Bahan tambahan kuliah IF4020 Kriptografi

Skema Pembagian Data Rahasia
(*Secret Sharing Scheme*)

Oleh: Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
ITB

- Misalkan anda memiliki PIN kartu ATM tabungan di bank yang tentu saja rahasia.
- Sebelum meninggal dunia, Anda ingin membagi (*sharing*) PIN itu kepada enam orang anak anda menjadi enam bagian.
- Namun untuk merekonstruksi PIN semula dibutuhkan *sedikitnya* tiga orang anak untuk merangkai bagian-bagiannya menjadi PIN yang utuh.
- Bagaimana cara melakukan pembagian ini?

→ *Secret sharing schemes*!!!

Terminologi

- *Secret*: data/informasi rahasia (*password*, kunci, PIN, pesan, file, dsb).

- *Secret* direpresentasikan sebagai sebuah *integer M*.
  Contoh: ‘`abcd`’ dinyatakan sebagai `102030405`
  `(A = 01, B = 02, C = 03,dst)`

- *Share*: hasil pembagian *secret*
- *Dealer*: pihak yang melakukan pembagian *secret*
- Partisipan: orang yang memperoleh *share*.

Skema Ambang (*threshold schemes*)

- Misalkan *t*, *w* adalah bilangan bulat positif dengan $t \leq w$.
- Skema ambang (*t*, *w*) adalah metode pembagian pesan *M* kepada *w* partisipan sedemikian sehingga sembarang himpunan bagian yang terdiri dari *t* partisipan dapat merekonstruksi *M*, tetapi jika kurang dari *t* maka *M* tidak dapat direkonstruksi.

- Ditemukan oleh Shamir (1979), dikenal sebagai skema ambang Shamir (*Shamir threshold scheme*).

Skema Shamir

- Idenya dari persoalan interpolasi:

  - Untuk membentuk persamaan linier $y = a_0 + a_1x$ diperlukan 2 buah titik: (x_1, y_1), (x_2, y_2)

  - Untuk membentuk persamaan kuadratik $y = a_0 + a_1x + a_2x^2$ diperlukan 3 buah titik (x_1, y_1), (x_2, y_2), (x_3, y_3)

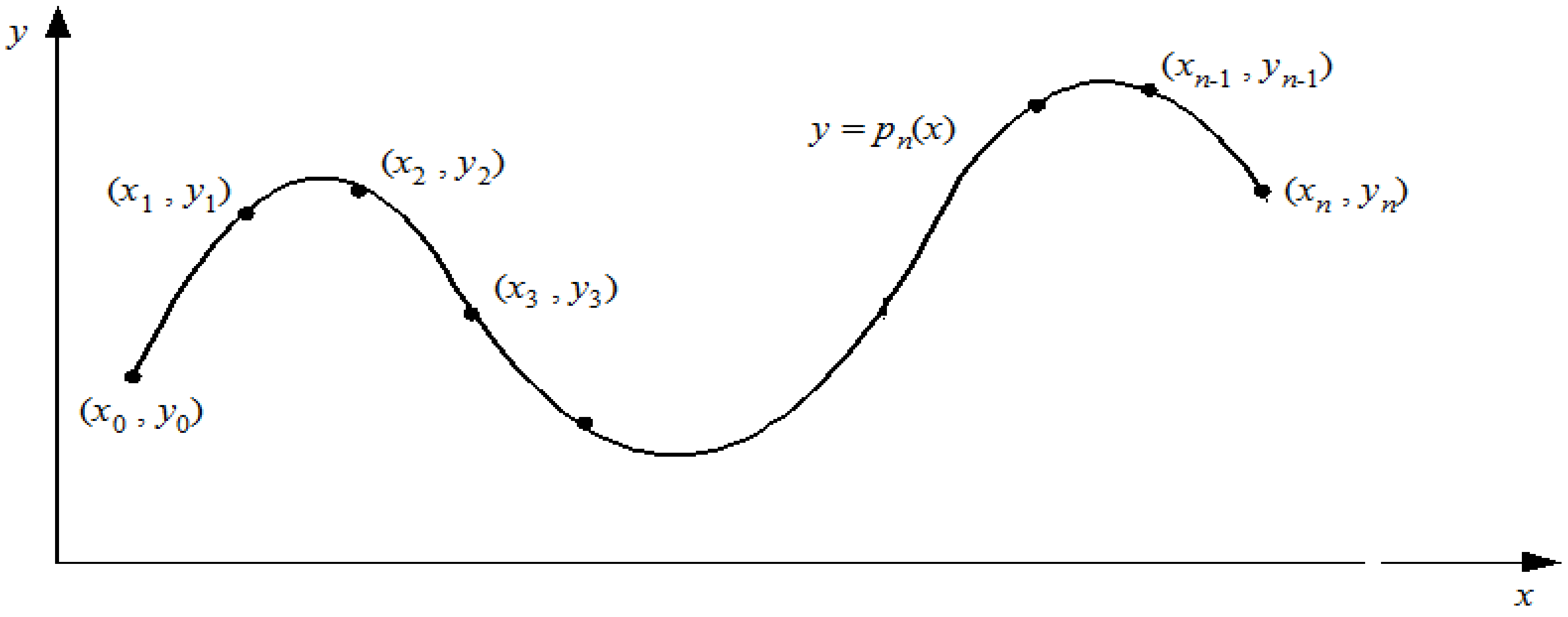
  - dst

  - Untuk membentuk polinomial $y = a_0 + a_1x + a_2x^2 + \ldots + a_nx_n$ diperlukan n + 1 titik.

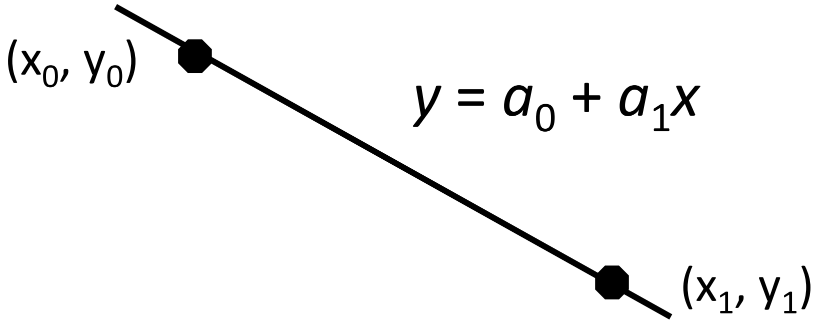
Interpolasi

- Polinom interpolasi derajat n yang menginterplolasi titik-titik (x_0, y_0), (x_1, y_1), ..., (x_n, y_n) adalah

$$y = p_n(x) = a_0 + a_1x + a_2x_2 + \ldots + a_nx^n$$



Contoh: Interpolasi linier



Substitusikan (x_0, y_0) dan (x_1, y_1) ke dalam $y = a_0 + a_1x$, diperoleh SPL:

$$y_0 = a_0 + a_1x_0$$
$$y_1 = a_0 + a_1x_1$$

dapat dipecahkan untuk menentukan a_0 dan a_1

- Untuk polinom interpolasi berderajat n:

$$y = p_n(x) = a_0 + a_1 x + a_2 x_2 + \ldots + a_n x^n$$

dibutuhkan (n+1) buah titik data.

- Dengan menyulihkan $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$ ke dalam $y = p_n(x)$, diperoleh n buah sistem persamaan lanjar dalam $a_0, a_1, a_2, \ldots, a_n$,

$$\begin{aligned}
&a_0 + a_1 x_0 + a_2 x_0^2 + \ldots + a_n x_0^3 = y_0 \\
&a_0 + a_1 x_1 + a_2 x_1^2 + \ldots + a_n x_1^3 = y_1 \\
&a_0 + a_1 x_2 + a_2 x_2^2 + \ldots + a_n x_2^3 = y_2 \\
&\ldots \qquad\qquad\qquad \ldots \\
&a_0 + a_1 x_n + a_2 x_n^2 + \ldots + a_n x_n^3 = y_n
\end{aligned}$$

- Solusi sistem persamaan lanjar ini diperoleh dengan menggunakan metode eliminasi Gauss yang sudah anda pelajari.

Skema (t, w)

Algoritma:

1. Pilih bilangan prima p, yang harus lebih besar dari semua kemungkinan nilai pesan M dan juga lebih besar dari jumlah w partisipan. Semua komputasi dihasilkan dalam modulus p.

2. Pilih $t – 1$ buah bilangan bulat acak dalam modulus p, misalkan s_1, s_2, …, s_{t-1}, dan nyatakan polinomial:

$$s(x) \equiv M + s_1x + s_2x^2 + \ldots + s_{t-1}x^{t-1} \pmod{p}$$

sedemikian sehingga $s(0) \equiv M \pmod{p}$.

3. Untuk w partisipan, kita pilih *integer* berbeda, $x_1, x_2, \ldots, x_w$ (mod p) dan setiap orang memperoleh *share* (x_i, y_i) yang dalam hal ini

$$y_i \equiv s(x_i) \pmod{p}.$$

Misalnya, untuk w orang kita memilih $x_1 = 1$, $x_2 = 2$, …, $x_w = w$.

Contoh: Skema (3, 8)

- Artinya: w = 8 partisipan, diperlukan t = 3 partisipan untuk melakukan rekonstruksi M.
- Misalkan M = 190503180520 (*secret*)
- Misalkan p = 1234567890133 (prima)
- Pilih 3 – 1 = 2 buah bilangan acak, s_1 = 482943028839, s_2 = 1206749628665 untuk membentuk polinom:

$$s(x) \equiv M + s_1 x + s_2 x^2 \pmod{p}$$

$$s(x) \equiv 190503180520 + 482943028839x + 1206749628665x^2 \pmod{1234567890133}$$

Polinom $s(x)$ harus dirahasiakan!

- Tiap partisipan memperoleh (x, $s(x)$). Misakan $x_1 = 1$, $x_2 = 2$, …, $x_8 = 8$, maka, setiap orang memperoleh *share*:

$s(x) \equiv 190503180520 + 482943028839x + 1206749628665x^2 \pmod{1234567890133}$

x = 1 → s(1) = 645627947891, diperoleh share 1 = (1, 645627947891)

x = 2 → s(2) = 1045116192326, diperoleh share 2 = (2, 1045116192326)

…

share 3 = (3, 154400023692)

share 4 = (4, 442615222255)

share 5 = (5, 675193897882)

share 6 = (6, 852136050573)

share 7 = (7, 973441680328)

x = 8 → s(8) = 1039110787147, diperoleh share 8 = (8, 1039110787147)

Misalkan t orang partisipan akan merekonstruksi M, dengan *share* masing-masing:

$$(x_1, y_1), (x_2, y_2) \ldots, (x_t, y_t).$$

Substitusikan setiap (x_k, y_k) ke dalam polinomial:

$$s(x) \equiv M + s_1 x + s_2 x^2 + \ldots + s_{t-1} x^{t-1} \pmod p$$

Ini berarti:

$$y_k \equiv s(x_k) \equiv M + s_1 x_k + s_2 x_k^2 \ldots + s_{t-1} x_k^{t-1} \pmod p, \quad 1 \le k \le t$$

Diperoleh sistem persamaan linier sebagai berikut:

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{t-1} \\ 1 & x_2 & \ldots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} M \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} \pmod{p}$$

Selesaikan sistem persamaan linier di atas, misalnya dengan metode eliminasi Gauss-Jordan, untuk memperoleh *M*.

Catatan: *p* tidak perlu rahasia, tetapi polinom *s*(*x*) dirahasiakan.

- Misalkan partisipan 2, 3, dan 7 ingin merekonstruksi *M*:

  Share mereka: (2, 1045116192326), (3, 154400023692), (7, 973441680328)
- Substitusikan setiap *share* ke dalam:

$$y_k \equiv s(x_k) \equiv M + s_1 x_k + s_2 x_k^2 \ldots + s_{t-1} x_k^{t-1} \pmod{p}, \quad 1 \le k \le t$$

- Lalu pecahkan sistem persamaan linier:

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 7 & 49 \end{pmatrix} \begin{pmatrix} M \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1945116192326 \\ 1544000023692 \\ 973441680328 \end{pmatrix} \pmod{1234567890133}$$

  yang menghasilkan solusi

  (M, s_1, s_2) = (190503180520, 482943028839, 1206749628665)

  Secret yang dicari adalah 190503180520

- Apa yang terjadi jika 2 orang partisipan mencoba merekonstruksi M?
- Tidak mungkin 2 buah titik bisa membentuk polinom derajat 2:

$$s(x) \equiv M + s_1 x + s_2 x^2 \pmod{p}$$

- Misalkan dicoba menggunakan titik ketiga (0, c), maka polinom tetap mengandung sebuah nilai yang tidak diketahui.

- Apa yang terjadi jika > 3 orang partisipan mencoba merekonsruksi M?
- Polinom tetap bisa ditemukan!

Metode Interpolasi Lagrange

- Alternatif lain: menggunakan metode interpolasi Lagrange
- Diberikan t buah titik: $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_t)$.

- Polinom Lagrange (mod p) yang melalui t titik adalah polinom derajat $t - 1$:

$$p(x) \equiv y_1L_1(x_1) + y_2L_2(x_2) + \ldots + y_tL_t(x_t) \pmod{p}$$

yang dalam hal ini: $L_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{x - x_i}{x_k - x_i}$ $\quad k = 1, 2, \ldots, t$

Untuk memperoleh M, hitung $p(x)$ pada $x = 0$.

Contoh: Jika partisipan 2, 3, dan 7 menggunakan interpolasi Lagrange:

$(x_1, y_1) = (2, 1045116192326)$

$(x_2, y_2) = (3, 154400023692)$

$(x_3, y_2) = (7, 973441680328)$

Hitung: $p(x) \equiv y_1 L_1(x_1) + y_2 L_2(x_2) + y_3 L_3(x_3)$ (mod p)

$$L_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{x - x_i}{x_k - x_i}$$

- Diperoleh:

  $p(x) \equiv 20705602144728/5 - 1986192751427x + (1095476582793/5)x^2$

  $\quad\quad (\text{mod } 1234567890133)$

  Karena kita bekerja dalam modulo p dan mengingat:

  $$1/5 = 5^{-1} \ (\text{mod } 1234567890133) = 740740734080$$

  Ganti 1/5 dapat diganti dengan 740740734080, sehingga diperoleh polinom tanpa modulo p:

  $$p(x) = 190503180520 + 482943028839x + 1206749207056021447 28x^2$$

- Untuk memperoleh M, hitung p(0), diperoleh p(0) = 190503180520 = M.

Referensi

- Trappe, W., Washington, L., *Introduction to Cryptography with Coding Theory*, 2nd edition, Pearson-Prentice Hall, 2006