Deteksi dan Identifikasi Pelaku Kecurangan Skema Pembagian Rahasia Linear Berbasis Skema Shamir

Oleh: Zulkaidah Nur Ahzan[(1)], Sugi Guritman[(3)], Bib Paruhum Silalahi[(3)]
nurahzanz1208@gmail.com[(1)], sugigu@apps.ipb.ac.id[(2)]
universitas timor[(1)], institut pertanian bogor[(2,3)]

Article history
Submission : 9/2/2020
Revised : 27/2/2020
Accepted : 30/3/2020

Keywords:
Cryptography, Linear Secret Sharing Scheme, Secret Sharing Scheme

Abstract

The method that can be used to maintain security of secret in the form of cryptographic keys is by using secret sharing scheme (SSS). This method is first proposed by Adi Shamir in 1979, where the proposed scheme is a (k, n) threshold scheme. Shamir scheme is a perfect scheme under the assumption that all shareholders present their original share. However, if there are dishonest shareholders who present faked shares then the honest shareholders get nothing but a faked secret. Secret sharing scheme based on linear scheme is a scheme that can detect and identify cheaters who submit faked shares at the secret reconstruction. Detectability of this scheme when $m \geq k$ *and identifiability when* $m - c \geq k$ *under the assumption that all shareholders present their shares randomly. After conducting a security analysis of the proposed scheme, it is obtained that to succeed in attack with cheaters who work together to fool honest shareholders then a new polynomial* $g(x)$ *such that* $g(1) = s_1$, $g(2) = s_2$, ..., $g(k - 1) = s_{k-1}$ *and a new detector that has the same value as detector d are needed.*

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. Metode ini boleh dikatakan metode yang efektif untuk menjaga keamanan suatu rahasia karena jika rahasia hanya diketahui oleh satu orang saja maka kemungkinan besar rahasia tersebut akan bocor. Sedangkan dengan menggunakan metode SPR suatu rahasia tidak akan mudah bocor karena

harus memenuhi kriteria tertentu yaitu jumlah minimum pemegang keping rahasia yang akan merekonstruksi rahasia. Metode ini telah dilakukan pada kasus pembukaan brankas bank atau peluncuran misil nuklir.

Skema pembagian rahasia pertama kali diperkenalkan oleh Shamir (1979 : 612) dan Blakley (1979 : 316). Skema yang diperkenalkan oleh Shamir adalah SPR-(k, n) dimana suatu rahasia akan dibagi menjadi n keping rahasia dan untuk merekonstruksi rahasia tersebut dibutuhkan sekurang-kurangnya k pemegang keping rahasia. Namun, SPR-(k, n) Shamir belum sempurna karena tidak memperhitungkan kemungkinan jika ada pemegang keping rahasia yang melakukan kecurangan dengan memberikan keping rahasia yang salah.

Harn dan Lin (2009 : 19) mengajukan skema yang dapat mendeteksi dan mengidentifikasi pelaku kecurangan dengan pemulihan rahasia dilakukan melalui pendekatan polinomial yaitu interpolasi Lagrange, serta jumlah pemegang keping rahasia yang berpartisipasi pada tahap rekonstruksi rahasia minimal sebanyak $k + 1$ partisipan. Yanxiao Liu (2016 : 2118) mengajukan skema linear (k, n), namun skema yang diajukan hanya merupakan skema untuk mendeteksi kecurangan. Liu, Yang, Wang, Zhu, dan Ji (2018 : 23) mengajukan skema yang berbasis polinomial bivariat simetrik, namun skema yang diajukan menggunakan dua parameter deteksi pada tahap rekonstruksi rahasia dan skema yang diajukan juga membangkitkan polinomial hasil interpolasi Lagrange untuk mendeteksi pelaku kecurangan. Pemulihan rahasia dengan melakukan interpolasi Lagrange menjadikan komputasi kurang efisien, seperti pada skema Harn dan Lin (2009 : 19) yang membutuhkan perulangan dalam pemulihan rahasianya sebanyak kombinasi pemegang keping rahasia dengan membangkitkan polinomial hasil interpolasi Lagrange; semakin banyak jumlah pemegang keping rahasianya maka semakin banyak pula kombinasi pemegang keping rahasianya. Beberapa skema sebelumnya juga belum mampu melawan kecurangan dengan jumlah minimal pemegang keping rahasia adalah sebanyak k partisipan, sedangkan dalam tahap pemulihan rahasia ada kalanya pemegang keping rahasia bisa saja sebesar ambang batasnya, yaitu sebanyak k partisipan. Kemudian pada skema Liu, Yang, Wang, Zhu, dan Ji (2018 : 23) melibatkan parameter deteksi lebih dari satu, sedangkan untuk skema tersebut dengan satu parameter deteksi keamanan skema yang diajukan sudah cukup baik. Oleh karenanya kami mengajukan suatu skema yang dapat mengatasi kekurangan-kekurangan pada skema-skema sebelumnya yaitu skema pembagian rahasia linear yang berbasis skema Shamir.

Adapun tujuan dari penelitian ini adalah sebagai berikut: (1) mengonstruksi SPR linear untuk mendeteksi dan mengidentifikasi kecurangan pada SPR Shamir; (2) menghitung batas dari kemampuan deteksi dan identifikasi dari skema yang diusulkan; (3) menganalisis keamanan skema yang diajukan.

Dalam penelitian ini membahas mekanisme skema pembagian rahasia linear berbasis skema Shamir serta kemampuan deteksi dan identifikasi kecurangan dari skema yang diajukan terhadap pelaku kecurangan pada rekonstruksi suatu rahasia. Sebagai tambahan dibahas analisis keamanan dari skema yang diajukan.

Kajian Teori

Sistem Persamaan Linear

Suatu persamaan dengan n variabel $x_1, x_2, \ldots, x_n$ dikatakan linear jika dapat dituliskan sebagai:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \quad (1)$$

dimana $a_1, a_2, \ldots, a_n,$ dan b adalah suatu bilangan konstan. Adapun variabel yang dimaksud di sini bukan merupakan fungsi trigonometri, eksponensial, akar, pangkat, dan tidak melibatkan perkalian atau pembagian dengan variabel lain.

Sistem persamaan linear (SPL) adalah koleksi berhingga dari persamaan-persamaan linear. Bentuk umum SPL dengan m persamaan dan n variabel adalah :

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned} \quad (2)$$

dimana a_{ij} dan $b_{ij}, i = 1, 2, \ldots, m\,;\, j = 1, 2, \ldots, n,$ adalah bilangan konstan; sedangkan $x_j, j = 1, 2, \ldots, n,$ adalah variabel (Anton dan Rorres 2010).

Selanjutnya bentuk SPL (2) dapat dituliskan ke dalam bentuk matriks sebagai berikut :

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \quad (3)$$

Jika dimisalkan $\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$, $= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, dan $\boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$ maka (3) dapat dituliskan ke dalam bentuk persamaan : $\boldsymbol{AX} = \boldsymbol{b}$. Masing-masing matriks, $\boldsymbol{A}$ berukuran $m \times n$, $\boldsymbol{X}$ berukuran $m \times 1$, dan $\boldsymbol{b}$ juga berukuran $m \times 1$.

Bentuk (3) dapat dituliskan dengan lebih efisien, yaitu seperti berikut:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right) \quad (4)$$

Selanjutnya bentuk (4) disebut matriks gandeng (*augmented matrix*), yang dinotasikan $(\boldsymbol{A}|\boldsymbol{b})$ (Anton dan Rorres, 2010).

Penyelesaian Suatu Sistem Persamaan Linear

Penyelesaian dari suatu SPL *n* variabel adalah bilangan-bilangan yang memenuhi :

$$x_1 = r_1, x_2 = r_2, \ldots, x_n = r_n \quad (5)$$

dimana bilangan-bilangan tersebut harus memenuhi semua persamaan linear dalam SPL tersebut.

Ada 3 (tiga) jenis penyelesaian dari suatu SPL, yaitu :

(i) SPL yang tidak memiliki penyelesaian
(ii) SPL yang memiliki tepat satu penyelesaian, atau penyelesaian tunggal
(iii) SPL yang memiliki tak berhingga penyelesaian atau banyak penyelesaian

SPL yang sekurang-kurangnya memiliki satu penyelesaian disebut SPL yang konsisten, sedangkan SPL yang tidak memiliki penyelesaian disebut SPL yang tak konsisten.

Suatu SPL $\boldsymbol{AX} = \boldsymbol{b}$, dengan matriks $\boldsymbol{A}$ berukuran $m \times n$, konsisten jika dan hanya jika rank matriks $\boldsymbol{A}$ sama dengan rank matriks diperbesarnya. Dengan kata lain, $r(\boldsymbol{A}) = r(\boldsymbol{A}|\boldsymbol{b})$. Dan ketika SPL konsisten, maka :

1. Jika $r(\boldsymbol{A}) = n$ maka, SPL memiliki tepat satu solusi (penyelesaian).
2. Jika $r(\boldsymbol{A}) < n$ maka SPL memiliki banyak solusi (Anton dan Rorres, 2010).

Definisi Rank

Dimensi yang sama antara ruang baris dan ruang kolom dari suatu matriks, disebut rank dari matriks tersebut (Anton dan Rorres, 2010). Sederhananya, rank dari suatu matriks adalah ukuran terbesar dari sub matriks tersebut yang determinannya tidak nol.

Definisi Bebas Linear

Misalkan *V* ruang vektor, $B = \{\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots, \boldsymbol{b_n}\} \subseteq V$. Himpunan *B* dikatakan bebas linear, jika persamaan :

$$c_1\boldsymbol{b_1} + c_2\boldsymbol{b_2} + \ldots + c_n\boldsymbol{b_n} = \boldsymbol{0} \quad (6)$$

hanya terpenuhi dengan $c_1 = c_2 = \ldots = c_n = 0$ (Anton dan Rorres, 2010).

Teorema Dasar Aljabar

Suatu polinomial berderajat *k* memiliki paling banyak *k* akar yang berbeda (Shah, 2012 : 300).

Definisi Polinomial

Polinomial adalah suatu ekspresi matematis yang terdiri dari jumlah pangkat dari satu atau lebih variabel (disebut juga *indeterminate*) yang dikalikan dengan koefisien. Bentuk umum dari suatu polinomial dengan *indeterminate x* tunggal adalah :

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$$

dengan $a_0, a_1, \ldots, a_n$ adalah bilangan konstan dan *x* adalah *indeterminate* (Barbeau, 2003 : 1).

Derajat Suatu Polinomial

Derajat suatu polinomial adalah pangkat tertinggi dari semua koefisien yang tak nol (Barbeau, 2003 : 1).

Definisi Fungsi Polinomial

Fungsi polinomial adalah suatu fungsi yang didefinisikan dengan menghitung nilai suatu polinomial (Leung, Mok, & Suen, 1992 : 4).

Polinomial Nol

Polinomial nol adalah suatu polinomial yang semua koefisiennya adalah nol dan berderajat $-\infty$. Polinomial nol memiliki akar yang tak terhingga banyaknya (Barbeau, 2003 : 2).

Definisi Interpolasi

Interpolasi adalah suatu proses yang dilakukan untuk mencari dan menghitung nilai suatu fungsi yang grafiknya melalui sekumpulan titik-titik yang diberikan (Cheney & Kincaid, 2008 : 125).

Interpolasi Lagrange

Interpolasi Lagrange adalah salah satu metode menginterpolasi suatu fungsi $f(x)$ pada titik-titik $x_0, x_1, x_2, \ldots, x_n$ yang bertujuan untuk mendapatkan polinomial berderajat n dengan menggunakan bentuk Lagrange, yaitu:

$$L_n(x) = \sum_{i=0}^{n} l_i(x) f(x_i) \quad (7)$$

dengan,

$$l_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \left(\frac{x - x_j}{x_i - x_j} \right) \quad (0 \leq i \leq n) \quad (8)$$

(Cheney & Kincaid, 2008 : 126).

Definisi Membagi

Misalkan a dan b adalah bilangan bulat. Bilangan a dikatakan membagi b atau $a|b$ jika terdapat bilangan bulat c sedemikian sehingga $b = ac$ (Menezes, Oorschot, & Vanstone, 1996 : 63).

Definisi Kongruen

Misalkan $n \geq 0$, $a, b,$ dan n adalah bilangan bulat. Bilangan a dikatakan kongruen terhadap b modulo n atau $a \equiv b \bmod n$, jika n membagi $a - b$ (Menezes, Oorschot, & Vanstone, 1996 : 67).

Definisi Kelas Ekuivalensi

Misalkan $n \geq 0$, a dan n adalah bilangan bulat. Kelas ekuivalensi dari suatu bilangan bulat a adalah himpunan semua bilangan bulat yang kongruen terhadap a modulo n (Menezes, Oorschot, & Vanstone, 1996 : 68).

Definisi Bilangan Bulat Modulo n

Bilangan bulat modulo n atau $\mathbb{Z}_n$, adalah himpunan kelas ekuivalensi dari bilangan-bilangan bulat $\{0, 1, 2, \ldots, n - 1\}$ dimana operasi penjumlahan, pengurangan, dan perkalian dilakukan pada modulo n (Menezes, Oorschot, & Vanstone, 1996 : 68).

Definisi Operasi Biner

Operasi biner $*$ pada himpunan tak kosong A adalah pemetaan dari $A \times A$ ke A (Menezes, Oorschot, & Vanstone, 1996 : 75).

Definisi Grup Komutatif

Suatu grup $(G, *)$ adalah suatu himpunan tak kosong G dengan operasi biner $*$ pada G yang memenuhi aksioma-aksioma berikut :

(i) Operasi $*$ pada grup bersifat asosiatif, yaitu $a * (b * c) = (a * b) * c$ untuk setiap $a, b, c \in G$.

(ii) Terdapat unsur identitas, misalkan $d \in G$, sedemikian sehingga $a * d = d * a = a$ untuk setiap $a \in G$.

(iii) Untuk setiap $a \in G$ terdapat $a^{-1} \in G$, sedemikian sehingga $a * a^{-1} = a^{-1} * a = d$, dimana a^{-1} adalah invers dari a.

Suatu grup dikatakan komutatif jika $a * b = b * a$ untuk setiap $a, b \in G$ (Menezes, Oorschot, & Vanstone, 1996 : 75).

Definisi Ring Komutatif

Suatu ring $(R, +, \times)$ adalah suatu himpunan tak kosong R dengan dua operasi biner yaitu penjumlahan $(+)$ dan perkalian $(\times)$ pada R, yang memenuhi aksioma-aksioma berikut :

(i) $(R, +)$ adalah suatu grup komutatif yang identitasnya adalah 0.

(ii) Operasi $\times$ bersifat asosiatif, yaitu $a \times (b \times c) = (a \times b) \times c$, untuk setiap $a, b, c \in R$.

(iii) Terdapat identitas terhadap perkalian, misalkan $e \neq 0$, sedemikian sehingga $a \times e = e \times a = a$ untuk setiap $a \in R$.

(iv) Operasi $\times$ bersifat distributif terhadap penjumlahan $(+)$, yaitu $a \times (b + c) = (a \times b) + (a \times c)$ dan $(a + b) \times c = (a \times c) + (b \times c)$ untuk setiap $a, b, c \in R$.

Suatu ring dikatakan komutatif jika pada operasi perkalian $(\times)$ terpenuhi sifat komutatifnya, yaitu $a \times b = b \times a$ untuk setiap $a, b \in R$ (Menezes, Oorschot, & Vanstone, 1996 : 77).

Definisi Lapangan

Lapangan adalah suatu ring komutatif dengan semua elemen tak-nolnya memiliki invers terhadap perkalian (Menezes, Oorschot, & Vanstone, 1996 : 77).

Definisi Polinomial Atas Lapangan F

Misalkan $(F, +, \times)$ adalah lapangan. Polinomial atas F adalah suatu persamaan dalam bentuk $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ dimana $a_0, a_1, a_2, \ldots, a_n \in F$ (Menezes, Oorschot, & Vanstone, 1996, 1996 : 78).

Definisi Kriptografi

Kriptografi adalah studi mengenai teknik atau metode dalam matematika yang terkait dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data (Menezes, Oorschot, & Vanstone, 1996 : 4).

Definisi Skema Pembagian Rahasia

Skema pembagian rahasia adalah protokol multi-partisipan yang berkaitan dengan pembentukan kunci, dalam hal ini kunci kriptografik (Menezes, Oorschot, & Vanstone, 1996 : 524).

Skema Ambang Batas

Suatu skema ambang batas (k, n) dengan $k \leq n$ adalah suatu metode dalam skema pembagian rahasia dimana seorang pihak terpercaya menghitung keping rahasia $s_i\ (1 \leq i \leq n)$ yang berasal dari rahasia awal s, dan mendistribusikan setiap s_i ke pengguna P_i secara aman sedemikian sehingga : sebarang k atau lebih dari k pengguna yang menggabungkan keping rahasianya dengan mudah dapat memulihkan rahasia s, sedangkan sebarang $k - 1$ atau kurang tidak dapat memulihkan rahasia s (Menezes, Oorschot, & Vanstone, 1996 : 525).

Skema-(k,n) Shamir

Tahap pembagian keping rahasia pada skema Shamir (1979) adalah sebagai berikut :

a. *Dealer* D memilih suatu bilangan prima $p >$ max (s, n), dengan rahasia $s = a_0$.
b. *Dealer* D memilih polinomial acak atas $\mathbb{Z}_p$, yaitu $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$, dengan $0 \leq a_j < p$; $j = 0, 1, 2, \ldots, k - 1$.
c. *Dealer* D menghitung n keping rahasia $s_i = f(i) \bmod p$, $i = 1,2,\ldots,n$ dan mendistribusikan tiap-tiap keping rahasia s_i ke partisipan P_i.

Tahap rekonstruksi rahasia dari skema Shamir adalah :

a. Sebarang m partisipan $(k \leq m \leq n)$, misalkan $P_{i_1},P_{i_2},\ldots,P_{i_m}$, menyatukan keping-keping rahasia $s_{i_1}, s_{i_2},\ldots, s_{i_m}$ bersama-sama. Dengan $\{i_1, i_2,\ldots, i_m\} \subset \{1, 2, \ldots, n\}$.
b. Menghitung polinomial interpolasi Lagrange$f(x)$ dari m titik-titik $(i_1,s_{i_1}),(i_2,s_{i_2}),\ldots,(i_m,s_{i_m})$, yaitu $f(x) = \sum_{i=1}^{m} l_i(x)y_i \bmod p$ dengan $l_i(x) = \prod_{t \neq i,\ t=1}^{m} \left(\frac{x - x_t}{x_i - x_t}\right)$ $(1 \leq i \leq m)$ dan y_i adalah nilai dari masing dari masing-masing keping rahasia yaitu $s_{i_1}, s_{i_2}, \ldots, s_{i_m}$. Nilai rahasia adalah $s = f(0)$.

Skema Pembagian Rahasia Linear

Definisi: SPR linear (k, n) adalah SPR dimana n keping rahasia $s_1, s_2, \ldots, s_n$ dapat dituliskan sebagai berikut.

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \boldsymbol{H} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_k \end{pmatrix}$$

$\boldsymbol{H}$ adalah matriks berukuran $n \times k$ yang diketahui oleh publik dan semua submatriksnya yang berukuran $k \times k$ bersifat bebas linear.

Skema Harn dan Lin

Harn dan Lin (2009) mengajukan SPR yang terdiri dari algoritme pembangkitan keping rahasia dan algoritme rekonstruksi rahasia.

Algoritme pembangkitan keping rahasianya sama dengan skema Shamir, sedangkan algoritme rekonstruksi rahasianya terbagi dua yaitu algoritme deteksi kecurangan dan algoritme identifikasi kecurangan.

Algoritme deteksi kecurangan dari skema ini adalah :

Input: $k, n, J, s_{i_1}, s_{i_2},\ldots, s_{i_j}$.($J$ = semua partisipan pada tahap rekonstruksi rahasia)
1. Menghitung polinomial interpolasi $f(x)$ dari j titik $(i_1,s_{i_1}),(i_2,s_{i_2}),\ldots,(i_j,s_{i_j})$. Misalkan derajat dari $f(x)$ adalah d.
2. Jika $d = k$ -1, maka $s = f(0)$ dan

Output:Tidak ada kecurangan dan rahasianya adalah s; selainnya

Output:Ada kecurangan

Algoritme identifikasi kecurangannya adalah sebagai berikut :

Input: $k, n, s, J, T, s_{i_1}, s_{i_2},\ldots, s_{i_j}$

dimana $T = \{T_1, T_2,\ldots, T_u\}$ = semua subset dengan t partisipan dari J dan $u = \binom{j}{k}$.

1. Menghitung $s^i = \mathrm{F}(T_i)$, $\forall T_i \in T$, $i = 1,2,\ldots,u$
2. Membagi $U = \{s^1, s^2,\ldots, s^u\}$menjadi v subset $U_i \ni U = U_1 \cup \ldots \cup U_v$ dimana $U_t \cap U_l = \emptyset$, untuk $l \leq t, l \leq v$ dan $t \neq l$, dan $U_i = \{s^{i_1},s^{i_2},\ldots,s^{i_{w_i}}\}$ dimana $s^{w_i} = s^{i_1} = s^{i_2} = \ldots = s^{i_{w_i}}$
3. Misalkan $w_z = \max_i\{w_i\}$, dan misalkan $s = s^{w_z}$
4. Mengambil $T_t \in T \ni s = F(T_t) = F_{T_t}\left(s_{i_{t_1}},s_{i_{t_2}},\ldots,s_{i_{t_k}}\right)$, dan misalkan $R = J - \{i_{t_1}, i_{t_2},\ldots, i_{t_k}\}$
5. Mengambil $i_r \in R$ secara berurut dan hapus dari R, dan menghitung $s^r = F\left(s_{i_r},s_{i_{t_2}},\ldots,s_{i_{t_k}}\right)$
6. Jika $s^r = s$, simpan i_r di H; selainnya simpan i_r di C
7. Mengulangi langkah 5 sampai $R = \emptyset$

Output: Himpunan *cheater* adalah C

Skema Yanxiao Liu

Yanxiao Liu (2016) mengajukan skema yang terdiri dari tahap pembangkitan keping rahasia dan tahap rekonstruksi rahasia. Pembangkitan keping rahasia dari skema ini adalah :

Input : rahasia $s \in \mathbb{Z}_p$ dengan p adalah bilangan prima

1. *Dealer* D menetapkan suatu polinomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$; $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}_p$ sedemikian sehingga $a_0 = s$.
2. *Dealer* D menetapkan suatu bilangan $r \in \mathbb{Z}_p$ dan suatu polinomial $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{k-1}x^{k-1}$; $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}_p$, dengan $ra_0 + b_0 = 0$ dan $ra_1 + b_1 = 0$.
3. *Dealer* D menghitung keping-keping rahasia $s_i = \{m_i, d_i\}$, $i = 1, 2, \ldots, n$; $m_i = f(i)$ dan $d_i = g(i)$, kemudian mendistribusikan tiap keping rahasia kepada masing-masing pemegang keping rahasia P_i.

Output : keping-keping rahasia s_i

Tahap rekonstruksi rahasia dari skema ini adalah sebagai berikut :

Misal ada k pemegang keping rahasia yang terlibat pada tahap ini, yaitu $P_1, P_2, \ldots, P_k$.

Input : keping-keping rahasia s_i, $i = 1, 2, \ldots, k$

1. Merekonstruksi polinomial hasil interpolasi Lagrange, yaitu $f'(x)$ dan $g'(x)$, masing-masing pada titik-titik $(1, m_1), (2, m_2), \ldots, (k, m_k)$ dan $(1, d_1), (2, d_2), \ldots, (k, d_k)$.
2. Misalkan a_0', a_1', b_0' dan b_1' masing-masing adalah koefisien dari x^0 dan x pada $f'(x)$ dan $g'(x)$. Jika terdapat suatu bilangan $r' \in \mathbb{Z}_p$ yang sama dan memenuhi $r'a_0' + b_0' = 0$ dan $r'a_1' + b_1' = 0$, maka *output* yang dihasilkan adalah $s = f'(0)$. Selainnya, $f'(0)$ adalah rahasia palsu dan ada kecurangan, *output* $\perp$.

Skema Liu, Yang, Wang, Zhu, dan Ji

Skema Liu, Yang, Wang, Zhu, dan Ji (2018) merupakan skema polinomial bivariat simetrik, dimana pada tahap pembagian keping-keping rahasia dan rekonstruksi rahasia berdasarkan polinomial bivariat. Skema ini terdiri dari dua algoritme, dimana algoritme pertama dapat dilakukan dengan m partisipan yang ikut serta pada tahap rekonstruksi rahasia; sedangkan algoritme kedua, jika m partisipan dapat mendeteksi kecurangan, maka $n - m$ lainnya yang tidak ikut serta pada tahap rekonstruksi rahasia dapat terlibat untuk mengidentifikasi kecurangan.

Metode Penelitian

Pada penelitian ini akan dibahas mekanisme skema pembagian rahasia linear berbasis skema Shamir serta kemampuan deteksi dan identifikasi kecurangan dari skema yang diajukan terhadap pelaku kecurangan pada rekonstruksi suatu rahasia. Sebagai tambahan dibahas analisis keamanan dari skema yang diajukan. Adapun langkah-langkah yang dilakukan pada penelitian ini adalah :

1. Melakukan studi literatur skema-(k, n) Shamir dan skema linear.
2. Mengonstruksi skema linear berbasis skema Shamir.
3. Mengonstruksi tahap pembagian keping rahasia dari skema yang diajukan.
4. Mengonstruksi tahap rekonstruksi rahasia dari skema yang diajukan.
5. Mendeteksi pelaku kecurangan dengan skema yang diajukan.
6. Mengidentifikasi pelaku kecurangan dengan skema yang diajukan
7. Menghitung batas kemampuan deteksi dari skema yang diajukan.
8. Menganalisis keamanan dari skema yang diajukan.

Hasil Penelitian dan Pembahasan

Skema-(k,n) Shamir

Pada bab sebelumnya telah dibahas mengenai tahap pembagian rahasia dan tahap rekonstruksi rahasia dari skema Shamir serta sifat-sifatnya. Sehingga pada bagian ini akan diilustrasikan kedua tahap tersebut. Ilustrasinya seperti berikut ini :

1. Tahap pembagian rahasia
   a. *Dealer* D memilih bilangan prima p = 800447, dengan $s = a_0$ = 451080, n = 12 dan k = 5.
   b. *Dealer* D memilih polinomial acak atas $\mathbb{Z}_{800447}$, yaitu
   $f(x) = 451080 + 170745x + 78603x^2 + 126954x^3 + 86323x^4$.
   c. *Dealer* D menghitung nilai dari 12 keping rahasia :
   $s_1 = f(1) \bmod 800447 = 113258$;
   $s_2 = f(2) \bmod 800447 = 301994$;
   $s_3 = f(3) \bmod 800447 = 83958$;
   $s_4 = f(4) \bmod 800447 = 597572$;

$s_5 = f(5) \bmod 800447 = 250328$;
$s_6 = f(6) \bmod 800447 = 321917$;
$s_7 = f(7) \bmod 800447 = 161547$;
$s_8 = f(8) \bmod 800447 = 389731$;
$s_9 = f(9) \bmod 800447 = 496946$;
$s_{10} = f(10) \bmod 800447 = 444527$;
$s_{11} = f(11) \bmod 800447 = 664667$;
$s_{12} = f(12) \bmod 800447 = 459523$.

Masing-masing keping rahasia s_i didistribusikan ke partisipan P_i, dengan $i = 1,2,\ldots,12$ sedemikian sehingga ada 12 pasangan terurut, yaitu : {(1,113258), (2,301994), (3,83958), (4,597572), (5,250328), (6,321917), (7,161547), (8,389731), (9,496946), (10,444527), (11,664667), (12,459523)}.

2. Tahap rekonstruksi rahasia
   a. Sebarang $m = 7$ partisipan (pemegang keping rahasia) menyatukan keping rahasianya bersama-sama. Misalkan dipilih partisipan {1, 3, 4, 7, 9, 10, 12} dengan masing-masing nilai keping rahasia $s_{i_1} = s_1 = 113258$; $s_{i_2} = s_3 = 83958$; $s_{i_3} = s_4 = 597572$; $s_{i_4} = s_7 = 161547$; $s_{i_5} = s_9 = 496946$; $s_{i_6} = s_{10} = 444527$; $s_{i_7} = s_{12} = 459523$. Sehingga diperoleh himpunan pasangan terurut (x_i, y_i): {(1,113258), (3,83958), (4,597572), (7,161547), (9,496946), (10,444527), (12,459523)}.
   b. Menghitung polinomial interpolasi Lagrange $f(x) = \sum_{i=1}^{m} l_i(x) y_i \bmod p$ dengan $l_i(x) = \prod_{t \neq i,\, t=1}^{m} \left(\frac{x - x_t}{x_i - x_t}\right)$ $(1 \le i \le m)$ dan y_i adalah nilai dari masing dari masing-masing keping rahasia yaitu $s_{i_1}, s_{i_2}, \ldots, s_{i_7}$.

$$f(x) = \sum_{i=1}^{7} y_i \left(\prod_{t \neq i,\, t=1}^{7} \frac{x - x_t}{x_i - x_t}\right) \bmod 800447$$

$$= (113258 \left(\frac{x-3}{1-3}\right).\left(\frac{x-4}{1-4}\right).\left(\frac{x-7}{1-7}\right).\left(\frac{x-9}{1-9}\right).\left(\frac{x-10}{1-10}\right).\left(\frac{x-12}{1-12}\right) + 83958.\left(\frac{x-1}{3-1}\right).\left(\frac{x-4}{3-4}\right).\left(\frac{x-7}{3-7}\right).\left(\frac{x-9}{3-9}\right).\left(\frac{x-10}{3-10}\right).\left(\frac{x-12}{3-12}\right) + \cdots + 444527.\left(\frac{x-1}{10-1}\right).\left(\frac{x-3}{10-3}\right).\left(\frac{x-4}{10-4}\right).\left(\frac{x-7}{10-7}\right).\left(\frac{x-9}{10-9}\right).\left(\frac{x-12}{10-12}\right) + 459523.\left(\frac{x-1}{12-1}\right).\left(\frac{x-3}{12-3}\right).\left(\frac{x-4}{12-4}\right).\left(\frac{x-7}{12-7}\right).\left(\frac{x-9}{12-9}\right).\left(\frac{x-10}{12-10}\right)) \bmod 800447$$

Nilai rahasia s adalah :

$$s = f(0) = (113258 \left(\frac{-3}{-2}\right).\left(\frac{-4}{-3}\right).\left(\frac{-7}{-6}\right).\left(\frac{-9}{-8}\right).\left(\frac{-10}{-9}\right).\left(\frac{-12}{-11}\right) + 83958 \left(\frac{-1}{2}\right).\left(\frac{-4}{-1}\right).\left(\frac{-7}{-4}\right).\left(\frac{-9}{-6}\right).\left(\frac{-10}{-7}\right).\left(\frac{-12}{-9}\right) + \ldots + 444527.\left(\frac{-1}{9}\right).\left(\frac{-3}{7}\right).\left(\frac{-4}{6}\right).\left(\frac{-7}{3}\right).\left(\frac{-9}{1}\right).\left(\frac{-12}{-2}\right) + 459523.\left(\frac{-1}{11}\right).\left(\frac{-3}{9}\right).\left(\frac{-4}{8}\right).\left(\frac{-7}{5}\right).\left(\frac{-9}{3}\right).\left(\frac{-10}{2}\right)) \bmod 800447$$

$$s = f(0) = \frac{146800197}{22} \bmod 800447 = 451080.$$

Skema Shamir memiliki sifat-sifat sebagai berikut :

1. *Perfect*.
   Sebarang $k - 1$ atau kurang dari $k - 1$ keping rahasia tidak dapat memberikan informasi tentang rahasia s.
2. *Minimal*
   Ukuran masing-masing keping rahasia tidak akan melebihi ukuran rahasia s.
3. *Extensible*
   Ketika nilai ambang batas dipertahankan maka ukuran masing-masing keping rahasia s_i dapat dihapus atau ditambahkan tanpa memengaruhi keping-keping rahasia yang lain.
4. *Dynamic*
   Keping-keping rahasia s_i dapat diubah tanpa mengubah rahasia s dengan mengubah polinomial yang digunakan.
5. *Flexible*
   Dalam skema ini jumlah keping rahasia yang didistribusikan kepada pengguna yang berada di tingkatan atas dapat berbeda dengan pengguna yang berada di tingkatan bawah. Misalnya seorang insiyur misil nuklir dapat membuka kunci peluncuran misil seorang diri, sedangkan untuk para asistennya diperlukan 3 orang asisten untuk membuka kunci misil tersebut.

Meskipun skema Shamir memiliki sifat yang *perfect*, *minimal*, *extensible*, *dynamic*, serta *flexible* namun skema Shamir juga memiliki kelemahan yaitu :

1. Tidak aman melawan kecurangan.
   Ketika ada pemegang keping rahasia yang berbuat curang dengan memberikan keping rahasia yang palsu, maka rahasia s tidak dapat dipulihkan. Sedangkan kecurangan tersebut tidak diketahui oleh pemegang keping rahasia yang jujur.
2. *Dealer* diberikan kepercayaan penuh.
   Dealer dapat mendistribusikan keping rahasia yang salah kepada para pemegang keping

rahasia. Sedangkan pemegang keping rahasia tidak mengetahui apakah keping rahasia yang diberikan oleh *dealer* adalah benar (valid) atau salah.

Skema Pembagian Rahasia Linear

Pada bab sebelumnya telah dibahas mengenai definisi dari skema pembagian rahasia linear. Sehingga pada bagian ini akan dibahas langkah-langkah yang dilakukan pada skema pembagian rahasia linear, yaitu :

1. Tahap pembagian keping rahasia
   a. *Dealer* D memilih suatu bilangan prima $p >$ max (s, n), dengan rahasia $s = a_0$.
   b. *Dealer* D memilih suatu matriks atas $\mathbb{Z}_p$, misalkan $\boldsymbol{H}$, yang berukuran $n \times k$; $n \geq k$. Matriks $\boldsymbol{H}$ yang dipilih harus memiliki sifat setiap k barisnya bebas linear.
   c. *Dealer* D menghitung n keping rahasia, dengan menghitung $\boldsymbol{S} = \boldsymbol{HA}$ dimana $\boldsymbol{S} = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$, $\boldsymbol{H} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1k} \\ h_{21} & h_{22} & h_{23} & \dots & h_{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{n1} & h_{n2} & h_{n3} & \dots & h_{nk} \end{pmatrix}$ dan $\boldsymbol{A} = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_k \end{pmatrix}$. Keping-keping rahasia s_i kemudian didistribusikan ke masing-masing partisipan P_i, $i = 1, 2, \dots, n$.
2. Tahap rekonstruksi rahasia
   a. Sebarang m partisipan $(k \leq m \leq n)$, misalkan $P_{i_1}, P_{i_2}, \dots, P_{i_m}$, menyatukan keping-keping rahasia $s_{i_1}, s_{i_2}, \dots, s_{i_m}$ bersama-sama. Dengan $\{i_1, i_2, \dots, i_m\} \subset \{1, 2, \dots, n\}$.
   b. Menghitung penyelesaian SPL : $\boldsymbol{MA} = \boldsymbol{S}$, dengan $\boldsymbol{M}$ = Sub matriks dari $\boldsymbol{H} = \begin{pmatrix} h_{i_1 1} & h_{i_1 2} & h_{i_1 3} & \dots & h_{i_1 k} \\ h_{i_2 1} & h_{i_2 2} & h_{i_2 3} & \dots & h_{i_2 k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_{i_m 1} & h_{i_m 2} & h_{i_m 3} & \dots & h_{i_m k} \end{pmatrix}$, $\boldsymbol{A} = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_k \end{pmatrix}$ dan $\boldsymbol{S} = \begin{pmatrix} s_{i_1} \\ s_{i_2} \\ \vdots \\ s_{i_m} \end{pmatrix}$. SPL yang diperoleh dijamin konsisten dan mempunyai tepat satu solusi.

Teorema 1 :
Skema Shamir adalah skema linear.
Bukti :
Pertama-tama akan direkonstruksi matriks $\boldsymbol{H}$. Pada tahap pembagian keping rahasia, keping-keping rahasianya dibangkitkan oleh polinomial $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1}$. Sehingga diperoleh :

$$a_0 + a_1 + a_2 + \dots + a_{k-1} = f(1)$$
$$a_0 + 2a_1 + 4a_2 + \dots + 2^{k-1} a_{k-1} = f(2)$$
$$\vdots$$
$$a_0 + na_1 + n^2 a_2 + \dots + n^{k-1} a_{k-1} = f(n)$$

Kemudian dituliskan ke dalam bentuk persamaan matriks :

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 4 & \dots & 2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \dots & n^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{pmatrix}$$

Misalkan $\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 4 & \dots & 2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \dots & n^{k-1} \end{pmatrix}$, $\boldsymbol{A} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{pmatrix}$ dan $\boldsymbol{S} = \begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(n) \end{pmatrix}$

Perhatikan bahwa $\boldsymbol{H}$ berukuran $n \times k$.
Kemudian akan dibuktikan bahwa setiap submatriks $\boldsymbol{H}$ yang berukuran $k \times k$ adalah bebas linear.
Misalkan sub matriks $\boldsymbol{H}$ yang berukuran $k \times k$ adalah $\boldsymbol{H}^* = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_k & \alpha_k^2 & \dots & \alpha_k^{k-1} \end{pmatrix}$ dengan $\{\alpha_1, \alpha_2, \dots, \alpha_k\} \subseteq \{1, 2, \dots, n\}$.
Sehingga akan dibuktikan bahwa:

$$c_0 \begin{pmatrix} h_{i_1 1} & h_{i_1 2} & \dots & h_{i_1 k} \\ h_{i_2 1} & h_{i_2 2} & \dots & h_{i_2 k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{i_m 1} & h_{i_m 2} & \dots & h_{i_m k} \end{pmatrix} + c_1 \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix} + c_2 \begin{pmatrix} \alpha_1^2 \\ \alpha_2^2 \\ \vdots \\ \alpha_k^2 \end{pmatrix} + \dots + c_{k-1} \begin{pmatrix} \alpha_1^{k-1} \\ \alpha_2^{k-1} \\ \vdots \\ \alpha_k^{k-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

hanya terpenuhi jika $c_0 = c_1 = c_2 = \dots = c_{k-1} = 0$.
Dari persamaan sebelumnya diperoleh:

$$c_0 + c_1 \alpha_1 + c_2 \alpha_1^2 + \dots + c_{k-1} \alpha_1^{k-1} = 0$$
$$c_0 + c_1 \alpha_2 + c_2 \alpha_2^2 + \dots + c_{k-1} \alpha_2^{k-1} = 0$$
$$\vdots$$
$$c_0 + c_1 \alpha_k + c_2 \alpha_k^2 + \dots + c_{k-1} \alpha_k^{k-1} = 0$$

Dari persamaan-persamaan linear di atas dapat diketahui bahwa $\alpha_1, \alpha_2, \dots, \alpha_k$ adalah k akar yang berbeda dari polinomial $p(\alpha) =$

$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{k-1}\alpha^{k-1}$. Hal ini kontradiksi dengan teorema dasar aljabar bahwa polinomial berderajat $k - 1$ memiliki paling banyak $k - 1$ akar yang berbeda. Oleh karena itu $p(\alpha)$ adalah polinomial nol.

Sehingga, karena $p(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{k-1}\alpha^{k-1} = 0$ dengan k akar yang berbeda, maka haruslah $c_0 = c_1 = c_2 = \ldots = c_{k-1} = 0$. ■

Skema Harn dan Lin

Pada bab sebelumnya telah dijelaskan mengenai mekanime skema Harn-Lin dimana pada tahap rekonstruksi rahasianya dilakukan dengan membangkitkan suatu polinomial hasil interpolasi Lagrange. Skema Harn-Lin mengidentifikasi pelaku kecurangan dengan menggunakan algoritme berikut ini :

Input: $k, n, s, J, T, s_{i_1}, s_{i_2}, \ldots, s_{i_j}$

dengan $T = \{T_1, T_2, \ldots, T_u\}$ = semua subset dengan t partisipan dari J dan $u = \binom{j}{k}$

1. Menghitung $s^i = \mathrm{F}(T_i), \forall T_i \in T, i = 1,2,\ldots,u$
2. Membagi $U = \{s^1, s^2, \ldots, s^u\}$menjadi v subset $U_i \ni U = U_1 \cup \ldots \cup U_v$ dimana $U_t \cap U_l = \emptyset$, untuk $l \le t, l \le v$ dan $t \ne l$, dan $U_i = \{s^{i_1}, s^{i_2}, \ldots, s^{i_{w_i}}\}$ dimana $s^{w_i} = s^{i_1} = s^{i_2} = \ldots = s^{i_{w_i}}$
3. Misalkan $w_z = \max_i\{w_i\}$, dan misalkan $s = s^{w_z}$
4. Mengambil $T_t \in T \ni s = F(T_t) = F_{T_t}\left(s_{i_{t_1}}, s_{i_{t_2}}, \ldots, s_{i_{t_k}}\right)$, dan misalkan $R = J - \{i_{t_1}, i_{t_2}, \ldots, i_{t_k}\}$
5. Mengambil $i_r \in R$ secara berurut dan hapus dari R, dan menghitung $s^r = F\left(s_{i_r}, s_{i_{t_2}}, \ldots, s_{i_{t_k}}\right)$
6. Jika $s^r = s$, simpan i_r di H; selainnya simpan i_r di C
7. Mengulangi langkah 5 sampai $R = \emptyset$

Output: Himpunan *cheater* adalah C

Pada langkah 1, menghitung s^i dilakukan dengan membangkitkan polinomial hasil interpolasi Lagrange untuk setiap subset dari pemegang keping rahasia. Sama halnya pada langkah 5, s^r dihitung dengan menggunakan pembangkitan polinomial hasil interpolasi Lagrange, dimana s^r merupakan nilai rahasia untuk setiap $T_t \in T$ yang memiliki nilai rahasia yang sama yang merupakan hasil perhitungan dari s^i sebelumnya. Karena pembangkitan polinomial hasil interpolasi Lagrange yang berulang-ulang inilah, mengakibatkan komputasi yang dilakukan tidak efisien.

Skema Yanxiao Liu

Berbeda dengan skema yang diajukan oleh Harn-Lin, skema Yanxiao Liu melakukan rekonstruksi rahasia dengan menggunakan skema berikut pada tahap rekonstruksi rahasianya :

Misal ada k pemegang keping rahasia yang terlibat pada tahap ini, yaitu $P_1, P_2, \ldots, P_k$.

Input: keping-keping rahasia s_i, $i = 1, 2, \ldots, k$

1. Merekonstruksi polinomial hasil interpolasi Lagrange, yaitu $f'(x)$ dan $g'(x)$, masing-masing pada titik-titik $(1, m_1), (2, m_2), \ldots, (k, m_k)$ dan $(1, d_1), (2, d_2), \ldots, (k, d_k)$.
2. Misalkan a_0', a_1', b_0' dan b_1' masing-masing adalah koefisien dari x^0 dan x pada $f'(x)$ dan $g'(x)$. Jika terdapat suatu bilangan $r' \in \mathbb{Z}_p$ yang sama dan memenuhi $r'a_0' + b_0' = 0$ dan $r'a_1' + b_1' = 0$, maka ouput yang dihasilkan adalah $s = f'(0)$. Selainnya, $f'(0)$ adalah rahasia palsu dan ada kecurangan, output $\perp$.

Skema yang diajukan dari segi komputasi lebih efisien dari skema Harn-Lin, karena tidak memerlukan pembangkitan polinomial interpolasi Lagrange yang berulang-ulang. Namun sayangnya, skema yang diajukan hanya mampu untuk mendeteksi kecurangan, belum mampu untuk mengidentifikasi pelaku kecurangan pada rekonstruksi rahasia.

Skema Liu, Yang, Wang, Zhu, dan Ji

Pada skema Liu, Yang, Wang, Zhu, dan Ji (2018 : 23), baik pada tahap pembagian keping-keping rahasia dan rekonstruksi kembali rahasia dilakukan dengan menggunakan polinomial bivariat (dua variabel), misalkan $f(x, y)$. Namun pada skema ini menggunakan dua parameter deteksi yaitu misalkan $e_{i,1} = f_i(d_1), e_{i,2} = f_i(d_2)$ untuk $i = 1, 2, \ldots, m$. Padahal dengan menggunakan polinomial bivariat simetrik dan satu parameter deteksi, kekuatan keamanan dari skema yang diajukan sudah cukup baik.

Skema yang Diajukan

Berdasarkan kajian dari skema-skema pembagian rahasia sebelumnya, maka diajukan skema pembagian rahasia linear berbasis skema Shamir dengan memperbaiki kekurangan-kekurangan yang ada pada skema-skema sebelumnya pada skema yang diajukan ini.

Skema ini merupakan pengembangan dari SPR-(k, n) Shamir dengan modifikasi pada tahap rekonstruksi rahasia. Jika pada SPR-(k, n) Shamir asli rekonstruksi rahasia dilakukan dengan menggunakan interpolasi Lagrange, maka

pada skema penelitian ini akan dilakukan rekonstruksi rahasia dengan menggunakan skema linear yang pemulihan rahasia dilakukan dengan pembangkitan suatu matriks publik.

Pada tahap pembagian keping-keping rahasia, *dealer* menggunakan polinomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$; $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}_p$, dengan rahasia $s = a_0$, untuk membangkitkan keping-keping rahasia yang akan didistribusikan kepada masing-masing pemegang keping rahasia yang berhak. Sedangkan pada tahap rekonstruksi rahasia dengan m ($\geq k$) pemegang keping rahasia yang berpartisipasi diajukan dua algoritme, yaitu algoritme deteksi kecurangan dan algoritme identifikasi pelaku kecurangan.

Sebagai tambahan, digunakan simbol c yang menunjukkan jumlah keping rahasia palsu, $I = \{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$ dan $M = \{i_1, i_2, \ldots, i_m\} \subseteq \{1, 2, \ldots, n\}$ sebagai himpunan semua pemegang keping rahasia pada tahap rekonstruksi. Serta H menunjukkan himpunan para pemegang keping rahasia yang jujur dan C adalah himpunan pemegang keping rahasia yang tidak jujur atau curang.

Tahap pembagian keping rahasia pada skema ini adalah :

Input : rahasia s, k, n, I.

1. *Dealer* D mendefinisikan suatu polinomial acak
   $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$; $a_0, a_1, \ldots, a_k \in \mathbb{Z}_p$
   . Rahasia s tersembunyi pada konstanta a_0.
2. *Dealer* D menghitung keping-keping rahasia $s_i = f(i) \bmod p$ dan kemudian membagikan masing-masing keping rahasia ke masing-masing pemegang keping rahasia P_i, $i = 1, 2, \ldots, n$.

Output : keping-keping rahasia s_i

Adapun tahap rekonstruksi rahasia dari skema ini terbagi ke dalam dua algoritme, yaitu algoritme deteksi kecurangan dan identifikasi pelaku kecurangan. Algoritme deteksi kecurangannya sebagai berikut :

Input : s, k, n, M, $s_{i_1}, s_{i_2}, \ldots, s_{i_m}$

1. Menentukan parameter deteksi $d = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ (diberikan oleh *dealer*).
2. Membangkitkan Sistem Persamaan Linear (SPL): $\boldsymbol{S} = \boldsymbol{HA}$ yang kemudian diubah ke dalam bentuk matriks, yaitu $\boldsymbol{S} = \begin{pmatrix} s_{i_1} \\ s_{i_2} \\ \vdots \\ s_{i_m} \end{pmatrix}$, $\boldsymbol{A} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{pmatrix}$, dan $\boldsymbol{H} = (h_{p,q})$, dengan $h_{p,q} = \begin{cases} 1, \text{untuk } q = 1 \\ i_p^{q-1}, \text{untuk } q \neq 1 \end{cases}$; $h_{p,q}$ adalah entri baris ke-p dan kolom ke-q pada matriks H.
3. Menghitung nilai $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$.
4. Jika $e = d$ maka :

Output: Tidak ada pelaku kecurangan dan rahasianya adalah s, selainnya

Output: Ada pelaku kecurangan

Sedangkan algoritme identifikasi kecurangan pada skema ini adalah :

Input : s, k, n, M, $s_{i_1}, s_{i_2}, \ldots, s_{i_m}$

1. Jika $m = k$ kembali ke algoritme deteksi sebelumnya.
2. Jika $m > k$ maka :

   Langkah 1 : Menghitung banyaknya kombinasi m dari k pemegang keping rahasia, yaitu $v = \binom{m}{k}$ dan misalkan $T = \{T_1, T_2, \ldots, T_v\}$ adalah semua subset m dari k pemegang keping rahasia.

   Langkah 2 : Untuk setiap $T_i \in T$ menghitung nilai $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ dimana $i = 1, 2, \ldots, v$.

   Langkah 3 : Memilih $T_t \in T$ sedemikian sehingga $e = d$ dan misalkan $R = M - \{i_{t_1}, i_{t_2}, \ldots, i_{t_k}\}$.

   Langkah 4 : Memilih $i_r \in R$ secara berurutan dan menghapusnya dari R.

   Langkah 5 : Misalkan s_r adalah keping rahasia yang bersesuaian dengan pemegang keping rahasia i_r yang diserahkan pada tahap rekonstruksi rahasia. Jika $s_r = f(r)$ maka masukkan i_r ke H, selainnya masukkan i_r ke C.

   Langkah 6 : Kembali ke langkah 4 hingga $R = \{\}$.

   Output: C adalah himpunan pelaku kecurangan.

Teorema 2 :

Skema yang diajukan adalah skema pembagian rahasia (k, n) yang *perfect*.

Bukti :

Skema (k, n) yang *perfect* adalah skema berambang batas dimana $k - 1$ keping rahasia atau kurang tidak dapat mengetahui informasi apapun tentang rahasia s. Sehingga sebarang $k - 1$

keping rahasia atau kurang tidak dapat mengonstruksi rahasia asli s. Sehingga akan dibuktikan bahwa kurang dari k keping rahasia tidak akan memperoleh informasi apapun tentang rahasia s.

Pada skema ini, sama dengan skema-skema sebelumnya, rahasia s dibagi menjadi n keping rahasia dengan menggunakan skema asli (k, n) Shamir. Setiap pemegang keping rahasia P_i mendapatkan keping rahasia $s_i = f(i) \bmod p$, dimana $f(i)$ adalah nilai dari suatu polinomial acak $f(x)$ yang tidak diketahui bentuknya oleh semua P_i. Misalkan $k - 1$ pemegang keping rahasia adalah $P_1, P_2, \ldots, P_{k-1}$ dengan masing-masing keping rahasia yang bersesuaian adalah $s_1, s_2, \ldots, s_{k-1}$. Pada tahap rekonstruksi rahasia $k - 1$ pemegang keping rahasia tersebut mengonstruksi SPL $\boldsymbol{S} = \boldsymbol{HA} \Leftrightarrow$

$$\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 4 & \ldots & 2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & k-1 & (k-1)^2 & \ldots & (k-1)^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{pmatrix}$$

. SPL yang dikonstruksi menghasilkan matriks $\boldsymbol{H}$ yang berukuran $(k - 1) \times k$. Karena jumlah baris dari matriks $\boldsymbol{H}$ kurang dari k, maka syarat bahwa setiap k baris dari matriks $\boldsymbol{H}$ bebas linear tidak terpenuhi. Akibatnya solusi dari $a_0, a_1, \ldots, a_{k-1}$ yang dihasilkan bukanlah tunggal. Dengan itu, $k - 1$ pemegang keping rahasia tersebut tidak berhasil untuk mendapatkan rahasia s. ■

Serangan Pelaku Kecurangan

Pada skema yang diajukan ini bertujuan untuk mengatasi serangan yang berupa kecurangan para pemegang keping rahasia yang tidak jujur dengan menyerahkan keping rahasia palsu pada tahap rekonstruksi rahasia. Tipe serangan yang mungkin adalah para pelaku kecurangan memberikan keping rahasia yang palsu tanpa kolaborasi (acak). Dengan kata lain kecurangan dapat dilakukan oleh satu atau lebih dari satu pemegang keping rahasia, dengan asumsi tanpa ada kerjasama di antara mereka.

Batas Kemampuan Deteksi dari Skema yang Diajukan

Teorema 3 :
Untuk serangan dengan para pelaku kecurangan yang melepaskan keping rahasia secara acak, skema yang diajukan dapat mendeteksi kecurangan jika $m \geq k$.
Bukti :
Pada skema yang diajukan, deteksi kecurangan ditentukan dengan nilai parameter deteksi d yang telah ditentukan sebelumnya oleh *dealer*, dan kemudian menghitung nilai e. Dalam perhitungan nilai e dibutuhkan sebesar $m(\geq k)$ keping rahasia untuk membentuk SPL yang akan digunakan untuk menghitung nilai a_j; $j = 0, 1, 2, \ldots, k - 1$. Jika $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = d$, maka tidak ada kecurangan dalam tahap rekonstruksi rahasianya. Sebaliknya jika $e \neq d$, maka ada kecurangan. ■

Teorema 4 :
Untuk serangan dengan dengan tipe sebelumnya yaitu para pemegang keping rahasia palsu yang melepaskan keping rahasianya dengan acak atau tanpa kolaborasi, skema yang diajukan dapat mengidentifikasi kecurangan jika $m - c \geq k$.
Bukti :
Untuk mengidentifikasi pelaku kecurangan pada skema yang diajukan ini ditentukan dengan nilai e yang diperoleh untuk setiap kombinasi pemegang keping rahasia, yaitu $T_1, T_2, \ldots, T_v$, $v = \binom{m}{k}$. Kemudian dilanjutkan dengan pemilihan nilai e, untuk semua kombinasi, yang memenuhi $e = d$. Sehingga akan ada $\binom{m-c}{k}$ kombinasi pemegang keping rahasia yang akan merekonstruksi rahasia yang asli. ■

Analisis Keamanan Skema yang Diajukan

Pada penelitian sebelumnya yang telah dikemukakan oleh Harn dan Lin telah dijelaskan beberapa tipe serangan. Salah satu serangan yang telah dijelaskan oleh Harn dan Lin adalah serangan yang terjadi ketika para pelaku kecurangan, dengan jumlah pelaku kecurangan paling sedikit sama dengan ambang batas ($c \geq k$), berkolaborasi untuk membodohi para partisipan yang jujur dengan melepaskan keping rahasia palsu mereka sedemikian sehingga partisipan yang jujur hanya mendapatkan rahasia palsu. Misalkan $I = \{1, 2, \ldots, n\}$, $m = 2k - 1$, $c = k$, dan $s_1, s_2, \ldots, s_m$ adalah keping-keping rahasia untuk m partisipan. Karena $m = 2k - 1$ dan $c = k$ maka partisipan yang jujur ada sebanyak $k - 1$, misalkan partisipan yang jujur adalah $P_1, P_2, \ldots, P_{k-1}$. Para pelaku kecurangan berhasil memberikan rahasia yang palsu kepada para partisipan yang jujur dengan cara mengonstruksi polinomial baru berderajat k - 1, misalkan $g(x)$,

sedemikian sehingga $g(x)$ melewati titik-titik $(1, s_1), (2, s_2), \ldots, \left(k - 1, s_{k-1}\right)$. Namun untuk skema yang diajukan ini, pelaku kecurangan tidak akan mungkin melakukan serangan seperti sebelumnya dan berhasil membodohi partisipan yang jujur dengan memberikan rahasia palsu. Pada skema yang diajukan ini, serangan sebelumnya sukses dilakukan jika pelaku kecurangan berhasil mengonstruksi $g(x)$ sedemikian sehingga $g(1) = s_1$, $g(2) = s_2$, …, $g(k - 1) = s_{k-1}$ dan membalikkan parameter deteksi $d = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ sedemikian sehingga para pelaku kecurangan mengetahui a_j dan p, $j = 1, 2, \ldots, k - 1$. Namun hal ini secara komputasi sulit dilakukan karena membutuhkan waktu yang lama untuk membalikkan d. Sebagai tambahan, perlu diketahui bahwa nilai $d = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ merupakan hasil perhitungan dari $a_0, a_1, \ldots, a_{k-1}$ yang merupakan koefisien dari polinomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$. Dengan kata lain, setiap satu polinomial $f(x)$ bersesuaian dengan satu parameter deteksi d. Oleh karena itu untuk menyukseskan serangan sebelumnya para pelaku kecurangan harus mengonstruksi $g(x)$ sedemikian sehingga $g(1) = s_1$, $g(2) = s_2$, …, $g(k - 1) = s_{k-1}$ dan mendapatkan parameter deteksi baru yang nilainya sama dengan d. Hal ini tentu sangat sulit dilakukan, sehingga tujuan para pelaku kecurangan untuk membodohi partisipan yang jujur tidak akan berhasil dengan menerapkan skema yang diajukan ini.

Keamanan parameter deteksi juga merupakan hal yang sangat penting dalam skema ini. *Dealer* yang diberikan kepercayaan penuh untuk menetapkan suatu parameter deteksi d tidak boleh secara sengaja ataupun tidak sengaja membocorkan detektor d. Jika detektor d terungkap oleh para pelaku kecurangan, maka para pelaku kecurangan tersebut dapat memodifikasi detektor asli d dengan suatu cara tertentu.

Percobaan-Percobaan

Pada bagian ini, akan diberikan beberapa contoh untuk simulasi skema yang diajukan.

Contoh 1: Skema dengan 1 orang pelaku kecurangan.

Misalkan skema yang dijadikan sebagai contoh adalah skema (5, 8). Dengan kata lain suatu rahasia s dibagi ke dalam 8 keping rahasia, dengan ambang batas paling sedikit 5 keping rahasia yang dapat merekonstruksi rahasia. Kemudian tahap pembagian rahasia dan rekonstruksi rahasianya adalah sebagai berikut :

1. Tahap pembagian rahasia
   a. *Dealer* D memilih bilangan prima $p = 673$, dengan $s = a_0 = 273$. Kemudian memilih polinomial acak atas $\mathbb{Z}_{673}$, yaitu $f(x) = 273 + 179x + 311x^2 + 170x^3 + 594x^4$
   b. *Dealer* D menghitung nilai dari 15 keping rahasia :
      $s_1 = f(1) \bmod 673 = 181$; $s_2 = f(2) \bmod 673 = 625$;
      $s_3 = f(3) \bmod 673 = 454$; $s_4 = f(4) \bmod 673 = 659$;
      $s_5 = f(5) \bmod 673 = 335$; $s_6 = f(6) \bmod 673 = 46$;
      $s_7 = f(7) \bmod 673 = 479$; $s_8 = f(8) \bmod 673 = 425$.
      Masing-masing keping rahasia didistribusikan ke s_i ke partisipan P_i, dengan $i = 1,2,\ldots,8$ sedemikian sehingga diperoleh 8 pasangan berurutan, yaitu : {(1, 181), (2, 625), (3, 454), (4, 659), (5, 335), (6, 46), (7, 479), (8, 425)}.

2. Tahap rekonstruksi rahasia
   Misalkan ada $m = 6$ pemegang keping rahasia yaitu $P_1, P_2, P_3, P_4, P_5, P_7$ yang menyerahkan keping rahasianya pada tahap rekonstruksi rahasia dan P_7 memutuskan untuk melakukan kecurangan dengan menyerahkan keping rahasia palsu $s_7^* = 478$.

   Deteksi Pelaku Kecurangan :
   Dealer sebelumnya memberikan parameter deteksi $d = 454$ kepada para pemegang keping rahasia yang akan mengonstruksi rahasia s. Kemudian ke-7 pemegang keping rahasia tersebut bersama-sama membangkitkan SPL $\boldsymbol{S} = \boldsymbol{HA}$ seperti di bawah ini :

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_7^* \end{pmatrix} = \begin{pmatrix} 181 \\ 625 \\ 454 \\ 659 \\ 335 \\ 478 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 5 & 25 & 125 & 625 \\ 1 & 7 & 49 & 343 & 382 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

   Sedemikian sehingga diperoleh matriks yang diperbesar dalam bentuk eselon baris adalah :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 181 \\ 0 & 1 & 3 & 7 & 15 & 444 \\ 0 & 0 & 2 & 12 & 50 & 58 \\ 0 & 0 & 0 & 6 & 60 & 318 \\ 0 & 0 & 0 & 0 & 24 & 123 \\ 0 & 0 & 0 & 0 & 0 & 672 \end{pmatrix}$$

Jelas bahwa matriks di atas adalah matriks yang tak konsisten. Oleh karena itu SPL tersebut tidak memiliki solusi tunggal, sehingga tidak akan dapat diperoleh nilai $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = d$. Ini berarti terjadi kecurangan pada tahap rekonstruksi rahasia.

Identifikasi Pelaku Kecurangan :

Pada tahap ini ada $v = \binom{m}{k} = \binom{6}{5} = 6$ kombinasi pemegang keping rahasia, yaitu : $T = \{T_1, T_2, \ldots, T_6\} = \{\{1, 2, 3, 4, 5\}, \{1, 2, 3, 4, 7\}, \{1, 2, 3, 5, 7\}, \{1, 2, 4, 5, 7\}, \{1, 3, 4, 5, 7\}, \{2, 3, 4, 5, 7\}\}$.

- Untuk $T_1 = \{1, 2, 3, 4, 5\}$, diperoleh SPL :

$$\begin{pmatrix} 181 \\ 625 \\ 454 \\ 659 \\ 335 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 5 & 25 & 125 & 625 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

Dengan solusi $a_0 = 273$, $a_1 = 179$, $a_2 = 311$, $a_3 = 170$, $a_4 = 594$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 454 = d$.

- Untuk $T_2 = \{1, 2, 3, 4, 7\}$, diperoleh SPL :

$$\begin{pmatrix} 181 \\ 625 \\ 454 \\ 659 \\ 478 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 7 & 49 & 343 & 382 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}$$

Dengan solusi $a_0 = 587$, $a_1 = 310$, $a_2 = 152$, $a_3 = 600$, $a_4 = 551$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 572 \neq d$.

Sehingga tanpa melakukan perhitungan untuk T_3, T_4, T_5, T_6 diperoleh bahwa pelaku kecurangan dalam tahap rekonstruksi rahasia tersebut adalah P_7 dan rahasia $s = a_0 = 273$.

Contoh di atas menunjukkan bahwa untuk dapat mendeteksi kecurangan terdapat jumlah partisipan $m = 7 \geq k$ dan dapat mengidentifikasi pelaku kecurangan jika $c = 1 \leq m - k$. Hal ini sesuai dengan teorema yang diperoleh sebelumnya bahwa untuk mendeteksi pelaku kecurangan yang melepaskan keping rahasianya secara acak dibutuhkan $m \geq k$ dan untuk mengidentifikasinya dibutuhkan $m - c \geq k$.

Contoh 2: Skema dengan 2 orang pelaku kecurangan.

Misalkan skema ambang batas (3, 6). Sedemikian sehingga rahasia s dibagi menjadi 6 bagian dan sebanyak 3 atau lebih keping rahasia dapat merekonstruksi rahasia s.

1. Tahap pembagian rahasia
   a. *Dealer* D memilih bilangan prima $p = 97$, dengan $s = a_0 = 17$. Kemudian memilih polinomial acak atas $\mathbb{Z}_{97}$, yaitu $f(x) = 17 + 51x + 55x^2$.
   b. *Dealer* D menghitung nilai dari 15 keping rahasia :
   $s_1 = f(1) \bmod 97 = 26$; $s_2 = f(2) \bmod 97 = 48$;
   $s_3 = f(3) \bmod 97 = 83$; $s_4 = f(4) \bmod 97 = 34$;
   $s_5 = f(5) \bmod 97 = 95$; $s_6 = f(6) \bmod 97 = 72$.
   Masing-masing keping rahasia didistribusikan ke s_i ke partisipan P_i, dengan $i = 1, 2, 3, 4, 5, 6$ sedemikian sehingga diperoleh 6 pasangan berurutan, yaitu : {(1, 26), (2, 48), (3, 83), (4, 34), (5, 95), (6, 72)}.
2. Tahap rekonstruksi rahasia
   Misalkan ada $m = 5$ pemegang keping rahasia yaitu P_1, P_2, P_3, P_4, P_6 yang menyerahkan keping rahasianya pada tahap rekonstruksi rahasia dengan P_1 dan P_6 memutuskan untuk melakukan kecurangan dengan menyerahkan keping rahasia palsu $s_1^* = 23$ dan $s_6^* = 71$.

   Deteksi Pelaku Kecurangan :
   Dealer sebelumnya memberikan parameter deteksi $d = 62$ kepada para pemegang keping rahasia yang akan mengonstruksi rahasia s. Kemudian ke-5 pemegang keping rahasia tersebut bersama-sama membangkitkan SPL $\boldsymbol{S} = \boldsymbol{HA}$ seperti di bawah ini :

$$\begin{pmatrix} s_1^* \\ s_2 \\ s_3 \\ s_4 \\ s_6^* \end{pmatrix} = \begin{pmatrix} 23 \\ 48 \\ 83 \\ 34 \\ 71 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \\ 1 & 6 & 36 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$$

   Sedemikian sehingga diperoleh matriks yang diperbesar dalam bentuk eselon baris adalah :

$$\begin{pmatrix} 1 & 1 & 1 & 23 \\ 0 & 1 & 3 & 25 \\ 0 & 0 & 2 & 10 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Matriks tersebut adalah matriks tak konsisten. Sehingga SPL yang diperoleh sebelumnya tidak memiliki solusi tunggal, akibatnya tidak akan dapat diperoleh nilai $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = d$. Ini berarti terjadi kecurangan pada tahap rekonstruksi rahasia.

Identifikasi Pelaku Kecurangan :

Pada tahap ini ada $v = \binom{m}{k} = \binom{5}{3} = 10$ kombinasi pemegang keping rahasia, yaitu : $T = \{T_1, T_2, \ldots, T_{10}\} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 6\}, \{1, 3, 4\}, \{1, 3, 6\}, \{1, 4, 6\}, \{2, 3, 4\}, \{2, 3, 6\}, \{2, 4, 6\}, \{3, 4, 6\}\}$.

Perhatikan bahwa banyaknya pemegang keping rahasia yang jujur adalah $m - c = 3$ orang, sedemikian sehingga ada $\binom{3}{3} = 1$ kombinasi pemegang keping rahasia yang akan merekonstruksi rahasia asli.

- Untuk $T_1 = \{1, 2, 3\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 48 \\ 83 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 8$, $a_1 = 10$, $a_2 = 5$dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 30 \neq d$.
- Untuk $T_2 = \{1, 2, 4\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 48 \\ 34 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 9$, $a_1 = 57$, $a_2 = 54$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 53 \neq d$.
- Untuk $T_3 = \{1, 2, 6\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 48 \\ 71 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 6 & 36 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 0$, $a_1 = 22$, $a_2 = 1$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 23 \neq d$.
- Untuk $T_4 = \{1, 3, 4\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 83 \\ 34 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 11$, $a_1 = 6$, $a_2 = 6$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 30 \neq d$.
- Untuk $T_5 = \{1, 3, 6\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 83 \\ 71 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 9 \\ 1 & 6 & 36 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 89$, $a_1 = 96$, $a_2 = 32$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 87 \neq d$.
- Untuk $T_6 = \{1, 4, 6\}$, diperoleh SPL :
  $\begin{pmatrix} 23 \\ 34 \\ 71 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 4 & 16 \\ 1 & 6 & 36 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 70$, $a_1 = 5$, $a_2 = 45$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 48 \neq d$.
- Untuk $T_7 = \{2, 3, 4\}$, diperoleh SPL :
  $\begin{pmatrix} 48 \\ 83 \\ 34 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$
  Dengan solusi $a_0 = 17$, $a_1 = 51$, $a_2 = 55$ dan $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p = 62 = d$.

Karena kombinasi pemegang keping rahasia dari T_7 berhasil memperoleh nilai $e = d = 62$, maka P_2, P_3, P_4 adalah pemegang keping rahasia yang jujur. Sebagai akibatnya P_1 dan P_6 teridentifikasi sebagai pelaku kecurangan (tidak diperlukan perhitungan yang lebih lanjut terhadap T_8, T_9, T_{10}.

Simpulan

Skema (k, n) Shamir adalah suatu skema ambang batas dimana pembangkitan rahasia dilakukan dengan pembangkitan interpolasi Lagrange. Skema pembagian rahasia linear yang berbasis skema Shamir merupakan generalisasi dari skema asli Shamir. Tahapan dari skema ini terdiri dari dua bagian, yaitu tahap pembagian keping-keping rahasia dan tahap rekonstruksi rahasia. Tahap pembagian keping rahasia menyerupai skema asli Shamir, sedangkan tahap rekonstruksi rahasia terdiri dari dua algoritme. Algoritme pada tahap rekonstruksi rahasia tersebut adalah algoritme deteksi kecurangan dan algoritme identifikasi pelaku kecurangan. Pada algoritme deteksi kecurangan dilakukan penentuan parameter deteksi d dan solusi dari

SPL yang dihasilkan yaitu $a_0, a_1, \ldots, a_{k-1}$. Jika $d = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ dimana p adalah suatu bilangan prima, maka tidak ada kecurangan yang terjadi dalam tahap rekonstruksi rahasia. Selainnya, berarti ada kecurangan dalam rekonstruksi rahasianya. Sedangkan pada algoritme identifikasi pelaku kecurangan dilakukan dengan menghitung nilai $e = \left\lfloor \left(\sqrt[k]{\prod_{j=0}^{k-1} a_j} + \sum_{j=0}^{k-1} a_j \right) \right\rfloor \bmod p$ untuk setiap kombinasi pemegang keping rahasia. Jika nilai $e \neq d$ untuk suatu kombinasi pemegang keping rahasia, maka terdapat pelaku kecurangan dari anggota kombinasi pemegang keping rahasia tersebut. Himpunan pelaku kecurangan dimasukkan ke dalam himpunan C, sedangkan himpunan pemegang keping rahasia yang jujur dimasukkan ke dalam H.

Skema yang diajukan dapat mendeteksi kecurangan jika $m \geq k$ dan dapat mengidentifikasi pelaku kecurangan jika $m - c \geq k$, dengan asumsi bahwa para pelaku kecurangan melepaskan keping rahasia tanpa kolaborasi (acak). Setelah melakukan analisis keamanan dari skema yang diajukan dihasilkan bahwa dengan menerapkan tipe serangan skema Harn dan Lin dengan para pelaku kecurangan berkolaborasi untuk membodohi partisipan yang jujur, maka serangan tersebut sulit untuk dilakukan dengan sukses. Hal ini dikarenakan untuk menyukseskan serangan tersebut dibutuhkan suatu polinomial baru $g(x)$ sedemikian sehingga $g(1) = s_1$, $g(2) = s_2$, …, $g(k-1) = s_{k-1}$ dan suatu parameter deteksi baru yang nilainya sama dengan detektor d.

Daftar Pustaka

Anton H, Rorres C. (2010). *Elementary Linear Algebra: Application Version*. *(10th ed.)*. New Jersey : John Wiley & Sons.

Barbeau, E.J. (2003). *Polynomials*. New York : Springer-Verlag.

Blakley, G.R. (1979). Safeguarding cryptographic keys. *AFIPS Conference Proceedings* : *1979 National Computer Conference Jun 4-7 1979*. New York : AFIPS Press.

Cheney, W., Kincaid, D. (2008). *Numerical Mathematics and Computing*. *(6th ed.)*. Belmont : Thomson Brooks/Cole.

Harn, L. & Lin, C.L. (2009). Detection and identification of cheaters in (*t*,*n*) secret sharing scheme. *Design, Codes and Criptography*, 52(1), 15-24.

Leung, K.T., Mok, I.A.C., Suen, S.N. *Polynomials and Equations*. Hong Kong : Hong Kong University Press.

Liu, Y.X. (2016). Linear (*k*, *n*) secret sharing scheme with cheating detection. *Security and Communication Network*, 9(13), 2115-2121.

Liu, Y.X., Yang, C.N., Wang, Y.C., Zhu, L., & Ji, W.J. (2018). Cheating identifiable secret sharing scheme using symmetric bivariate polynomial", dalam *Information Science*. Vol. 453, 21-29.

Menezes, A.J., van-Oorschot, P.C., Vanstone, S.A. 1996. *Handbook of Applied Cryptography*. Florida : CRC Press.

Shah MA. 2012. Fundamental theorem of algebra a study. *IJCER* 2(8), 297-317.

Shamir, A. (1979). How to share a secret. *Communication of the ACM*, 22(11), 612-613.