Tạp chí Tin học và Điều khiển học, T.27, S.1 (2011), 253–262

MỞ RỘNG LƯỢC ĐỒ NGƯỠNG CỦA SHAMIR CHO VIỆC CHIA SẺ ĐỒNG THỜI NHIỀU BÍ MẬT

VŨ HUY HOÀNG[1], HỒ THUẦN[2]

[1] *Cục Cơ yếu 893 - Ban Cơ yếu Chính phủ*
[2] *Viện Công nghệ thông tin, Viện Khoa học và Công nghệ Việt Nam*

Abstract. Secret sharing schemes are important techniques in the key management in cryptography and distributed computation. In 1979, Shamir [6] proposed a threshold secret sharing scheme, in which one secret is divided into w pieces (shares) and delivered to w users such that only groups of t or more users ($t < w$) could cooperately reconstruct the secret.

In this paper, the main idea of the proposed secret sharing scheme is the use of the secrets to be shared as the coefficients of the polynomial $a(x)$. Numerical examples are given not only to illustrate the approach, but also show deeper comprehension of the method presented in [9].

Tóm tắt. Các lược đồ chia sẻ bí mật là những kỹ thuật quan trọng để quản lí khóa trong mật mã và trong tính toán phân tán. Năm 1979, Shamir [6] đề xuất một lược đồ chia sẻ bí mật ngưỡng, theo đó một bí mật được chia làm w mảnh và trao cho w người dùng, sao cho chỉ những nhóm t người dùng hay nhiều hơn ($t < w$) có thể hợp tác với nhau để khôi phục lại bí mật.

Ý tưởng chính của lược đồ chia sẻ bí mật được đề xuất trong bài báo này là việc sử dụng ngay các bí mật cần được chia sẻ làm các hệ số của đa thức $a(x)$. Những ví dụ được đưa ra ở đây ngoài việc minh họa cho chính cách tiếp cận mới của bài báo này, còn có ý nghĩa giúp hiểu sâu sắc hơn về phương pháp được trình bày trong [9].

1. ĐẶT VẤN ĐỀ

Chia sẻ bí mật là một công cụ quan trọng và được nghiên cứu rộng rãi trong mật mã và tính toán phân tán. Một lược đồ phân chia bí mật là một giao thức trong đó người điều hành D (điều phối) phân chia một bí mật thành những mảnh nhỏ được gọi là các phần chia và phân phối một cách bí mật cho một tập người tham gia hệ thống (thành viên) sao cho chỉ một số tập con xác định (gọi là các tập được quyền) là có thể khôi phục được bí mật đã phân chia. Vì vậy, cùng với sự phát triển của các kỹ thuật mật mã thì lược đồ chia sẻ bí mật được nghiên cứu và phát triển mạnh mẽ như các lược đồ được trình bày trong: L. Csirmaz [1], Farras O, Marti-Farré J, Padró C [2], J. Martí-Farré, C. Padró [3], hay phương pháp dãy độc lập được được giới thiệu bởi C. Blundo, A. De Santis, R. De Simone, U. Vaccaro trong [4] và được tổng quát hoá bởi Padró và Sáez trong [5].

Vào năm 1979, Shamir [6] đề xuất lược đồ chia sẻ bí mật (hay còn được gọi là phân chia bí mật) và được gọi là lược đồ ngưỡng của Shamir. Lược đồ ngưỡng Shamir cho một cách

chuyển một bí mật đơn thành w phần chia. Tuy nhiên trong trường hợp phân chia đồng thời t bí mật mà ta áp dụng t lần lược đồ Shamir rõ ràng là không hiệu quả, bởi vì với mỗi một khóa K đều phải thiết lập lại việc chia sẻ, dẫn đến tăng không gian lưu trữ và khối lượng tính toán.

Bài báo đề xuất sử dụng t bí mật k_j $(0 \leq j \leq t-1)$, để xây dựng một đa thức $a(x)$ có bậc tối đa là $t-1$ và sau đó tạo ra w phần chia bằng cách tìm giá trị của đa thức tại w điểm mới. Do đó lược đồ sẽ hiệu quả về không gian lưu trữ và khối lượng tính toán. Mỗi thành viên p_i sẽ có một điểm (x_i, y_i) trên đa thức. Việc sử dụng thêm một hàm băm và hệ mật RSA an toàn với số mũ giải mã lớn [8] ở đây nhằm làm tăng độ an toàn của lược đồ.

2. PHƯƠNG PHÁP CHIA SẺ NHIỀU BÍ MẬT SỬ DỤNG HỆ PHƯƠNG TRÌNH ĐẠI SỐ TUYẾN TÍNH

Giai đoạn khởi tạo

1. D chọn w phần tử khác nhau, khác không trong Z_p và kí hiệu là x_i $(1 \leq i \leq w)$. Với $i \leq i \leq w$ D sẽ trao giá trị x_i cho thành viên p_i. Các giá trị x_i là công khai.

Phân phối các mảnh

2. Giả sử D muốn phân chia t bí mật $k_j \in Z_p$ $(0 \leq j \leq t-1)$, trong đó p là số nguyên tố lớn và $t < w$. D sẽ chọn một cách ngẫu nhiên t phần tử phân biệt khác 0 của $Z_p \backslash \{x_1, x_2, ..., x_w\}$. Ký hiệu các phần tử đó là $\bar{x}_j$ với $(0 \leq j \leq t-1)$, và D tính $\bar{k}_j = k_j + h(\bar{x}_j)(\mod p)$, trong đó $(0 \leq j \leq t-1)$ và h là hàm băm.

3. D xây dựng đa thức $a(x)$ có bậc tối đa là $t-1$, trong đa thức này các hệ số $a_0, a_1, ..., a_{t-1}$ theo thứ tự tương ứng là $\bar{k}_0, \bar{k}_1, ..., \bar{k}_{t-1}$, với $(0 \leq j \leq t-1)$. Vì vậy đa thức $a(x)$ có thể viết như sau

$$a(x) = \bar{k}_0 + \bar{k}_1 x + ... + \bar{k}_{t-1} x^{t-1} (\mod p).$$

4. Tính đa thức $a(x)$ tại w điểm phân biệt $y_i = a(x_i)$ trong đó $(1 \leq i \leq w)$.

5. Các phần chia được cho bởi $(x_i, y_i),\ y_i = a(x_i)$, với $(1 \leq i \leq w)$.

Pha khôi phục

Để xây dựng lại t bí mật $k_j \in Z_p$, một tập được quyền những người tham gia có thể tính giá trị các khóa k_j như sau.

6. Sử dụng bất kỳ t phần chia nào có được từ bước 5 ở trên để tạo ra đa thức $a(x)$. Không làm mất tính tổng quát, giả sử chúng ta có t phần chia $(x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), ..., (x_{i_t}, y_{i_t})$, ta có hệ phương trình dưới dạng ma trận như sau

$$\begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 & ... & & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & ... & & x_{i_2}^{t-1} \\ ... & ... & ... & ... & ... & ... \\ 1 & x_{i_t} & x_{i_t}^2 & ... & & x_{i_t}^{t-1} \end{bmatrix} \begin{bmatrix} \bar{k}_0 \\ \bar{k}_1 \\ ... \\ \bar{k}_{t-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ ... \\ y_{i_t} \end{bmatrix}. \quad (1)$$

Vì ma trận các hệ số của hệ phương trình (1) là một ma trận Vandermonde nên luôn tồn tại nghịch đảo [7]. Do đó tính được $\bar{k}_0, \bar{k}_1, ..., \bar{k}_{t-1}$.

7. Người điều hành D sử dụng khóa công khai của thành viên p_{i_j} để mã hóa $\bar{x}_j$ theo công thức

$$\bar{c}_j = \bar{x}_j^{e_{i_j}} \mod n_{i_j},$$

trong đó e_{i_j}, n_{i_j} là khóa công khai của hệ mật RSA an toàn với số mũ giải mã lớn và $0 \le j \le t-1$.

Người điều hành D sẽ trao giá trị $\bar{c}_j$ cho thành viên p_{i_j} (về mặt cài đặt, có $t!$ cách mã hóa tập $\bar{x}_j$ để chuyển cho các thành viên tương ứng trong tập được quyền).

8. Mỗi thành viên $(0 \le j \le t-1)$ trong tập được quyền sẽ khôi phục giá trị $\bar{x}_j$ bằng cách tính

$$\bar{x}_j = \bar{c}_j^{d_{i_j}} \mod n_{i_j},$$

trong đó d_{i_j} là khóa bí mật của p_{i_j} và trao giá trị $\bar{x}_j$ tính được cho $t-1$ thành viên khác trong cùng tập được quyền.

9. Tập được quyền những người tham gia sử dụng $\bar{x}_j$ với $(0 \le j \le t-1)$ và các hệ số $\bar{k}_0, \bar{k}_1, ..., \bar{k}_{t-1}$ tính được từ bước 6 sẽ khôi phục được t khoá bí mật tương ứng là $k_0, k_1, ..., k_{t-1}$ bằng cách tính $k_j = \bar{k}_j - h(\bar{x}_j) (\mod p)$, với $(0 \le j \le t-1)$.

Để đánh giá, so sánh về độ phức tạp tính toán và khả năng tiết kiệm bộ nhớ của lược đồ đề xuất so với việc áp dụng nhiều lần lược đồ Shamir, trong [9] đã nghiên cứu, đưa ra các nhận xét và mệnh đề chứng minh việc Mở rộng lược đồ ngưỡng của Shamir cho việc chia sẻ đồng thời nhiều bí mật sẽ hiệu quả về không gian lưu trữ và khối lượng tính toán.

3. ỨNG DỤNG

Để minh họa các kết quả đã trình bày ở trên, ta xét một số ví dụ.

Ví dụ 1. Giả sử rằng $p = 809,\ t = 4,\ w = 6$ các toạ độ x công khai là $x_i = i,\ 1 \le i \le 6$. Bốn khoá cần chia sẻ $k_0 = 573,\ k_1 = 401,\ k_2 = 798,\ k_3 = 231$, và sử dụng hàm băm SHA-256, hệ mật RSA an toàn với số mũ giải mã lớn [8].

Áp dụng phương pháp sử dụng hệ phương trình tuyến tính như sau.

Giai đoạn khởi tạo

1. Chọn 6 phần tử khác nhau, khác không trong Z_p và kí hiệu là x_i. Ở đây để đơn giản, chọn $x_i = i + t$, với $1 \le i \le 6$. Trao các giá trị x_i cho p_i. Các giá trị x_i là công khai.

Phân phối các phần chia

2. Gán $\bar{x}_j = j$, với $(0 \le j \le 3)$ ta được $\bar{x}_0 = 0, \bar{x}_1 = 1, \bar{x}_2 = 2, \bar{x}_3 = 3$ và D tính $h(\bar{x}_0) = h(0)$

$= 433883212099411497594202361048882449582237669531742356572968063381374025953 05.$
$\bar{k}_0 = k_0 + h(\bar{x}_0)(\mod p) = 502.$
$h(\bar{x}_1) = h(1)$
$=4863546394320983479810981416129475392683997525756979530563709854272065892231 5.$
$\bar{k}_1 = k_1 + h(\bar{x}_1)(\mod p) = 150.$
$h(\bar{x}_2) = h(2)$
$=9609416164397606683336786797142615845823004849543027621779532866613333115986 1.$
$\bar{k}_2 = k_2 + h(\bar{x}_2)(\mod p) = 8.$
$h(\bar{x}_3) = h(3)$
$=3529321542678644715485769779836788470161467772717632509296534524868920532167 8.$
$\bar{k}_3 = k_3 + h(\bar{x}_3)(\mod p) = 276.$

3. Tạo đa thức $a(x)$, trong đa thức này các hệ số $a_0, a_1, ..., a_{t-1}$ theo thứ tự tương ứng là $\bar{k}_0, \bar{k}_1, ..., \bar{k}_{t-1}$, với $(0 \le j \le t-1)$. Ta có

$a(x) = \bar{k}_0 + \bar{k}_1 x + ... + \bar{k}_{t-1}x^{t-1}(\mod p) = 502 + 150x + 8x^2 + 276x^3(\mod 809).$

4. Tính $a(x)$ tại 6 điểm khác biệt đã được chọn ở bước 1, trong đó $y_i = a(x_i)$, $(1 \le i \le 6)$

$y_1 = a(5) = 356$, $y_2 = a(6) = 631$, $y_3 = a(7) = 341$, $y_4 = a(8) = 333$, $y_5 = a(9) = 645$, $y_6 = a(10) = 506$.

5. Các phần chia được cho bởi $(5, 356)$, $(6, 631)$, $(7, 341), (8, 333)$, $(9, 645), (10, 506)$, tương ứng với 6 phần chia cho 6 thành viên.

Pha khôi phục

6. Sử dụng bất kỳ 4 phần chia nào có được từ bước 5 ở trên để tạo ra đa thức a(x). Chẳng hạn, nếu sử dụng 4 phần chia (6, 631), (7, 341), (9, 645), (10, 506), sẽ thu được 4 phương trình tuyến tính 4 ẩn. Ta có thể viết dưới dạng ma trận như sau

$$\begin{bmatrix} 1 & 6 & 6^2 & 6^3 \\ 1 & 7 & 7^2 & 7^3 \\ 1 & 9 & 9^2 & 9^3 \\ 1 & 10 & 10^2 & 10^3 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 631 \\ 341 \\ 645 \\ 506 \end{bmatrix}.$$

Do đó tính được $a_0 = 502,\ a_1 = 150,\ a_2 = 8,\ a_3 = 276$ trong Z_p. Gán $\bar{k}_0 = a_0,\ \bar{k}_1 = a_1,\ \bar{k}_2 = a_2,\ \bar{k}_3 = a_3$.

7. Người điều hành D sử dụng khóa công khai của thành viên p_{i_j} để mã hóa $\bar{x}_j$ theo công thức $\bar{c}_j = \bar{x}_j^{l_{i_j}}$, trong đó $e_{i_j},\ n_{i_j}$ là khóa công khai của hệ mật RSA an toàn với số mũ giải mã lớn và $0 \le j \le t-1$, ta có

Khóa công khai của thành viên p_0 :

$n_0 = 21388778669,\ e_0 = 13$, với $\bar{x}_0 = 0$ ta có $\bar{c}_0 = 0$. Giá trị $\bar{c}_0$ người điều hành D sẽ trao cho thành viên p_0.

Khóa công khai của thành viên p_1 :

$n_1 = 69465342119,\ e_1 = 7$, với $\bar{x}_1 = 1$ ta có $\bar{c}_1 = 1$. Giá trị $\bar{c}_1$ người điều hành D sẽ trao cho thành viên p_1.

Khóa công khai của thành viên p_2 :

$n_2 = 30639320424421,\ e_2 = 5$, với $\bar{x}_2 = 2$ ta có $\bar{c}_2 = 32$. Giá trị $\bar{c}_2$ người điều hành D sẽ trao cho thành viên p_2.

Khóa công khai của thành viên p_3 :

$n_3 = 92411498779,\ e_3 = 7$, với $\bar{x}_3 = 3$ ta có $\bar{c}_3 = 2187$. Giá trị $\bar{c}_3$ người điều hành D sẽ trao cho thành viên p_3.

8. Mỗi thành viên p_{i_j} $(0 \le j \le t-1)$ trong tập được quyền sẽ khôi phục giá trị $\bar{x}_j$ bằng cách tính $\bar{x}_j = \bar{c}_j^{d_{i_j}} \mod n_{i_j}$, trong đó d_{i_j} là khóa bí mật của p_{i_j}.

Khóa bí mật của thành viên p_0 :

$d_0 = 9871313029$, với $\bar{c}_0 = 0$ ta có $\bar{x}_0 = 0$ và trao giá trị $\bar{x}_0$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_1 :

$d_1 = 39694131223$, với $\bar{c}_1 = 1$, ta có $\bar{x}_1 = 1$ và trao giá trị $\bar{x}_1$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_2 :

$d_2 = 6127861858729$, với $\bar{c}_2 = 32$, ta có $\bar{x}_2 = 2$ và trao giá trị $\bar{x}_2$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_3 :

$d_3 = 52805065783$, với $\bar{c}_3 = 2187$, ta có $\bar{x}_3 = 3$ và trao giá trị $\bar{x}_3$ cho 3 thành viên khác trong cùng tập được quyền.

9. Sử dụng các giá trị $\bar{k}_0 = a_0,\ \bar{k}_1 = a_1,\ \bar{k}_2 = a_2,\ \bar{k}_3 = a_3$ có được từ bước 6 và thay $\bar{x}_0, \bar{x}_1, \bar{x}_2, \bar{x}_3$ vào công thức $k_j = \bar{k}_j - h(\bar{x}_j) \pmod p,\ (0 \le j \le t-1)$ để khôi phục các khoá k_0, k_1, k_2, k_3. Ta có $k_0 = 573,\ k_1 = 401,\ k_2 = 798,\ k_3 = 231$.

Ví dụ 2. Giả sử rằng

$p = 763976375864056784716823659532567468486534398245367198245 61$,

$t = 4,\ w = 6$, các toạ độ x công khai là $x_i = i,\ 1 \le i \le 6$. Bốn khoá cần chia sẻ:

$k_0 = 96746848653439824536823619824379595762349324 0983457$,

$k_1 = 30983464289957967468486534398262349324153895125674 01$,

$k_2 = 54984307825796746848653435760439826767935423079 8$,

$k_3 = 75342109867382361982437952453695762349054231 5$,

và sử dụng hàm băm SHA-256, hệ mật RSA an toàn với số mũ giải mã lớn [8].

Áp dụng phương pháp sử dụng hệ phương trình tuyến tính như sau:

Giai đoạn khởi tạo

1. Chọn 6 phần tử khác nhau, khác không trong Z_p và kí hiệu là x_i. Ở đây để đơn giản, chọn $x_i = i + t$, với $1 \le i \le 6$. Trao các giá trị x_i cho p_i. Các giá trị x_i là công khai.

Phân phối các phần chia

2. Gán $\bar{x}_j = j$, với $(0 \le j \le 3)$ ta được $\bar{x}_0 = 0,\ \bar{x}_1 = 1,\ \bar{x}_2 = 2,\ \bar{x}_3 = 3$ và D tính

$h(\bar{x}_0) = h(0)$
$= 433883212099411497594202361048882449582237669531742356572968063381374025953 05.$
$\bar{k}_0 = k_0 + h(\bar{x}_0)(\mod p)$
$= 375601078823190147890928855672094897201010244791442155531 13.$
$h(\bar{x}_1) = h(1)$
$=486354639432098347981098141612947539268399752575697953056370985427206589223 15.$
$\bar{k}_1 = k_1 + h(\bar{x}_1)(\mod p)$
$= 332706132906270673870944150337472909664052776535045016561 82.$
$h(\bar{x}_2) = h(2)$
$=960941616439760668333678679714261584582300484954302762177953286661333311598 61.$
$\bar{k}_2 = k_2 + h(\bar{x}_2)(\mod p)$
$=130004412943799208026295241383183188302312589872565003087 18.$
$h(\bar{x}_3) = h(3)$
$=352932154267864471548576977983678847016146777271763250929653452486892053216 78.$
$\bar{k}_3 = k_3 + h(\bar{x}_3)(\mod p)$
$= 604298138320024785965115669412780319919572714598105222717 12.$

3. Tạo đa thức $a(x)$, trong đa thức này các hệ số $a_0, a_1, ..., a_{t-1}$ theo thứ tự tương ứng là $\bar{k}_0, \bar{k}_1, ..., \bar{k}_{t-1}$, với $(0 \leq j \leq t-1)$. Ta có

$a(x) = \bar{k}_0 + \bar{k}_1 x + ... + \bar{k}_{t-1} x^{t-1}(\mod p).$
$= 375601078823190147890928855672094897201010244791442155531 13$
$+ 332706132906270673870944150337472909664052776535045016561 82.x$
$+130004412943799208026295241383183188302312589872565003087 18.x^2$
$+604298138320024785965115669412780319919572714598105222717 12\ .x^3$
$(\mod\ 763976375864056784716823659532567468486534398245367198245 61).$

4. Tính $a(x)$ tại 6 điểm khác biệt đã được chọn ở bước 1, trong đó $y_i = a(x_i)$, $(1 \leq i \leq 6)$:

$y_1 = a(5) = 608989891226659568276005067616994951939566383280389339370 68.$
$y_2 = a(6) = 646469638327181994999483247899319091200948084386847887286 5.$
$y_3 = a(7) = 143707317653677569449583696677437642386902988003616711200 22.$
$y_4 = a(8) = 652077903289402470331486902093356728824755218336980451860 06.$
$y_5 = a(9) = 631689295475700909635410000318966277031881397555204157537 23.$
$y_6 = a(10) = 652424820676494464284752369700678332579580220265450371552 01.$

5. Các phần chia được cho bởi:

(5, 608989891226659568276005067616994951939566383280389339370 68),
(6, 646469638327181994999483247899319091200948084386847887286 5),
(7, 143707317653677569449583696677437642386902988003616711200 22),
(8, 652077903289402470331486902093356728824755218336980451860 06),
(9, 631689295475700909635410000318966277031881397555204157537 23),
(10, 652424820676494464284752369700678332579580220265450371552 01),

tương ứng với 6 phần chia cho 6 thành viên.

Pha khôi phục

6. Sử dụng bất kỳ 4 phần chia nào có được từ bước 5 ở trên để tạo ra đa thức $a(x)$. Chẳng hạn, nếu sử dụng 4 phần chia

(6, 64646963832718199499948324789931909120094808438684788728 65),

(7, 14370731765367756944958369667743764238690298800361671120022),

(9, 631689295475700909635410000318966277031881397555204157537 23),

(10, 65242482067649446428475236970067833257958022026545037155201),

sẽ thu được 4 phương trình tuyến tính 4 ẩn. Ta có thể viết dưới dạng ma trận như sau

$$\begin{bmatrix} 1 & 6 & 6^2 & 6^3 \\ 1 & 7 & 7^2 & 7^3 \\ 1 & 9 & 9^2 & 9^3 \\ 1 & 10 & 10^2 & 10^3 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} y_2 \\ y_3 \\ y_5 \\ y_6 \end{bmatrix}.$$

Do đó tính được:

a_0 = 375601078823190147890928855672094897201010244791442155531 13,

a_1 = 332706132906270673870944150337472909664052776535045016561 82,

a_2 = 130004412943799208026295241383183188302312589872565003087 18,

a_3 = 604298138320024785965115669412780319919572714598105222717 12,

trong Z_p. Gán $\bar{k}_0 = a_0,\ \bar{k}_1 = a_1,\ \bar{k}_2 = a_2,\ \bar{k}_3 = a_3$.

7. Người điều hành D sử dụng khóa công khai của thành viên p_{i_j} để mã hóa $\bar{x}_j$ theo công thức $\bar{c}_j = \bar{x}_j^{l_{i_j}} \mod n_{i_j}$, trong đó $e_{i_j},\ n_{i_j}$ là khóa công khai của hệ mật RSA an toàn với số mũ giải mã lớn và $0 \le j \le t-1$, ta có:

Khóa công khai của thành viên p_0 :

n_0 =

34986293162227433508179884910771498007562415976011686787890685604000003452300 5

05611687608699774193634182361065614157997836926202066216221867256173128701445 40

34693276303454101111284910920308344107617062585909958358015607766995730712541 69

58420423765180862105609891592199585348255065212002686049246879082717832178729 21

40115387314294227188690548308214917109297220172115628258566418070312550083727 88

65713028392511,

e_0 = 43556142965880123323311949751266331066371,

với $\bar{x}_0 = 0$ ta có $\bar{c}_0 = 0$. Giá trị $\bar{c}_0$ người điều hành D sẽ trao cho thành viên p_0.

Khóa công khai của thành viên p_1 :

$n1$ =

16741052714908875472710492356658305321461117149867075679832815473479254155906277 36936092804434677263426518338194570485695836377211407086402207264713236176841341 86060800875925792056191182046449356174317225732587969985552452125946088740873204 75071523131147437107746432526311105614854444616601891168042114908939018916139429 28241023956508398550498803775887759566676 17,

$e_1 = 7922816251426433759354395033 7$,

với $\bar{x}_1 = 1$ ta có $\bar{c}_1 = 1$. Giá trị $\bar{c}_1$ người điều hành D sẽ trao cho thành viên p_1.

Khóa công khai của thành viên p_2 :

$n_2 =$

605868340493056480944814923207766156962808672145327834178110073801299573195494133539145972097263875123308026982504390825384275488264784047940355407411697288211470789482969787752017455937768103962241942251000766239092675526114537817213581800235801254356841148492402835051319065183390472086340132822873935583552883961576464516107907,

$e_2 = 1180591620717411303427$,

với $\bar{x}_2 = 2$ ta có

$\bar{c}_2 =$

389562692045860855174461162819000441450232370149664549247334010630671256352673847125859297060640434449501390056806379421240960356832342775778270655484773018908356992320174742677192056554017862377954650372249486235555955527030094220693567618416152832482417001489213240280758509427090612291145048453265123588781633633486786200422228.

Giá trị $\bar{c}_2$ người điều hành D sẽ trao cho thành viên p_2.

Khóa công khai của thành viên p_3 :

$n_3 =$

690521750900152492791455692246237796556979441950841671201369251631974253255171502868469689601387297110754491745684686826739779131085873712937863816923566053469472343302526506835150424961940846703659685993863558252245322380955420387252923784279847596240607988619126588794547291397386193070485500597997955307,

$e_3 = 1099511627777$,

với $\bar{x}_3 = 3$ ta có

$\bar{c}_3 =$

446284346279724811998304778241750908835925780563255127357335072065751980517003500968629828085046403756611811444790620307670993419228795995178171958042740126986324511470237323221930891977152165914653171837178156810145674908863384280186434167612577890964179973205789622891194522644319468371358813216413400791.

Giá trị $\bar{c}_3$ người điều hành D sẽ trao cho thành viên p_3.

8. Mỗi thành viên p_{i_j} $(0 \le j \le t-1)$ trong tập được quyền sẽ khôi phục giá trị $\bar{x}_j$ bằng cách tính $\bar{x}_j = \bar{c}_j^{d_{i_j}} \mod n_{i_j}$, trong đó d_{i_j} là khóa bí mật của p_{i_j}.

Khóa bí mật của thành viên p_0 :

$d_0 =$

344833362991899974678582683076712194792791636475628486351442074827610972616390269519234436579546537458481932503412954095366041244733436258144278700448825174512894629315764933099984875703597280800654670632918902564608391909159588335991945180846

618313426190663917701649085519992489219205098002455262379602440389930145283361626
403115124055682812369184128091575615011997883134960539695008729187176342261733831
731,

với $\bar{c}_0 = 0$ ta có $\bar{x}_0 = 0$ và trao giá trị $\bar{x}_0$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_1 :

$d_1 =$

113228074442598180399082868023946275100863247065714145510633086802749059342279345
323791919081307706476224370724372680817429941767482604911851892136848822463884822
287418231051983690671641316069839330375342956570649788916359077528609250317442991
429516747500457385654739926551522091273370106075550049286732372788354031840115650
244263610899893349356963359467031098073,

với $\bar{c}_1 = 1$ ta có $\bar{x}_1 = 1$ và trao giá trị $\bar{x}_1$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_2 :

$d_2 =$

462571949181683172070596956115702449017068233031081289312549625337970537054116972 4
390360195171184419285992575872982502674890633023412713252119669168290448145566109 9
719953509209706132201629805112485422149207373669417156513761930742631220425723431 3
411959150922235387084797502954716320487104964342692035808499541167037857668392458603,

với $\bar{c}_2 =$

389562692045860855174461162819000441450232370149664549247334010630671256352673847 1
258592970606404344495013900568063794212409603568323427757782706554847730189083569 9
232017474267719205655401786237795465037224948623555595552703009422069356761841615 2
832482417001489213240280758509427090612291145048453265123588781633633486786200422228,

ta có $\bar{X}_2 = 2$ và trao giá trị $\bar{X}_2$ cho 3 thành viên khác trong cùng tập được quyền.

Khóa bí mật của thành viên p_3 :

$d_3 =$

600632386092574533800606728179818494568151668560161751246802485069341963732107666 6
731402353553658646376773795094358811073078615000512583032568384907657882610491708 6
280279462502648269922054587450129504897064468943126882030695271502422987161289678 9
211666332177739542027693739491478351849727989379758218895353,

với $\bar{c}_3 =$

446284346279724811998304778241750908835925780563255127357335072065751980517003500 9
686298280850464037566118114447906203076709934192287959951781719580427401269863245 1
147023732322193089197715216591465317183717815681014567490886338428018643416761257 7
890964179973205789622891194522644319468371358813216413400791,

ta có $\bar{X}_3 = 3$ và trao giá trị $\bar{X}_3$ cho 3 thành viên khác trong cùng tập được quyền.

9. Sử dụng các giá trị $\bar{k}_0 = a_0,\ \bar{k}_1 = a_1,\ \bar{k}_2 = a_2,\ \bar{k}_3 = a_3$ có được từ bước 6 và thay $\bar{x}_0,\ \bar{x}_1,\ \bar{x}_2,\ \bar{x}_3$ vào công thức $k_j = (\bar{k}_j - h(\bar{x}_j)) \mod p,\ (0 \le j \le t-1)$ để khôi phục các khoá k_0, k_1, k_2, k_3. Ta có:

k_0 = 967468486534398245368236198243795957623493240983457,
k_1 = 309834642899579674684865343982623493241538951256740 1,
k_2 = 549843078257967468486534357604398267687935423079 8,
k_3= 753421098673823619824379524536957623490542315.

4. KẾT LUẬN

Phương pháp chia sẻ nhiều bí mật được đề xuất này là một cải tiến từ lược đồ ngưỡng của Shamir. Phương pháp này có thể được áp dụng để chia sẻ nhiều bí mật cùng một lúc, tiết kiệm được không gian lưu trữ và khối lượng tính toán, phù hợp với việc phân phối nhiều khóa khi sử dụng mật mó để bảo vệ thụng tin.

TÀI LIỆU THAM KHẢO

[1] L. Csirmaz, Secret sharing schemes on graphs, *Studia Scientiarum Mathematicarum Hungarica, Akadộmiai Kiadú* **44** (3) (September 2007) 297–306.

[2] O. Farras, J. Marti-Farré, C. Padró, Ideal multipartite secret sharing schemes, Advances in cryptology, Eurocrypt 2007, *Conference on the theory and applications of cryptographic techniques*, Springer, 2007 (448–465).

[3] J. Martí-Farré, C. Padró, Secret sharing schemes with three or four minimal qualified subsets, *Designs Codes Cryptography* **34** (2005) 17–34.

[4] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Designs Codes Cryptography* **11** (1997) 107–122.

[5] C. Padró, G. Sáez, Secret sharing schemes with bipartite access structure, *IEEE Trans. Inform. Theory* **46** (7) (2000) 2596–2604.

[6] A. Shamir, How to share a secret, *Communications of the ACM* **22** (11) (1979) 612–613.

[7] D.R. Stinson, *Cryptography: Theory and practice*, CRC Press. Boca Raton, 2002.

[8] Vũ Huy Hoàng, Hồ Thuần, Một phương pháp đơn giản xây dựng hệ RSA an toàn với số mũ giải mã lớn, *Tạp chí Nghiên cứu Khoa học và Công nghệ Quân sự* **11** (2) (2011) 73–80.

[9] Vũ Huy Hoàng, Nguyễn Đăng Khoa, Phương pháp chia sẻ bí mật hiệu quả, *Tạp chí Công nghệ Thông tin và Truyền thông: Các công trình nghiên cứu, phát triển và ứng dụng Công nghệ Thông tin và Truyền thông* **V-1, 3** (23) (2010) 55–60.

Nhận bài ngày 30 - 3 - 2011
Nhận lại sau sửa ngày 21 - 10 -2011