J-MATH
Journal of Mathematics Theory and Applications
Vol. 4, No. 1, Oktober 2025, pp. 01 – 08
ISSN Online: 3025-2628

IDENTIFIKASI PELAKU KECURANGAN DENGAN MENGGUNAKAN POLINOMIAL BIVARIAT SIMETRIS

Aprilia Lopo[1*], Zulkaidah Nur Ahzan[2], Fitriani[3], Nugraha K. F. Dethan[4]
[1,4] Program Studi Matematika, Fakultas Pertanian, Sains dan Kesehatan, Universitas Timor
[2,3] Program Studi Pendidikan Matematika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Timor
Lopoaprilia04@gmail.com[1], idhamanieszt@gmail.com[2], bhrfitriani@gmail.com[3], nugrahadethan@unimor.ac.id[4]

ABSTRACT
The purpose of this study is to identify fraudsters using Symmetric Bivariate Polynomials with one share detecion. This type of research is quantitative using the method Secret Sharing Scheme (SPR). Where in this study combines several schemes, one of which is Scheme Liu et al. (2018). The scheme Liu et al. (2018) is a Symmetric Bivariate Polynomial scheme, in the writing of the Liu et al. (2018) scheme they identy fraudsters using two share detections. In the study, researchers also use Symmetric Bivariate Polynomials to identify fraudsters, so that the results are obtained, namely at the secret shering stage using Symmetric Bivariate Polynomials, at the reconstruction stage using Lagrange interpolation and using Symmetric Bivariate Polynimials with one share detection $e_{i,1} = f_i(d)$ where (d) is a random integer. Thus it can be concluded that the identification of fraudsters using Symmetric Bivariate Polynimoials is able to identify fraudsters and by using one share detection is faster in the computation process.
Keyword: **Symmetrical Bivariate Polinomial, Fraud Identification Scheme**

ABSTRAK
Tujuan dari penelitian ini adalah mengidentifikasi pelaku kecurangan menggunakan Polinomial Bivariat Simetris dengan satu *share* deteksi. Jenis penelitian ini adalah kuantitatif dengan menggunkan metode Skema Pembagian Rahasia (SPR). Dimana pada penelitian ini menggabungkan beberapa skema, salah satunya yaitu Skema Liu *et al.* (2018). Skema Liu *et al.* (2018) merupakan skema Polinomial Bivariat Simetris, dalam tulisan skema Liu *et al.* (2018) mereka mengidentifikasi pelaku kecurangan menggunakan dua *share* deteksi. Pada penelitian ini, peneliti juga menggunakan Polinomial Bivariat Simetris untuk mengidentifikasi pelaku kecurangan, sehingga diperoleh hasilnya yaitu pada tahap pembagian rahasia menggunakan Polinomial Bivariat Simetris, pada tahap rekontruksi menggunakan interpolasi lagrange dan menggunakan Polinomial Bivariat Simetris dengan satu *share* deteksi $e_{i,1} = f_i(d)$ dimana (d) adalah bilangan bulat acak. Dengan demikian dapat disimpulkan bahwa identifikasi pelaku kecurangan menggunakan Polinomial Bivariat Simetris mampu mengidentifikasi pelaku kecurangan dan dengan menggunakan satu *share* deteksi lebih cepat dalam proses komputasi.
Kata kunci: Polinomial Bivariat Simetris, Skema Identifikasi Kecurangan

PENDAHULUAN

Skema pembagian rahasia (SPR) adalah suatu metode kriptografi yang dapat dilakukan untuk mengatasi permasalahan dalam menyimpan suatu rahasia yang berupa kunci kriptografik seperti PIN (*Personal Identification Number*) atau kata sandi (*Password*) Metode SPR dilakukan dengan membagi satu rahasia menjadi beberapa bagian yang disebut keping-keping rahasia dan kemudian didistribusikan ke beberapa orang yang berhak terhadap keping-keping rahasia tersebut (Ahzan dkk, 2020). Skema berbagi rahasia berbasis Polinomial Bivariat telah diperluas ke skema kriptografi lainnya, seperti komputasi cloud, rekontruksi rahasia ganda, dan skema berbagi gambar rahasia. Skema pembagian berbasis Polinomial Bivariat telah menarik lebih banyak perhatian dalam penelitian skema pembagian rahasia.

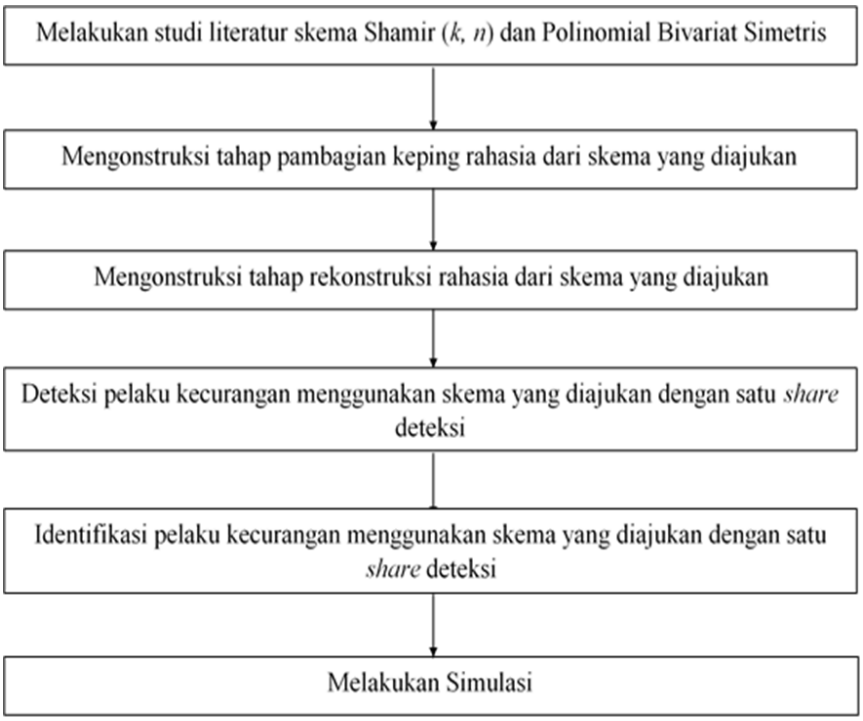
Skema pembagian rahasia pertama kali di kenal pada tahun 1979 oleh Shamir dan Blakley dimana mereka memperkenalkan konsep berbagi rahasia untuk menyimpan sebuah informasi atau keping rahasia dengan aman. Dalam skema pembagian rahasia dengan ambang batas (k, n), Namun skema berbagi rahasia shamir (k, n) juga memiliki kelemahan yaitu tidak memperhitungkan kemungkinan

jika ada pemegang keping rahasia yang melakukan kecurangan dengan memberikan keping rahasia yang salah.

Skema Liu *et al*. (2018) merupakan skema Polinomial Bivariat Simetris, dimana pada tahap pembagian keping-keping rahasia dan rekonstruksi rahasia berdasarkan Polinomial Bivariat. Skema ini terdiri dari dua algoritma, dimana algoritma pertama dapat dilakukan dengan *m* partisipan yang ikut serta pada tahap rekonstruksi rahasia; sedangkan algoritma kedua, dapat mencapai kemampuan yang lebih kuat dari identifikasi kecurangan dengan kolaborasi dari sisa *n*–*m*. Kedua algoritma tersebut efisien dalam hal kemampuan identifikasi kecurangan. Meskipun sebagian besar skema identifikasi kecurangan hanya melibatkan *m* pengguna yang berpartisipasi dalam rekontrukasi rahasia, rasionalistas mengundang *n*–*m* pengguna untuk mengidentifikasi pelaku kecurangan yang dijelaskan oleh Yang *et al*. (2012). Didalam tulisan Liu *et al*. (2018) mereka mengidentifikasi pelaku kecurangan dan juga menggunakan dua share deteksi untuk mengindentifikasi kecurangan. Di sini peneliti menggunakan algoritma pertama untuk mengindentifikasi pelaku kecurangan dengan satu *share* deteksi kecurangan

METODE

Pada penelitian ini akan dibahas mekanisme skema pembagian rahasia berbasis skema Shamir serta kemampuan dalam mengidentifikasi menggunakan Polinomial Bivariat Simetris dengan satu *share* deteksi terhadap pelaku kecurangan pada rekonstruksi suatu rahasia. Adapun langkah-langkah dalam menyelesaikan penelitian ini yaitu:



Gambar 3.1 Kerangka Pikir Penelitian

HASIL DAN PEMBAHASAN

1. Skema Shamir (*k, n*)

Pada bab sebelumnya telah dibahas mengenai tahap pembagian rahasia dan tahap rekonstruksi rahasia dari skema shamir *(k, n*) serta sifat-sifatnya. Sehingga pada bagian ini atau pada Bab ini akan diberikan ilustrasi pada kedua tahap dalam skema shamir (*k, n*).

2. Sifat-Sifat Skema Shamir (*k, n*)

Terdapat beberapa sifat dalam skema pembagian rahasia antara lain yaitu:

1. *Perfect*
   Sebarang $k-1$ atau kurang dari $k-1$ keping rahasia tidak dapat memberikan informasi tentang rahasia *s*.
2. *Minimal*
   Ukuran masing-masing setiap bagian keping rahasia s_i tidak melebihi ukuran data asli dari *s*.
3. *Dynamic*
   Keping-keping s_i yang sudah ada, dapat diubah tanpa mengubah rahasia S dengan cara mengubah polinomial yang digunakan.
4. *Extendable*
   Ketika nilai ambang batas dipertahankan maka ukuran masing-masing keping rahasia s_i dapat dihapus atau ditambahkan tanpa mempengaruhi keping-keping rahasia yang lainnya.
5. *Flexible*
   Dalam skema ini jumlah keping rahasia yang didistribusikan kepada setiap pengguna yang berada di tingkat atas dapat berbeda dengan pengguna yang berada ditingkat bawah.

3. Kelemahan Skema Shamir (*k, n*)

Meskipun dalam skema pembagian rahasia terdapat sifat yang *Perfect, Minimal, Dynamic, Extendable,* serta *Flexible* namum pada skema pembagian rahasia juga memiliki kelemahan yaitu:

1. Tidak aman melawan kecurangan
2. *Dealer* diberikan kepercayaan penuh

4. Skema Deteksi dan Identifikasi Yang Diajukan

Pada beberapa bagian skema baik itu skema shamir, dimana mereka menggunakan polinomial dengan satu variabel untuk memjaga suatu rahasia. Polinomial Bivariat $F(x,y)$ juga merupakan alat dasar untuk membangun skema pembagian rahasia fungsional seperti skema yang dapat diverifikasi, dimana semua pengguna dapat memverifikasi kebenaran sebelum rahasia direkonstruksi.Berikut ini diberikan Algoritma Skema Deteksi dan Identifikasi Dengan Menggunakan Polinomial Bivariat Simetris:

Algoritma Skema Pembagian Rahasia.

1. Tahap Pembagian Keping Rahasia
   a) *Input*: rahasia *s*
   b) *Dealer D* memilih Polinomial Bivariat Simetris $F(x,y)$ berderajat $k-1$;

$$F(x,y) = a_{0,0} + a_{1,0}x + a_{1,1}xy + a_{2,0}x^2 + a_{0,2}y^2 + a_{1,2}x^2y + a_{2,1}x^2y + a_{2,2}x^2y^2 + \cdots + a_{k-1,k-2}x^{k-1}y^{k-2} + a_{k-2,k-1}x^{k-2}y^{k-1} + a_{k-1,k-1}x^{k-1}y^{k-1}$$

   Rahasia s disembunyikan dalam suku konstan dengan $s = F(0,0)$. (q adalah bilangan prima yang bergantung pada ukuran rahasia *s* atau jumlah *n* pengguna).
   c) *Dealer D* menghitung n bagian polinomial dua variabel $f_i(y) = F(i,y), i = 1,2,\cdots,n,$ dan mengirimkan setiap bagian polinomial $f_i(y)$ untuk pengguna P_i

2. Tahap Rekontruksi Rahasia

Misalkan $m \geq k$ pengguna (misalnya $P_1, P_2, \cdots, P_m$) berpartisipasi dalam tahap ini. Algoritma Deteksi dan Identifikasi Kecurangan (Liu *et al*., 2018) yaitu:

a. Semua m pengguna memilih satu bilangan bulat acak misalkan, $d_1 > n$. Setiap pengguna $P_i, i \in [1,m]$ menghitung secret share $v_i = f_i(0)$ dan satu *share* deteksi yaitu $e_i = f_i(d)$

b. Semua m pengguna memperlihatkan secret *share* dan satu share deteksi bersamaan. Menghitung polinomial terinterpolasi $g_0(x)$ dan $h_d(x)$ dalam $\{v_1, v_2, \dots, v_m\}$
   - Jika tiga polinomial $h_d(x), g_0(x)$ berderajat k – 1 dan $h_d(0) = g_0(d)$ maka rahasianya adalah $s = g_0(0)$,, output (s, n).
   - Selainnya itu ada kecurangan

c. Semua m pengguna mempublikasikan pembagian polinomial mereka $f_i(y), i = 1,2, \cdots, m$ yang memenuhi $f_i(d) = e_i, f_i(0) = v_i,\ i = 1,2, \cdots, m$.. (pengguna yang bagian polinomialnya tidak konsisten dengan bagian rahasianya dan satu bagian deteksi yang dipublikasikan pada Langkah 2 akan diidentifikasi sebagai penipu) semua m pengguna ini memilih satu sama lain menggunakan aturan sebagai berikut:
   - Jika $f_i(j) = f_j(i), P_i$dan $P_j$suara untuk satu sama lain;
   - Jika $f_i(j) \neq f_j(i), P_i$ dan $P_j$tidak saling memilih.

Untuk lebih jelas maka akan diberikan simulasi dari algoritma skema deteksi dan identifikasi menggunakan Polinomial Bivariat Simatris dengan satu *shares* deteksi:
Misalkan diberikan skema ambang batas (3, 5) dengan $k = 3, n = 5$, dimana $n = 2k - 1$

1. Tahap Pembagian Keping Rahasia
   a. Pilih bilangan prima $q = 1171$
   b. *Dealer D* memilih Polinomial Bivariat Simetris $F = (x, y)$ berderajat $k - 1$.
   $$F(x, y) = 5 + 3x + x^2 + 3y + 6xy + x^2y + y^2 + xy^2 + 2x^2y^2$$
   c. *Dealer D* menghitung n bagian Polinomial $F(i, y) = f_i(y), i = 1,2, \dots, n$ dan mengirimkan setiap polinomial $f_i(y)$untuk pengguna P_i diman $P_i : f_i(y) \bmod q$ sehingga diperoleh nilai sebagai berikut:
   $$P_1 : f_1(y) = 9 + 10y + 4y^2$$
   $$P_2 : f_2(y) = 15 + 19y + 11y^2$$
   $$P_3 : f_3(y) = 23 + 30y + 22y^2$$
   $$P_4 : f_4(y) = 33 + 43y + 37y^2$$
   $$P_5 : f_5(y) = 45 + 58y + 56y^2$$

2. Tahap Rekontruksi Rahasia
   a. Sebarang $m = 4$ partisipan misalkan P_1, P_2, P_4, P_5 dan memilih bilangan bulat $d = 6$, sehingga diperoleh:
      1. $v_i = f_i(0) \bmod q,\quad i \in [1, m]$ didapat :
      $$v_1 = f_1(0) = [9 + 10(0) + 4(0)^2] \bmod 1171 = 9$$
      $$v_2 = f_2(0) = [15 + 19(0) + 11(0)^2] \bmod 1171 = 15$$
      $$v_4 = f_4(0) = [33 + 43(0) + 37(0)^2] \bmod 1171 = 33$$
      $$v_5 = f_5(0) = [45 + 58(0) + 56(0)^2] \bmod 1171 = 45$$

      2. $e_i = f_i(d) \bmod q,\quad i \in [1, m]$ didapat:
      $$e_1 = f_1(6) = [9 + 10(6) + 4(6)^2] \bmod 1171 = 213$$
      $$e_2 = f_2(6) = [15 + 19(6) + 11(6)^2] \bmod 1171 = 525$$

$$e_4 = f_4(6) = [33 + 43(6) + 37(6)^2] \bmod 1171$$
$$= 452$$
$$e_5 = f_5(6) = [45 + 58(6) + 56(6)^2] \bmod 37$$
$$= 67$$

b. Menghitung polynomial interpolasi lagrange.

1. Menghitung $g_0(x)$ dengan $g_0(x)$ adalah polinomial interpolasi lagrange dalam $(v_1, v_2, \dots, v_m)$ sebagai berikut:

   $g_0(x) = \sum_{i=1}^{m} v_i \prod_{i \neq m}^{m} \left(\frac{x - x_j}{x_i - x_j}\right) \bmod q, \quad (0 \leq i \leq j)$

   Sehingga diperoleh nilai dari $g_0(x)$ adalah:

   $g_0(x) = \sum_{i=1}^{4} v_i \left(\prod_{m \neq 1, m=1}^{4} \frac{x - x_m}{x_i - x_m}\right) \bmod 1171$

   $= \left\{9\left(\frac{x-2}{1-2}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right) + 15\left(\frac{x-1}{2-1}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right) + 33\left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)\left(\frac{x-5}{4-5}\right) + 45\left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)\left(\frac{x-4}{5-4}\right)\right\} \bmod 1171$

   $g_0(x) = \{(1)x^2 + (3)x + 5\} \bmod 1171$
   $= x^2 + 3x + 5$

2. Menghitung $h_d(x)$ dengan $h_d(x)$ adalah polinomial interpolasi lagrange dalam $(e_1, e_2, \dots, e_m)$ sebagai berikut:

   $h_d(x) = \sum_{i=1}^{4} e_i \left(\prod_{m \neq 1, m=1}^{4} \frac{x - x_m}{x_i - x_m}\right) \bmod 1171$

   $= \left\{213\left(\frac{x-2}{1-2}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right) + 525\left(\frac{x-1}{2-1}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right) + 452\left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)\left(\frac{x-5}{4-5}\right) + 67\left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)\left(\frac{x-4}{5-4}\right)\right\} \bmod 1171$

   $h_d(x) = \left\{\left(-\frac{697}{6}\right)x^2 + \left(\frac{1321}{2}\right)x - \left(\frac{994}{3}\right)\right\} \bmod 1171$
   $= 79x^2 + 75x + 59$

c. Karena dua polinomial $h_d(x), g_0(x)$ berderajat $k - 1$ maka kita akan tentukan rahasia s nya dengan $g_0(d) = h_d(0)$, seingga diperoleh nilai rahasianya sebagai berikut:

1. $g_0(d)$ mod q:

   $g_0(x) = (x^2 + 3x + 5) \bmod 1171$
   $g_0(d) = (6d^2 + 3d + 5) \bmod 1171$
   $g_0(6) = ((6)^2 + 3(6) + 5) \bmod 1171$
   =59 mod 1171
   =59

2. $h_0(d)$ mod q:

   $h_d(x) = 79x^2 + 75x + 59$
   $h_d(x) = [79x^2 + 75x + 59]$
   $h_d(0) = [79(0)^2 + 75(0) + 59]$
   =59

Karena $h_d(0) = g_0(x) = 59$ dan rahasia $s = g(0) = 59$ maka tidak ada kecurangan.

3. Tahap Deteksi Menggunakan Skema Yang Diajukan

Pada tahap deteksi ini akan dijelaskan metode dalam mendeteksi pelaku kecurangan menggunakan Polinomial Bivariat Simetris dengan menggunakan satu *shares* deteksi. Misalkan pelaku kecurangan p_i membagikan rahasia palsu terhadap v_4^* dengan nilai $v_4^* = 11$ sehingga polinomial interpolasinya yaitu:

Menghitung $g_0(x)$ dengan $g_0(x)$ merupakan polinomial interpolasi lagrange dalam $(v_1, v_2, \dots, v_m)$ sebagai berikut:

$$g_0(x) = \sum_{i=1}^{4} v_i \left(\prod_{m\neq i, m=1}^{4} \frac{x-x_m}{x_i-x_m}\right) \bmod 1171$$

$$= \left\{9\left(\frac{x-2}{1-2}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right) + 15\left(\frac{x-1}{2-1}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right) + 33\left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)\left(\frac{x-5}{4-5}\right) + 11\left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)\left(\frac{x-4}{5-4}\right)\right\} \bmod 1171$$

$$g_0(x) = \left\{\left(-\frac{17}{6}\right)x^3 + \left(\frac{125}{6}\right)x^2 - \left(\frac{110}{3}\right)x + \left(\frac{83}{3}\right)\right\} \bmod 1171$$

$$= 973x^3 + 216x^2 + 744x + 414$$

Karena polinomial dari $g_0(x)$ tidak berderajat $k-1$ dan juga nilai rahasia $h_d(0) \neq g_0(d)$ sudah pasti ada yang melakukan kecurangan.

4. Tahap Identifikasi Menggunakan Skema Yang Diajukan

Berikut akan dijelaskan cara untuk mengidentifikasi pelaku kecurangan meggunakan Polinomial Bivariat Simetris dengan satu *shares* deteksi. Saat $m = k = 4$ terlibat dalam rekontuksi rahasia.
Maka Tabel identifikasi penipu sebagai berikut:

Tabel 1. Identifikasi Penipu

	Votes	Dari	Bandingkan dengan $T = \frac{m+k-5}{2}$	Identitas
P_1	$V_1 = 2$	P_2, P_3	$V_1 > T$	Jujur
P_2	$V_2 = 3$	P_1, P_3, P_4	$V_2 > T$	Jujur
P_3	$V_3 = 3$	P_1, P_2, P_4	$V_3 > T$	Jujur
P_4	$V_4 = 1$	P_3	$V_4 < T$	Penipu

Misalkan $P_1, P_2, \dots, P_4$ ikut serta dalam rahasia rekontruksi dan jumlah penipu P_4 adalah $t = 1$ yang memenuhi $t < \frac{m-k+3}{2} = \frac{4}{2}$. *Dealer* D menetapkan $d = 6$. Penipu P_4 diterbitkan berbagai rahasia palsu $v_4^* = 11$ dan $e_4 = 452$ Kecurangan ini dapat dengan mudah terdeteksi karena $g_0^*(x)$ dari 4 bagian rahasia yang dipublikasikan memiliki darajat yang lebih besar dari pada $k-1$. Dalam proses identifikasi kecurangan, setiap pengguna menerbitkan bagian polinomial mereka, penipu P_4 menerbitkan bagian polinomial palsu $f_4^* = 815 + 342y + 417y^2 + 777y^3$ yang memenuhi persamaan berikut:

$$f_4^*(d) = e_4, f_4^*(0) = v_4^*, f_4^*(1) = f_1(4), f_4^*(2) = f_2(4)$$

Dalam pemungutan suara, penipu P_4 memperoleh 1 suara, sementara pengguna yang jujur mendapatkan setidaknya 2 suara lebih banyak dibandingkan penipu manapun. Jumlah suara curang kurang dari ambang T, $v_i = 1 < \mathrm{T} = \frac{m+k-5}{2}$,, dan setiap pengguna yang jujur mendapatkan lebih dari T suara, oleh karena itu P_4 berasil diidentifikasi sebagai penipu. Hasil dari identifikasi penipu menggunakan skema yang diajukan dapat dilihat pada tabel di atas.

KESIMPULAN DAN SARAN

Polinomial Bivariat $F(x, y)$ juga merupakan alat dasar untuk membangun skema pembagian rahasia fungsional seperti skema yang dapat diverifikasi, dimana semua pengguna dapat memverifikasi

kebenaran sebelum rahasia direkonstruksi. Skema berbagi rahasia berbasis Polinomial Bivariat telah diperluas ke skema kriptografi lainnya, seperti komputasi cloud, rekontruksi rahasia ganda, dan skema berbagi gambar rahasia. Dalam penilitian ini, peneliti juga menggunakan Polinomial Bivariat Simetris untuk mendeteksi dan mengidentifikasi pelaku kecurangan dengan satu share deteksi.

Berdasarkan penelitian ini akan diperoleh Algoritma deteksi dan identifikasi pelaku kecurangan dengan satu *share* deteksi sebagai berikut:

1. Tahap Pembagian Keping Rahasia
   a) *Input*: rahasia *s*
   b) *Dealer D* memilih Polinomial Bivariat Simetris $F(x,y)$ berderajat $k-1$;
   $$F(x,y) = a_{0,0} + a_{1,0}x + a_{1,1}xy + a_{2,0}x^2 + a_{0,2}y^2 + a_{1,2}x^2y + a_{2,1}x^2y + a_{2,2}x^2y^2 + \cdots + a_{k-1,k-2}x^{k-1}y^{k-2} + a_{k-2,k-1}x^{k-2}y^{k-1} + a_{k-1,k-1}x^{k-1}y^{k-1}$$
   Rahasia s disembunyikan dalam suku konstan dengan $s = F(0,0)$. (q adalah bilangan prima yang bergantung pada ukuran rahasia *s* atau jumlah *n* pengguna).
   c) *Dealer D* menghitung n bagian polinomial dua variabel $f_i(y) = F(i,y), i = 1,2,\cdots,n,,$ dan mengirimkan setiap bagian polinomial $f_i(y)$ untuk pengguna P_i

2. Tahap Rekontruksi Rahasia
   Misakan $m \geq k$ pengguna (misalnya $P_1, P_2, \cdots, P_m$) berpartisipasi dalam tahap ini. Algoritma Deteksi dan Identifikasi Kecurangan (Liu *et al*. 2018) yaitu:
   a) Semua *m* pengguna memilih satu bilangan bulat acak misalkan, $d_1 > n$.. Setiap pengguna $P_i, i \in [1,m]$ menghitung *secret share* $v_i = f_i(0)$ dan satu *share deteksi* yaitu $e_i = f_i(d)$.
   b) Semua m pengguna memperlihatkan *secret share* dan satu *share* deteksi bersamaan. Menghitung polinomial terinterpolasi $g_0(x)$ dan $h_d(x)$ dalam $\{v_1, v_2, \ldots, v_m\}$
      - Jika tiga polinomial $h_d(x), g_0(x)$ berderajat $k-1$ dan $h_d(0) = g_0(d)$ maka rahasianya adalah $s = g_0(0),,$ *output* (s, n).
      - Selainnya itu ada kecurangan
   c) Semua m pengguna mempublikasikan pembagian polinomial mereka $f_i(y), i = 1,2,\cdots,m$ yang memenui $f_i(d) = e_i, f_i(0) = v_i,\ i = 1,2,\cdots,m.$ pengguna yang bagian polinomialnya tidak konsisten dengan bagian rahasianya dan satu bagian deteksi yang dipublikasikan pada Langkah2 akan diidentifikasi sebagai penipu) semua m pengguna ini memilih satu sama lain menggunakan aturan sebagai berikut:
      - Jika $f_i(j) = f_j(i), P_i$ dan P_j suara untuk satu sama lain;
      - Jika $f_i(j) \neq f_j(i), P_i$ dan P_j tidak saling memilih.

Berdasarkan penelitian skema pembagian rahasia ini, yang mana dengan menggunakan satu *share* deteksi, Peneliti telah selesai dalam mendeteksi dan mengidentifikasi potensi pelaku kecurangan sehingga pada penelitian ini peneliti berharap dapat bermanfaat bagi pembaca dalam mencari refrensi untuk penelitian-penelitian selanjutnya.

UCAPAN TERIMA KASIH

Pada kesempatan ini maka penulis menyampaikan terima kasih, kepada semua pihak yang telah memberikan motivasi serta semangat dan juga arahan dalam mengerjakan skripsi ini. Tidak lupa juga, penulis mengucapkan terima kasih kepada kedua orang tua yang selalu mendukung dan mendoakan penulis.

REFERENCES

Ahzan, Z. N., Guritman, S., & Silalahi, B. P. (2020). Deteksi dan Identifikasi Pelaku Kecurangan Skema Pembagian Rahasia Linear Berbasis Skema Shamir. Jurnal Karya Pendidikan Matematika Universitas Muhammadiyah Semarang, 27–41.

Barbeau, E. . (2003). Polynomials. Springer- Verlag.

Blakley, G. R. (1979). Safeuardin cryptoraphic keys. National Computer Conference.

Cheney, W., & Kincaid, D. (2008). Numerical Mathematics And Computing (6th ed.).

Harn, L., & Lin, C. (2009). Detection and identification of cheaters in (t, n) secret sharing scheme. Designs, Codes, and Cryptography, 52(1), 15–24.

Liu, Y., Yang, C., Wang, Y., Zhu, L., & Ji, W. (2018). Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. Information Sciences, 453, 21–29.

Menezes, A. J., Oorschot, P. C. Van, & Vanstone, S. A. (1996). Handbook Of Applied Cryptoraphy. CRC Press.

Sukirman. (2006). Penantar Teori Bilangan. Hanggar Kreator : yoyakarta.

Surianty, S. (2017). Teori Grup (Struktur Aljabar 1). UGM Press.

Wu, S., Hsu, C., Xia, Z., Zhang, J., & Wu, D. (2020). Symmetric-bivariate-polynomial-based lightweight authenticated group key agreement for industrial internet of things. Journal of Internet Technology, 21(7), 1969–1979.