Aplikasi *Chinese Remainder Theorem* dalam *Secret Sharing*

Suhailie - 13517045[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]suhailie20@gmail.com

***Abstraks*—Seiring berjalannya waktu, teknologi dan informasi semakin berkembang dan menjadi penting dalam kehidupan sehari - hari. Dengan adanya teknologi, informasi menjadi lebih mudah untuk didapatkan baik secara legal maupun illegal. Dalam hal ini, *secret sharing* merupakan salah satu cara untuk menjaga rahasia dari suatu informasi dengan menggunakan *chinese remainder theorem*.**

Kata kunci—secret sharing, chinese remainder theorem, asmuth-bloom, mignotte.

I. PENDAHULUAN

Secret sharing merupakan suatu metode mendistribusikan suatu rahasia atau informasi kepada sebuah jumlah orang tertentu. Dalam *secret sharing*, ada seorang pemegang rahasia S misalkan D, dan n orang pemegang bagian rahasia. Rahasia S hanya dapat ditemukan bila suatu kondisi terpenuhi. Jenis *secret sharing* yang sering digunakan adalah *threshold secret sharing*, di mana rahasia S akan terungkap bila ada sejumlah t orang atau lebih sebagai pemegang bagian rahasia yang mengumpulkan dan membangun bagian – bagian rahasia yang ada menjadi sebuah rahasia S yang utuh.

Threshold secret sharing terbagi menjadi beberapa jenis berdasarkan cara kerjanya, ada Shamir's *threshold secret sharing*, Blakley's *geometric threshold secret sharing*, Mignotte's *threshold secret sharing*, Asmuth-Bloom's *threshold secret sharing*. Kedua Mignotte dan Asmuth-Bloom *secret sharing* menggunakan aplikasi *chinese remainder theorem*.

Pada makalah ini akan dibahas cara pengaplikasian *chinese remainder theorem* dalam *threshold secret sharing* yaitu Mignotte's dan Asmuth-Bloom's.

II. CHINESE REMAINDER THEOREM

Chinese Remainder Theorem adalah sebuah teorema yang mengungkapkan jika diketahui beberapa sisa dengan pembagi n = {n_1,n_2,n_3,...} bilangan bulat positif, dan bilangan dalam n merupakan relatif prima, maka selalu ada bilangan x yang memenuhi sistem kongruensi tersebut, dengan kondisi $0 \leq x \leq N$, di mana N merupakan hasil perkalian dari bilangan pembagi tersebut (n).

$$x \equiv a_1 mod\ n_1$$
$$x \equiv a_2 mod\ n_2$$
$$\dots\dots\dots$$
$$x \equiv a_k mod\ n_k$$

Chinese Remainder Theorem pertama kali ditemukan seorang matematikawan China yang bernama Sun Zi, yang ditulis dalam buku Sunzi Suanjing (孙子算经).

Gambar 1. Sun Zi
(sumber : https://worldhistory.us/chinese-history/the-art-of-war-sun-tzu-created-history.php)

Misal diberikan sebuah sistem kongruensi :

$$x \equiv 3\ mod\ 5$$
$$x \equiv 5\ mod\ 7$$
$$x \equiv 7\ mod\ 11$$

Dengan mencari N sebagai hasil perkalian dari bilangan pembagi yang relatif prima,

$$N = 5\ x\ 7\ x\ 11$$
$$N = 385$$

dan karena,

$$77\ .3\ \equiv 1\ mod\ 5$$
$$55\ .6\ \equiv 1\ mod\ 7$$
$$35\ .6\ \equiv 1\ mod\ 11$$

maka didapat solusi x,

$$x \equiv 3 \,.\, 77 \,.\, 3 + 5 \,.\, 55 \,.\, 6 + 7 \,.\, 35 \,.\, 6 \; mod \; 385$$
$$x \equiv 3813 \; mod \; 385$$
$$x \equiv 348 \; mod \; 385$$

Perhatikan bahwa 348 dibagi 5 menyisakan 3, bila dibagi 7 menyisakan 5 dan bila dibagi 11 menyisakan 7. Solusi 348 merupakan bilangan terkecil dari solusi sistem kongruensi diatas.

III. SECRET SHARING

A. Definisi Threshold Secret Sharing

Threshold secret sharing adalah salah satu metode pembagian sebuah rahasia S menjadi beberapa beberapa bagian rahasia (I). Misalkan kita ingin membagi rahasia S ke dalam n bagian rahasia, dengan sejumlah n pemegang bagian rahasia memegang satu dari bagian rahasia tersebut.

Untuk menemukan rahasia S, diperlukan sejumlah k bagian rahasia. Namun, rahasia S tersebut tidak dapat ditemukan bila hanya ada bagian rahasia sejumlah kurang dari k.

B. Mignotte's Threshold Secret Sharing

Mignotte's *threshold secret sharing* memiliki sebuah urutan unik yaitu (k,n)-rangkaian Mignotte. K dan n merupakan bilangan bulat positif, dengan syarat $2 \leq k \leq n$. N merupakan jumlah orang pemegang bagian rahasia dan k merupkan jumlah pemegang bagian rahasia yang dibutuhkan untuk mengungkapkan rahasia.

Cara untuk membuat skema Mignotte's *threshold secret sharing* adalah :

a. (k,n)-rangkaian Mignotte memiliki serangkaian bilangan bulat positif yang membesar $m_1 < ..... < m_n$, di mana

$$m_{n-k+2} \times ... \times m_n < m_1 \times ... \times m_k$$

b. Kita memilih sebuah rahasia S sebagai sebuah bilangan bulat di mana $A < S < B$, A adalah m_{n-k+2} ... m_n dan B adalah m_1 ... m_k.

c. Untuk bagian rahasia I_i, didapatkan dengan syarat $1 \leq i \leq n$.

$$I_i = S \; mod \; m_i$$

d. Dengan adanya I sebanyak n, maka diperlukan I sejumlah k untuk dapat mengungkapkan rahasia S.

C. Asmuth – Bloom's Threshold Secret Sharing

Asmuth-Bloom's *threshold secret sharing* juga memiliki urutan unik yaitu (k,n)-rangkaian Asmuth-Bloom, dengan syarat $2 \leq k \leq n$.

Cara untuk membuat skema Asmuth-Bloom's *threshold secret sharing* adalah :

a. Buat sebuah rangkaian bilangan bulat positif yang membesar $y < m_1 < ..... < m_n$, di mana

$$y \times m_{n-k+2} \times ... \times m_n < m_1 \times ... \times m_k$$

b. Kita memilih sebuah rahasia S sebagai sebuah bilangan bulat yang berada dalam set Z/yZ.

c. Kita memilih sebuah bilangan bulat (X), sehingga $S + X \,.\, y < m_1 \times .... \times m_k$.

d. Untuk bagian rahasia I_i, didapatkan dengan syarat $1 \leq i \leq n$.

$$I_i = (S + X \times y) \; mod \; m_i$$

e. Dengan adanya I sebanyak n, diperlukan I sejumlah k untuk menentukan rahasia S.

D. Shamir's Secret Sharing

Pada tahun 1979 Adi Shamir mengemukakan skema pembagian secret yang dinamakan skema ambang Shamir (Shamir threshold scheme). Skema pembagian tersebut berbunyi:

Misalkan t dan w adalah bilangan bulat positif dengan t <= w. Skema ambang (t, w) adalah metode pembagian secret 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.

Ide dari Shamir's secret sharing adalah penggunaan polinomial, di mana titik koordinat sejumlah k dapat menjelaskan polinomial dengan derajat k-1.

Untuk dapat menggunakan skema ambang Shamir tersebut maka secret harus direpresentasikan dengan integer M. Misalnya secret 'ABCD' dinyatakan sebagai M = 102030405 dengan mengkodekan A = 01, B = 02, C = 03, dan seterusnya. Orang yang melakukan pembagian secret dinamakan dealer. Dealer haruslah orang yang dipercaya oleh semua parstisipan.

Secara teknis, pembagian secret M menjadi sejumlah share menggunakan konsep interpolasi polinom yang dikenal di dalam metode numerik. Di dalam teori interpolasi, untuk membentuk persamaan linier y = a0 + a1x diperlukan 2 buah titik yaitu (x1, y1) dan (x2, y2). Selanjutnya, untuk membentuk persamaan kuadratik y = a0 + a1x + a2x2 diperlukan 3 buah titik, untuk membentuk persamaan kubik diperlukan empat titik, dan seterusnya. Secara umum untuk membentuk polinomial y = a0 + a1x + a2x2 + … + anxn diperlukan n + 1 titik.

Titik-titik tersebut disulihkan ke dalam persamaan polinom y, selanjutnya kita memperoleh sistem persamaan linier dan menyelesaikannya dengan metode eliminasi Gauss untuk memperoleh koefisien-koefisien polinom. Misalkan untuk

menginterpolasi dua buah titik dengan sebuah garis lurus y = a0 + a1x, maka dua buah titik yaitu (x0, yo) dan (x1, y1) disulihkan ke dalam persamaan garis menjadi:

$$y_1 = a_0 + a_1 x_1$$
$$y_2 = a_0 + a_1 x_2$$

Selanjutnya sistem persamaan linier diselesaikan dengan metode eliminasi untuk menentukan a0 dan a1. Semakin banyak jumlah titiknya maka sistem persamaan linier menjadi besar, namun metode eliminasi Gauss dapat diterapkan untuk mencari solusi sistem tersebut.

Skema (t, w) yang ditemukan oleh Adi Shamir dapat dituliskan algoritmanya sebagai berikut (Trapper, 2006):

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 secara acak t – 1 buah bilangan bulat dalam modulus p, misalkan s1, s2, …, st– 1, dan nyatakan polinomial:

$$s(x) = M + s_1 x + s_2 x^2 + \ldots + st - 1\, xt - 1 \,(mod\ p)$$

sedemikian sehingga s(0) = M (mod p). Sebagai catatan, p tidak perlu rahasia, tetapi polinom s(x) harus dirahasiakan.

3. Untuk w partisipan, kita pilih integer berbeda, x1, x2, …, xw (mod p),dan setiap orang memperoleh share (xi, yi) yang dalam hal ini yi = s(xi) (mod p). Untuk memudahkan perhitungan, misalkan untuk w orang kita memilih x1 = 1, x2 = 2, …, xw = w.

4. Misalkan t orang partisipan akan merekonstruksi M, dengan share masing-masing (x1, y1), (x2, y2) …, (xt, yt). Sulihkan setiap (xk, yk) ke dalam polinomial s(x) = M + s1x + s2x2 + … + st – 1 xt – 1 (mod p). Ini berarti:

5. Jika dimisalkan M = s0 maka kita dapat menulis ulang sistem persamaan ke dalam bentuk matriks:

Selesaikan sistem persamaan linier di atas dengan metode eliminasi Gauss untukmemperoleh s0 = M.

Untuk mengilustrasikan skema di atas, ambil contoh sebagai berikut. Misalkan ada w = 8 partisipan akan membagi secret M = 190503180520 dan mereka sepakat bahwa diperlukan t = 3 partisipan untuk melakukan rekonstruksi M. Misalkan dipilih bilangan prima p = 190503180520. Selanjutnya pilih 3 – 1 = 2 buah bilangan acak, sebut s1 = 482943028839 dan s2 = 1206749628665, untuk membentuk polinom s(x) = M + s1x + s2x2 (mod p), yaitu

$$s(x) = 190503180520 + 482943028839x + 1206749628665x^2 \ (mod\ 1234567890133\ )$$

Setiap partisipan memperoleh (x, s(x)). Misakan x1 = 1, x2 = 2, …, x8 = 8, maka, setiap orang memperoleh share:

(1, 645627947891)
(2, 1045116192326)
(3, 154400023692)
(4, 442615222255)
(5, 675193897882)
(6, 852136050573)
(7, 973441680328)
(8, 1039110787147)

Untuk merekonstruksi kembali secret M dibutuhkan paling sedikit 3 partisipan. Misalkan partisipan 2, 3, dan 7 ingin merekonstruksi M. Mereka perlu memecahkan sistem persamaan linier:

Dengan metode eliminasi Gauss sistem persamaan linier tersebut dapat dipecahkan dan solusinya adalah (M, s1, s2) = (190503180520, 482943028839, 1206749628665). Dengan kata lain secret M = 190503180520 dapat diperoleh kembali.

Nilai M tidak dapat ditemukan karena mustahil dua buah buah titik dapat membentuk polinom kuadratik s(x) = M + s1x + s2x2 (mod p). Misalkan mereka mencoba menggunakan titik ketiga yaitu (0, c) dengan c adalah sembarang secret, maka polinom unik yang melalui ketiga titik tersebut tetap tidak berhasil menemukan nilai M.

Sistem persamaan linier yang terbetuk memiliki lebih dari 3 persamaan dengan tiga peubah yang tidak diketahui, pada kondisi seperti ini sistem persamaan linier tetap dapat dipecahkan dan polinom interpolasi tetap bisa ditemukan! Dengan kata lain, minimal dibutuhkan 3 partisipan untuk bisa merekonstruksi M dengan skema (3, 8) tersebut.

IV. PENGAPLIKASIAN CHINESE REMAINDER THEOREM DALAM THRESHOLD SECRET SHARING

Seperti yang telah dijelaskan sebelumnya, ada beberapa jenis *threshold secret sharing* yang menggunakan aplikasi *chinese remainder theorem* untuk menentukan suatu rahasia, yaitu Mignotte's *threshold secret sharing* dan Asmuth-Bloom's *threshold secret sharing.*

Dalam Mignotte's *threshold secret sharing*, kita mendapat sejumlah n bagian rahasia I, di mana memunculkan sebuah sistem kongruensi :

$$S \equiv I_1 mod\ m_1$$
$$S \equiv I_2 mod\ m_2$$
$$\ldots\ldots\ldots$$
$$S \equiv I_n mod\ m_n$$

Dengan adanya sistem kongruensi tersebut, kita bisa menggunakan *chinese remainder theorem* untuk menentukan rahasia S, di mana hanya diperlukan sejumlah k bagian rahasia I saja untuk menentukan rahasia S.

Dalam Asmuth-Bloom's *threshold secret sharing*, kita juga

mendapat sejumlah n bagian rahasia I, di mana memunculkan sebuah sistem kongruensi :

$$S + X \times y \equiv I_1 mod\ m_1$$
$$S + X \times y \equiv I_2 mod\ m_2$$
$$\dots\dots\dots$$
$$S + X \times y \equiv I_n mod\ m_n$$

Dengan mengumpamakan S + X x y sebagai sebuah variabel seperti T, maka kita dapat menggunakan chinese remainder theorem untuk menentukan variabel T. Dan dengan ditemukan T, maka kita dapat menemukan rahasia S karena X dan y telah kita ketahui di awal.

Contoh persoalan :

Pada contoh ini, kita akan menggunakan Asmuth-Bloom *secret sharing*.

Misalkan kita memilik k = 3 dan n = 4, dengan rangkaian y = 3, m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19. Rahasia S adalah 2 dengan X adalah 51 yang telah memenuhi syarat Asmuth-Bloom's *threshold secret sharing*.

Maka kita bisa mendapat bagian rahasia I dengan cara :

$$T = S + X \times y = 155$$

$$I_1 = T\ mod\ m_1 = 1$$
$$I_2 = T\ mod\ m_2 = 12$$
$$I_3 = T\ mod\ m_3 = 2$$
$$I_4 = T\ mod\ m_4 = 3$$

Kita memilih sejumlah k bagian rahasia I, misalkan {1,12,2}. Dengan bagian rahasia tersebut, kita dapat menemukan bahwa rahasia S adalah 2.

Dengan *chinese remainder theorem*,

$$T \equiv 1\ mod\ 11$$
$$T \equiv 12\ mod\ 13$$
$$T \equiv 2\ mod\ 17$$

$$N = m_1 \times m_2 \times m_3 = 11 \times 13 \times 17 = 2431$$

$$221 \times 1 = 1\ mod\ 11$$
$$187 \times 8 = 1\ mod\ 13$$
$$143 \times 5 = 1\ mod\ 17$$

maka didapati,

$$T \equiv 1 \times 221 \times 1 + 12 \times 187 \times 8 + 2 \times 143 \times 5\ mod\ 2431$$
$$T \equiv 19603\ mod\ 2431$$
$$T \equiv 155\ mod\ 2431$$

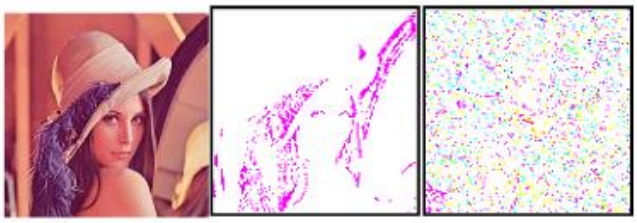
$$155 = S + X \times y$$
$$155 = S + 51 \times 3$$
$$S = 2$$

Pada hasil akhir, didapatkan rahasia S adalah 2.

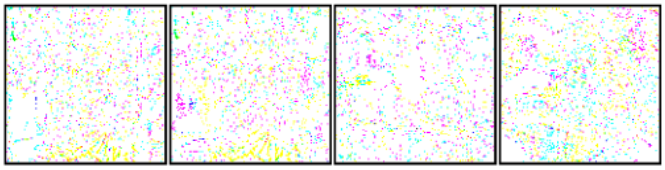
V. PENGAPLIKASIAN THRESHOLD SECRET SHARING

Seperti yang telah dijelaskan sebelumnya, threshold secret sharing merupakan metode untuk distribusi pembagian rahasia. Rahasia yang dimaksud bukan hanya berupa suatu bilangan atau suatu angka, namun juga bisa berupa tipe data lain.

Suatu gambar bisa dirahasiakan dengan metode secret sharing, seperti pada contoh berikut :



Gambar 2. Gambar yang telah diubah
(sumber :
http://shodhganga.inflibnet.ac.in/bitstream/10603/140312/12/12_chapter%204.pdf)



Gambar 3. Bagian – Bagian Gambar Rahasia
(sumber :
http://shodhganga.inflibnet.ac.in/bitstream/10603/140312/12/12_chapter%204.pdf)

Pembagian pada gambar di atas menggunakan Asmuth-Bloom *secret sharing*.

V. KESIMPULAN

Penggunaan metode *secret sharing* dapat diimplementasikan untuk distribusi akses kontrol sebuah grup atau perkumpulan dengan jumlah yang banyak. Terlebih untuk beberapa informasi atau rahasia yang penting, *secret sharing* merupakan salah satu metode yang bisa digunakan untuk mengontrol distribusi rahasia dari informasi tersebut.

VII. UCAPAN TERIMA KASIH

Pada kesempatan ini, penulis mengucapkan terima kasih kepada dosen yang telah mengajarkan mata kuliah IF2120 – Matematika Diskrit, terutama Dr. Judhi Santoso M.Sc. selaku dosen di kelas saya yang telah membimbing saya dalam menguasai mata kuliah Matematika Diskrit ini. Selain itu, penulis juga mengucapkan terima kasih kepada semua pihak

yang telah membantu dan mendukung pengerjaan makalah ini, baik secara langsung maupun tidak langsung.

REFERENSI

[1] Munir, Rinaldi, *Matematika Diskrit- Bahan Kuliah (Teori Bilangan)*, Bandung: Informatika Bandung, 2018.

[2] Oded Goldreich, Dana Ron dan Madhu Sudan, "Chinese Remaindering with Errors" , *IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330 – 1338.

[3] C.A. Asmuth and J. Bloom. "A modular approach to key safeguarding". *IEEE Transactions on Information Theory*, IT-29(2):208-210, 1983.

[4] Sorin Iftene. "General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting". *Electronic Notes in Theoretical Computer Science* (ENTCS). Volume 186, (July 2007). Pages 67–84. Year of Publication: 2007. ISSN 1571-0661

[5] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.5: The Chinese remainder theorem, pages 873-876.

[6] Ronald Cramer. Basic Secret Sharing (Lectures 1-2), Class Notes. October 2008, version 1.1.

[7] Shamir, Adi (1979), "How to share a secret", *Communications of the ACM*, 22 (11): 612–613.

[8] http://shodhganga.inflibnet.ac.in/bitstream/10603/140312/12/12_chapter%204.pdf diakses pada 10 Desember 2018 pukul 10.00 WIB

[9] https://catatankriptografi.wordpress.com/2012/05/11/skema-pembagian-data-rahasia-dari-shamir-bagian-1/ diakses pada 10 Desember 2018 pukul 10.50 WIB

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 10 Desember 2018

Suhailie – 13517045