3, l_j(1)\}$.

$$KP_{GM}^1 l_{GM}(1) = f(w_{GM}, 1, 1)\prod_{i=1}^{n}\frac{(1-w_i)}{(w_{GM}-w_i)} \quad (17)$$

$$KP_{GM}^2 l_{GM}(1) = f(1, w_{GM}, 1)\prod_{i=1}^{n}\frac{(1-w_i)}{(w_{GM}-w_i)} \quad (18)$$

$$KP_{GM}^3 l_{GM}(1) = f(1, 1, w_{GM})\prod_{i=1}^{n}\frac{(1-w_i)}{(w_{GM}-w_i)} \quad (19)$$

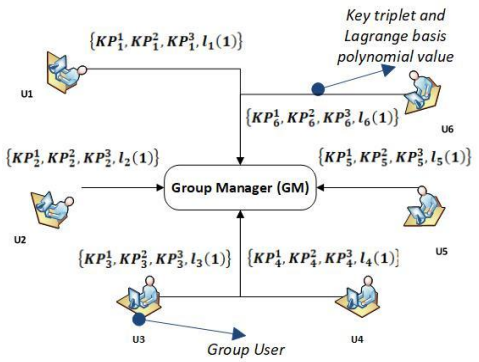

Fig-3: Key Triplet and Lagrange Basis Polynomial Value Deliver to GM

After getting all the values $\{KP_j^1, KP_j^2, KP_j^3, l_j(1)\}$from *n* users of the group, Group Manager computes the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:02/February-2020 www.irjmets.com

total value of all the interpolating values at x = 1, y = 1 and z = 1 as:

$$\sum par\ a_{f(x,1,1)} = \sum_{i=0}^{n} KP_j^1 l_j(1) + KP_{GM}^1 l_{GM}(1) \quad (20)$$

$$\sum par\ a_{f(1,x,1)} = \sum_{i=0}^{n} KP_j^2 l_j(1) + KP_{GM}^2 l_{GM}(1) \quad (21)$$

$$\sum par\ a_{f(1,1,x)} = \sum_{i=0}^{n} KP_j^3 l_j(1) + KP_{GM}^3 l_{GM}(1) \quad (22)$$

When all group members are authenticated, Group Manager can check the values of equations (15), (16), (17) and (2). The total of all the interpolating values $\sum par\ a_{f(x,1,1)}$ must be equal to the value of $\sum par\ a_{f(1,x,1)}$ and must be equal to the value of $\sum \text{par}\ a_{f(1,1,x)}$. Calculated total interpolating values must be equal to the total value of all the parameters as in equation (11).

If all the three sum results calculated by GM are equal hence satisfying the following condition, then all the participating users are valid group members [9].

$$\sum par\ a_{f(x,1,1)} = \sum par\ a_{f(1,x,1)} = \sum par\ a_{f(1,1,x)} = \sum_{i=0}^{n} a_i \quad (23)$$

We noticed that the calculated key triplets and Lagrange basis polynomial values are not satisfying the condition in equation (23) when the group member count is more than the maximum degree of the variables x, y and z. An alternative way to verify is to compare the user-calculated values $\{KP_j^1, KP_j^2, KP_j^3, l_j(1)\}$ by Group Manager for validating the authenticity of group users.

Once issue with this method is that the group authentication is performed by checking each user instead of doing the validation for the entire group in a single computation.

IV. RESULTS AND DISCUSSION

Calculation of Group Key

An application is developed for Calculation of Group Keys with the proposed method in C#.NET Windows Forms. This application allows the user to define a tri-variate polynomial and enter the Group Manager Secret and Group User Secrets. This application is also designed to generate random secret values for Group Members within a specified range and number of group users.

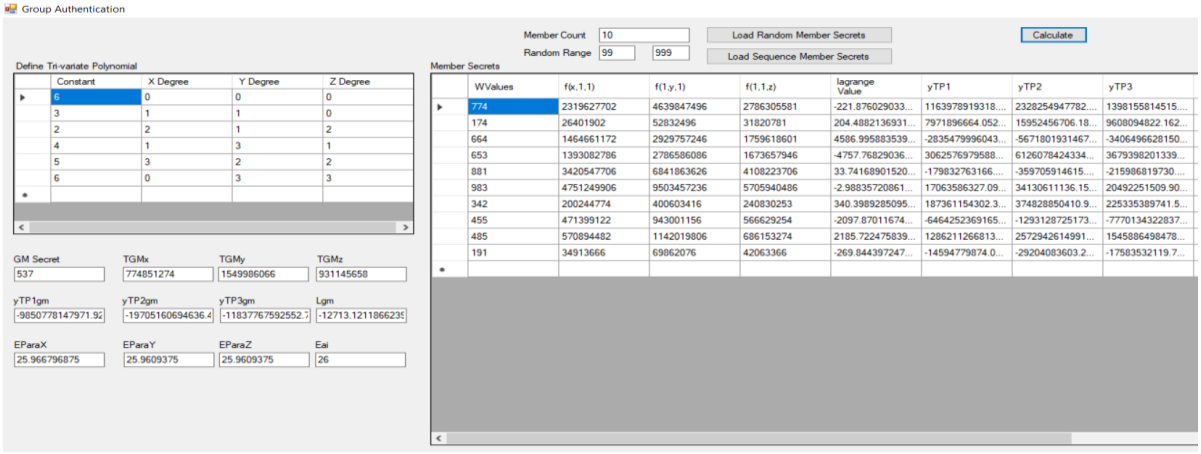

Fig- 4: Application For Calculation of Group Key and Verifying the Group Membership

Invalid Member Key Detection

When a member tries to intrude into the group with an estimated secret share, the proposed method identifies the intruding member as the incoming share would be different from the existing shares communicated by the group members. When a member uses an existing user's secret, the proposed method can identify the compromised secret key by checking the group member shares received during the initial group key establishment process.

When a group member is left, Forward secrecy has to be maintained. GM achieves this by informing the exit event to all the group members and recalculate the Lagrange basis polynomials with the remaining group members. Recalculated Lagrange basis values are shared to the remaining active group members. When a new member is joining into the group, Backward secrecy has to be maintained. GM informs the entry of new member to all the existing group members and shares recalculated Lagrange basis values with the new member shared secret.

Confidentiality

Confidentiality of the group communication is achieved by using the key triplets generated during the registration process. Key triplets of each user is specific to that member and if any user compromises on these private values, the Group member identifies the culprit by checking the key triplet values. GM calculates its own key triplets which are part of the group key calculation. As Group Manage key triplet is private and confidential information, non-member users would not be able to construct the group key.

Integrity

When an attacker uses a compromised key triplet, Group Manager would identify the attacker using the condition in equation (23). When two users submitting the same set of triplets, the equation (23) will fail ensuring the integrity of the system.

Availability

The proposed method is proved to work with ***n+1*** users with n degree multi-variate polynomial ensuring the availability of the system.

Performance Results

The proposed method verifies the group key at once instead of checking all the group member and group manager key shares. The time complexity is $O(n)$ for n users. The proposed method requires each user to communicate with the Group Manager and the users do not need to communicate among themselves. This increases performance as the users do not need to communicate with every user in the group.

V. CONCLUSION

Group authentication scheme using multi-variate polynomials and LaGrange interpolation is proposed ensuring security. The proposed method can be used from bi-variate, tri-variate and higher variable multi-variate polynomials. The security of the proposed method increases with the number of variables in the polynomials. Unauthenticated or mischievous users are not allowed using the proposed method. The proposed method is designed to be adaptable for any number of users. New users can be included to an existing group or existing users can be excluded with no security breach.

VI. REFERENCES

[1] https://brilliant.org/wiki/lagrange-interpolation/

[2] Suresh Grandhi, P.S. Avadhani, "International Journal of Engineering Resarch & Technology", Volume 8, Issue 11, November 2019.

[3] A. Shamir, "How to Share a Secret", Communication ACM 22,11, Nov. 1979: Pages:612-613.

[4] 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: pages:386:389

[5] https://en.wikipedia.org/wiki/Polynomial

[6] Lein Harn, "Group Authentication", IEEE Transaction on Computers, Vol. 62, No. 9, Sep-2013:pages: 1893-1898

[7] 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.