MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong các giao dịch điện tử, chữ ký số được sử dụng nhằm đáp ứng yêu cầu chứng thực về nguồn gốc và tính toàn vẹn của thông tin. Các mô hình ứng dụng chữ ký số hiện tại cho phép đáp ứng tốt các yêu cầu về chứng thực nguồn gốc thông tin được tạo ra bởi những thực thể có tính độc lập. Tuy nhiên, khi mà các thực thể tạo ra thông tin là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, hệ thống kỹ thuật,...) thì nguồn gốc thông tin ở cấp độ tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận lại không được chứng thực. Hiện tại, có thể chưa được đặt ra yêu cầu có tính cấp thiết về vấn đề này, nhưng trong một tương lai không xa, khi Chính phủ điện tử và Thương mại điện tử cùng với hạ tầng công nghệ thông tin và truyền thông đã phát triển mạnh mẽ thì nhu cầu ứng dụng chữ ký số với các yêu cầu đặt ra như thế sẽ là tất yếu.

Xuất phát từ thực tế đó, NCS đã chọn đề tài "**Nghiên cứu, phát triển các lược đồ chữ ký sô tập thể**" với mong muốn có những đóng góp vào sự phát triển khoa học và công nghệ chung của đất nước.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của Luận án bao gồm:

- Cơ sở của các hệ mật khóa công khai và các lược đồ chữ ký số.
- Nguyên lý xây dựng các hệ mật khóa công khai và lược đồ chữ ký số.
- Các mô hình ứng dụng mật mã khóa công khai và chữ ký số.

Phạm vi nghiên cứu của Luận án bao gồm:

- Hệ mật khóa công khai RSA, hệ mật ElGamal, chuẩn chữ ký số GOST R34.10-94 của Liên bang Nga và các cơ sở toán học liên quan.
- Phương pháp mã hóa và giải mã, phương pháp hình thành và kiểm tra chữ ký số.

3. Mục tiêu nghiên cứu

- Đề xuất mô hình ứng dụng chữ ký số nhằm đáp ứng các yêu cầu đặt ra khi triển khai một Chính phủ điện tử trong thực tế xã hội, áp dụng phù hợp cho đối tượng là các tổ chức, cơ quan hành chính, các doanh nghiệp,....
- Phát triển một số lược đồ chữ ký số theo mô hình đã đề xuất.

4. Phương pháp nghiên cứu

- Phát triển một số lược đồ cơ sở dựa trên các hệ mật và các chuẩn chữ ký số được đánh giá có độ an toàn cao, sử dụng các lược đồ này làm cơ sở để xây dựng các lược đồ chữ ký số theo mục tiêu nghiên cứu đặt ra.
- Xây dựng một số lược đồ chữ ký tập thể theo mô hình ứng dụng mới đề xuất có khả năng ứng dụng trong thực tiễn.

5. Nội dung nghiên cứu

- Các hệ mật RSA, hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-

94 của Liên bang Nga.

- Phát triển một số lược đồ cơ sở dựa trên hệ mật RSA, hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94.
- Xây dựng một số lược đồ chữ ký số dựa trên các lược đồ cơ sở theo mô hình ứng dụng mới đề xuất.

6. Ý nghĩa khoa học và thực tiễn

- Mô hình chữ ký số tập thể được đề xuất trên cơ sở các yêu cầu đặt ra cho việc chứng thực các văn bản, tài liệu,... trong các thủ tục hành chính ở các tổ chức, cơ quan, các doanh nghiệp,... khi triển khai một Chính phủ điện tử trong thực tế xã hội.
- Các lược đồ chữ ký tập thể được đề xuất ở đây có tính ứng dụng thực tế, khả thi và không vi phạm về vấn đề bản quyền.

7. Bố cục của luận án

Luận án bao gồm 3 chương cùng với các phần Mở đầu, Kết luận và Danh mục các công trình, bài báo đã được công bố của tác giả liên quan đến các vấn đề nghiên cứu của Luận án.

Chương 1: Khái quát về mô hình chữ ký số tập thể và hướng nghiên cứu của đề tài.

Trình bày một số khái niệm và thuật ngữ liên quan đến các nội dung nghiên cứu và được sử dụng trong Luận án. Định hướng nghiên cứu của đề tài Luận án. Đề xuất mô hình ứng dụng chữ ký số phù hợp cho các yêu cầu thực tế đặt ra.

Chương 2: Phát triển các lược đồ chữ ký số tập thể dựa trên hệ mật RSA.

Trình bày tổng quan về hệ mật RSA: phương pháp hình thành khóa, phương pháp mã hóa và giải mã thông tin, phương pháp hình thành và kiểm tra chữ ký, phân tích cơ sở xây dựng, mức độ an toàn của hệ mật RSA, từ đó đề xuất lược đồ chữ ký số làm cơ sở để xây dựng và phát triển các lược đồ chữ ký số tập thể. Xây dựng 3 lược đồ chữ ký số tập thể theo mô hình chữ ký số đã được đề xuất ở Chương 1.

Chương 3: Phát triển các lược đồ chữ ký số tập thể dựa trên hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94.

Trình bày tổng quan về hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94 của Liên bang Nga: phương pháp hình thành khóa, phương pháp hình thành và kiểm tra chữ ký, phân tích cơ sở xây dựng và mức độ an toàn của hệ mật ElGamal và GOST R34.10-94. Đề xuất 2 lược đồ cơ sở dựa trên hệ mật ElGamal và GOST R34.10-94, từ đó phát triển 6 lược đồ chữ ký số tập thể theo mô hình mới đề xuất.

CHƯƠNG 1
KHÁI QUÁT VỀ MÔ HÌNH CHỮ KÝ SỐ TẬP THỂ VÀ HƯỚNG NGHIÊN CỨU CỦA ĐỀ TÀI

1.1 Hướng nghiên cứu của đề tài Luận án

Trên thực tế, nhiều khi một thực thể ký (con người, thiết bị kỹ thuật,...) là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, hệ thống kỹ thuật,...) và thông điệp dữ liệu (bản tin, thông báo, tài liệu,...) được thực thể ký tạo ra với tư cách là một thành viên hay bộ phận của tổ chức đó. Trong trường hợp này, thông tin không chỉ có nguồn gốc từ thực thể (ký) tạo ra nó, mà còn có nguồn gốc từ tổ chức mà ở đó thực thể ký là một thành viên hay bộ phận của tổ chức này. Vấn đề ở đây là, thông tin cần phải được chứng thực về nguồn gốc và tính toàn vẹn ở 2 cấp độ: cấp độ *cá nhân thực thể ký* và cấp độ *tổ chức* mà thực thể ký là một thành viên hay bộ phận của nó. Các mô hình ứng dụng chữ ký số hiện tại chủ yếu mới chỉ đảm bảo cho nhu cầu chứng thực thông tin ở cấp độ cá nhân của thực thể ký, còn việc chứng thực đồng thời ở cả 2 cấp độ như thế hiện tại vẫn chưa được đặt ra. Có thể là, một yêu cầu như vậy chưa thực sự cần thiết được đặt ra ở thời điểm hiện tại, nhưng rõ ràng đó sẽ là nhu cầu thực tế và ngày càng trở nên cần thiết trong bối cảnh Chính phủ điện tử, Thương mại điện tử hay nói chung là các giao dịch điện tử đang được phát triển với qui mô toàn cầu.

Từ những phân tích trên đây, hướng nghiên cứu của đề tài Luận án là đề xuất mô hình ứng dụng chữ ký số, được gọi là mô hình *chữ ký số tập thể*, nhằm đáp ứng cho các yêu cầu chứng thực nguồn gốc và tính toàn vẹn thông tin ở nhiều cấp độ khác nhau và xây dựng các lược đồ chữ ký số theo mô hình mới đề xuất nhằm đáp ứng tốt các yêu cầu mà thực tiễn đặt ra.

1. 2 Mô hình chữ ký số tập thể

Mô hình chữ ký số tập thể được đề xuất có cấu trúc cơ bản của một PKI truyền thống với thiết kế bổ sung nhằm bảo đảm đồng thời các chức năng về *chứng thực số* cho một tổ chức (đơn vị hành chính, hệ thống kỹ thuật,...) với các hỗ trợ về an toàn bảo mật thông tin và khả năng liên kết các tổ chức với nhau trong các dịch vụ chứng thực số. Trong mô hình này, thực thể ký là thành viên của một tổ chức và được phép ký lên các thông điệp dữ liệu với danh nghĩa thành viên của tổ chức này. Ngoài ra, các thực thể ký có thể hợp tác với nhau để hình thành các nhóm ký trong trường hợp một thông điệp dữ liệu cần được ký bởi một số thành viên của tổ chức đó. Cũng trong mô hình này, Cơ quan chứng thực – CA (Certificate Authority) là bộ phận chức năng có nhiệm vụ bảo đảm các dịch vụ chứng thực số, như: chứng nhận một thực thể là thành viên của tổ chức, chứng thực chữ ký số cá nhân của một thực thể hay đa chữ ký của một nhóm ký trong việc hình thành chữ ký tập thể...

1. 3 Lược đồ chữ ký số tập thể

Một lược đồ chữ ký số xây dựng theo mô hình mới đề xuất bao gồm các thành phần cơ bản như sau:

- Thuật toán hình thành các tham số hệ thống và khóa.
- Thuật toán chứng nhận và kiểm tra tính hợp pháp của đối tượng ký.
- Thuật toán hình thành và kiểm tra chữ ký cá nhân.
- Thuật toán hình thành và kiểm tra chữ ký tập thể.
- Thuật toán mã hóa và giải mã thông tin.

Ở đây, thuật toán mã hóa và giải mã thông tin không phải là yêu cầu bắt buộc đối với các lược đồ chữ ký tập thể. Nó chỉ cần thiết trong các ứng dụng thực tế, mà ở đó vấn đề bảo mật cho các thông điệp dữ liệu được đặt ra.

1.4 Kết luận Chương 1

Các kết quả đã đạt được ở Chương 1 bao gồm:

- Thống nhất một số khái niệm và thuật ngữ liên quan được sử dụng trong Luận án.
- Đề xuất mô hình ứng dụng cho các lược đồ chữ ký số có thể áp dụng cho các tổ chức xã hội như: các cơ quan hành chính nhà nước, các doanh nghiệp,... nhằm bảo đảm việc chứng thực cho các thông điệp dữ liệu trong các giao dịch điện tử (Chính phủ điện tử, Thương mại điện tử,...) phù hợp với việc chứng thực các văn bản, tài liệu,... trong các thủ tục hành chính thực tế hiện nay.

CHƯƠNG 2
PHÁT TRIỂN CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ DỰA TRÊN HỆ MẬT RSA

2.1 Lược đồ cơ sở - LD 1.01

2.1.1 Phương pháp hình thành các tham số hệ thống và khóa

a) Hình thành các tham số hệ thống

1- Sinh 2 số nguyên tố *p* và *q* lớn, mạnh;

2- Tính *modulo n* theo công thức: $n = p \times q$;

3- Chọn giá trị t thỏa mãn: $m/2 < t < \phi(n)$, với: $\phi(n) = (p-1)\times(q-1)$ và $m < \phi(n)$;

4- Lựa chọn hàm băm $H : \{0,1\}^* \mapsto Z_m$.

b) Hình thành khóa

1- Chọn khóa bí mật (x) thỏa mãn: $1 < x < n$, $\gcd(x,n) = 1$;

2- Tính khóa công khai (y) theo công thức: $y = (x)^{-t} \bmod n$

c) Bí mật và công khai các tham số

1- Bí mật các tham số: p, q, x.

2- Công khai các tham số: n, t.

3- Chứng nhận y bởi một Cơ quan chứng thực – CA (Certificate Authority) tin cậy.

2.1.2 Phương pháp hình thành và kiểm tra chữ ký

a) Thuật toán hình thành chữ ký

Dữ liệu vào: Thông điệp dữ liệu cần ký M; khóa bí mật *x* của đối tượng ký.

Kết quả đầu ra: chữ ký số (R,S).

Thuật toán bao gồm các bước:

1- Tính: $R = k^t \bmod n$, với: $k = H(x \| M)$

2- Tính: $E = H(R \| M)$

3- Tính: $S = k \times (x)^E \bmod n$

b) Thuật toán kiểm tra chữ ký

Dữ liệu vào: Thông điệp dữ liệu M; chữ ký (R,S); khóa công khai *y* của đối tượng ký.

Kết quả đầu ra: khẳng định về tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước:

1- Tính: $E = H(R \| M)$

2- Tính: $\overline{R} = S^t \times y^E \bmod n$

3- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

2.2 Lược đồ chữ ký số đơn - LD 1.02

2.2.1 Phương pháp hình thành các tham số hệ thống và khóa

a) Thuật toán hình thành các tham số hệ thống

Tương tự như lược đồ LD 1.01.

b) Thuật toán hình thành khóa

+ Hình thành khóa của CA:

1- Chọn khóa bí mật (x_{ca}) thỏa mãn: $1 < x_{ca} < n$, $\gcd(x_{ca}, n) = 1$;

2- Tính khóa công khai (y_{ca}) theo công thức: $y_{ca} = (x_{ca})^{-t} \bmod n$.

+ Hình thành khóa của các đối tượng ký U_i (*i = 1,2,...*):

1- Chọn khóa bí mật (x_i) thỏa mãn: $1 < x_i < n$, $\gcd(x_i, n) = 1$;

2- Tính khóa công khai (y_i) theo công thức: $y_i = (x_i)^{-t} \bmod n$.

2.2.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

a) Thuật toán chứng nhận đối tượng ký

Dữ liệu vào: Khóa công khai y_i và thông tin nhận dạng ID_i của U_i, khóa bí mật x_{ca} của CA.

Kết quả đầu ra: (u_i, v_i) là chứng nhận của CA đối với U_i.

Thuật toán bao gồm các bước:

1- Tính: $u_i = (H(x_{ca} \| y_i \| ID_i))^t \bmod n$

2- Tính: $t_i = H(u_i \| y_i \| ID_i)$

3- Tính: $v_i = \left(H(x_{ca} \| y_i \| ID_i) \times (x_{ca})^{t_i}\right) \bmod n$

4- Công khai (u_i, v_i) là chứng nhận của CA đối với U_i.

b) Thuật toán kiểm tra tính hợp pháp của đối tượng ký

Dữ liệu vào: Khóa công khai y_i, ID_i của U_i, (u_i, v_i), khóa công khai

y_{ca} của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chứng nhận (u_i,v_i).

Thuật toán bao gồm các bước:

1- Tính: $t_i = H(u_i \| y_i \| ID_i)$

2- Tính: $\overline{u}_i = (v_i)^t \times (y_{ca})^{t_i} \bmod n$

3- Kiểm tra nếu $\overline{u}_i = u_i$ thì (u_i,v_i) hợp lệ, do đó tính hợp pháp của đối tượng ký U_i và tính toàn vẹn của y_i được công nhận.

2.2.3 Phương pháp hình thành và kiểm tra chữ ký số tập thể

a) Thuật toán hình thành chữ ký số tập thể

Dữ liệu vào: Thông điệp dữ liệu cần ký M, khóa bí mật x_i của U_i , khóa bí mật x_{ca} của CA.

Kết quả đầu ra: (R,S) là chữ ký tương ứng với M.

Thuật toán bao gồm các bước:

1- U_i tính: $R_i = (k_i)^t \bmod n$, với: $k_i = H(x_i \| M)$

2- CA tính: $R_{ca} = (k_{ca})^t \bmod n$, với: $k_{ca} = H(x_{ca} \| M)$

3- CA tính: $R = R_i \times R_{ca} \bmod n$

4- CA tính: $E = H(R \| M)$ và gửi cho đối tượng ký U_i

5- U_i tính: $S_i = k_i \times (x_i)^E \bmod n$ và gửi cho CA.

6- CA kiểm tra chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu chữ ký cá nhân hợp lệ thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

7- CA tính: $S_{ca} = k_{ca} \times (x_{ca})^E \bmod n$

8- CA tính: $S = S_i \times S_{ca} \bmod n$

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu M, khóa công khai y_i của U_i , khóa công khai y_{ca} của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước:

1- Tính: $Y = y_i \times y_{ca} \bmod n$

2- Tính: $E = H(R \| M)$

3- Tính: $\overline{R} = S^t \times Y^E \bmod n$

4- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (R_i,S_i) - chữ ký cá nhân của U_i .

Kết quả ra: Khẳng định tính hợp lệ của (R_i,S_i).

Thuật toán bao gồm các bước:

1- Tính giá trị $\overline{R}_i$ theo công thức: $\overline{R}_i = (S_i)^t \times (y_i)^E \bmod n$

2- Kiểm tra nếu $\overline{R}_i = R_i$ thì chữ ký cá nhân (R_i,S_i) của U_i hợp lệ. Ngược lại, nếu $\overline{R}_i \neq R_i$: chữ ký cá nhân (R_i,S_i) của U_i là giả mạo.

2.3 Lược đồ đa chữ ký song song - LD 1.03

2.3.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 1.02.

2.3.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như lược đồ LD 1.02.

2.3.3 Phương pháp hình thành và kiểm tra chữ ký số tập thể

a) Thuật toán hình thành chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu M, khóa bí mật (x_1, x_2,… x_i,…, x_N) của các thành viên nhóm G_i, khóa bí mật x_{ca} của CA.

Kết quả ra: (R,S) - chữ ký tập thể của nhóm G_j tương ứng với M.

Thuật toán bao gồm các bước:

1- Hình thành phần thứ nhất (R) của chữ ký tập thể theo các bước:

1a- U_i ($i=\overline{1,N}$) tính: $R_i = (H(x_i \parallel M))^t \bmod n$, với: $k_i = H(x_i \parallel M)$

1b- Các thành viên nhóm ký gửi giá trị R_i ($i=\overline{1,N}$) cho CA.

1c- CA tính giá trị R_j theo công thức:

$$R_j = \prod_{i=1}^{N} R_i \bmod n$$

1d- CA tính: $R_{ca} = (k_{ca})^t \bmod n$, với: $k_{ca} = H(x_{ca} \parallel M)$

1e- CA tính: $R = R_j \times R_{ca} \bmod n$

2- Hình thành phần thứ hai (S) của chữ ký tập thể theo các bước:

2a- CA tính: $E = H(R \parallel M)$ và gửi cho các thành viên nhóm ký

2b- U_i ($i=\overline{1,N}$) tính: $S_i = k_i \times (x_i)^E \bmod n$

2c- Các thành viên nhóm ký gửi giá trị S_i ($i=\overline{1,N}$) cho CA.

2d- CA kiểm tra chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu các chữ ký cá nhân hợp lệ thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

2e- CA tính giá trị S_j theo công thức:

$$S_j = \prod_{i=1}^{N} S_i \bmod n$$

2g- CA tính: $S_{ca} = k_{ca} \times (x_{ca})^E \bmod n$

2h- CA tính: $S = S_j \times S_{ca} \bmod n$

3- Công khai (R,S) là chữ ký tập thể của nhóm G_j tương ứng với M.

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu M, chữ ký tập thể (R,S), khóa công khai của các thành viên nhóm ký (y_1, y_2,… y_i,…, y_N), khóa công khai y_{ca} của CA.

Kết quả ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước:

1- Tính khóa công khai chung của nhóm ký:

$$Y_j = \prod_{i=1}^{N} y_i \bmod n$$

2- Tính: $Y = Y_j \times y_{ca} \bmod n$

3- Tính: $E = H(R \| M)$

4- Tính: $\overline{R} = S^t \times Y^E \bmod n$

5- Kiểm tra nếu $\overline{R} = R$ thì (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (R_i,S_i) là chữ ký cá nhân của thành viên U_i ($i = \overline{1,N}$).

Kết quả ra: khẳng định tính hợp lệ của chữ ký (R_i,S_i).

Thuật toán bao gồm các bước:

1- Tính giá trị $\overline{R}_i$ ($i = \overline{1,N}$) theo công thức: $\overline{R}_i = (S_i)^t \times (y_i)^E \bmod n$

2- Tính giá trị $\overline{R}_j$ theo công thức:

$$\overline{R}_j = \prod_{i=1}^{N} \overline{R}_i \bmod n$$

3- Kiểm tra nếu $\overline{R}_j = R_j$ thì chữ ký cá nhân (R_i,S_i) của các thành viên trong nhóm ký đều hợp lệ. Ngược lại, nếu $\overline{R}_j \neq R_j$ đã có sự giả mạo trong các chữ ký cá nhân (R_i,S_i).

2.4 Lược đồ đa chữ ký nối tiếp - LD 1.04

2.4.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 1.02.

2.4.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như lược đồ LD 1.02.

2.4.3 Phương pháp hình thành và kiểm tra chữ ký tập thể

a) Thuật toán hình thành chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu cần ký M, khóa bí mật của các thành viên trong nhóm ký (x_1, x_2,… x_i,…, x_N), khóa bí mật (x_{ca}) của CA.

Kết quả ra: (R,S) là chữ ký tập thể của nhóm G_j tương ứng với M.

Thuật toán bao gồm các bước:

1- Hình thành phần thứ nhất (R) của chữ ký tập thể theo các bước:

1a- U_i ($i = \overline{1,N}$) tính: $R_i = R_{i-1} \times (k_i)^t \bmod n$ với: $R_0 = 1$ và: $k_i = H(x_i \| M)$

1b- Thành viên U_i ($i = \overline{1,N}$) gửi giá trị R_i cho CA.

1c- CA kiểm tra nếu $i < N$ thì gửi R_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước hình thành phần thứ nhất của các chữ ký cá nhân (1a). Nếu $i = N$ thì $R_j = R_N$, CA chuyển sang thực hiện bước tiếp theo.

1d- CA tính: $R_{ca} = (k_{ca})^t \bmod n$, với: $k_{ca} = H(x_{ca} \| M)$

1e- CA tính: $R = R_j \times R_{ca} \bmod n$

2- Hình thành phần thứ hai (S) của chữ ký tập thể theo các bước:

2a- CA tính: $E = H(R \| M)$ và gửi cho các thành viên nhóm ký

2b- Thành viên U_i ($i = \overline{1,N}$) tính: $S_i = S_{i-1} \times k_i \times (x_i)^E \bmod n$ với: $S_0 = 1$

2c- Thành viên U_i ($i = \overline{1,N}$) gửi giá trị S_i cho CA.

2d- CA kiểm tra chữ ký cá nhân (R_i,S_i) bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu chữ ký cá nhân hợp lệ thì thực hiện bước tiếp theo (2e). Ngược lại, kết thúc việc hình thành chữ ký tập thể.

2e- Nếu $i < N$: CA gửi S_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước hình thành phần thứ hai của chữ ký cá nhân (2b). Nếu $i = N$ thì $S_j = S_N$, CA chuyển sang thực hiện các bước tiếp theo.

2g- CA tính: $S_{ca} = k_{ca} \times (x_{ca})^E \bmod n$

2h- CA tính: $S = S_j \times S_{ca} \bmod n$

3- Công khai (R,S) là chữ ký tập thể của nhóm G_j tương ứng với M.

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu cần thẩm tra M, chữ ký tập thể (R,S), khóa công khai (y_1, y_2,… y_i,…, y_N) của các thành viên nhóm ký, khóa công khai y_{ca} của CA.

Kết quả ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước:

1- Tính khóa công khai chung của nhóm:

$$Y_j = \prod_{i=1}^{N} y_i \bmod n$$

2- Tính: $Y = Y_j \times y_{ca} \bmod n$

3- Tính: $E = H(R \| M)$

4- Tính: $\overline{R} = S^t \times Y^E \bmod n$

5- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (R_i,S_i) - chữ ký cá nhân của thành viên U_i.

Kết quả ra: khẳng định tính hợp lệ của chữ ký (R_i,S_i).

Thuật toán bao gồm các bước:

1- Tính giá trị: $\overline{R}_i = (S_i)^t \times (Y_i)^E \bmod n$ với: $Y_i = (y_1 \times y_2 \times ... \times y_i) \bmod n$

2- Kiểm tra nếu: $\overline{R}_i = R_i$ thì chữ ký cá nhân (R_i,S_i) hợp lệ. Ngược lại, nếu $\overline{R}_i \neq R_i$ thì (R_i,S_i) là giả mạo.

2.4 Kết luận Chương 2

Các kết quả đã đạt được ở Chương 3 bao gồm 4 lược đồ chữ ký số mới, trong đó lược đồ cơ sở được phát triển từ hệ mật RSA. Lược đồ cơ sở được sử dụng để xây dựng 3 lược đồ chữ ký tập thể theo mô hình đã được đề xuất ở Chương 1.

CHƯƠNG 3
PHÁT TRIỂN CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ DỰA TRÊN HỆ MẬT ELGAMAL VÀ CHUẨN CHỮ KÝ SỐ GOST R34.10-94

3.1 Lược đồ cơ sở loại 1 - LD 2.01

3.1.1 Phương pháp hình thành các tham số hệ thống và khóa

1 - Chọn cặp số nguyên tố p và q đủ lớn, thỏa mãn: $q \mid (p-1)$.

2 - Chọn phần tử sinh: $g = h^{(p-1)/q} \bmod p$, có bậc q của nhóm Z_p^*, với: $1 < h < p$.

3 - Chọn khóa bí mật (x) là một giá trị trong khoảng: $1 < x < q$.

4 - Tính khóa công khai tương ứng (y) theo công thức: $y = g^{-x} \bmod p$

5 - Lựa chọn hàm băm H: $\{0,1\}^* \mapsto Z_q$

6 - Bí mật: x ; công khai: p, q, g.

7- Chứng nhận và công khai y bởi một CA đáng tin cậy.

3.1.2 Phương pháp hình thành và kiểm tra chữ ký

a) Thuật toán hình thành chữ ký

Dữ liệu đầu vào: Thông điệp dữ liệu cần ký M, khóa bí mật x của đối tượng ký.

Kết quả đầu ra: (R,S) là chữ ký số tương ứng với M.

Thuật toán bao gồm các bước:

1 -Tính: $k = H(x \parallel M)$, $R = \left(g^k \bmod p\right) \bmod q$

2 - Tính: $E = H(M)$, $S = \left(k \times E^{-1} + x \times R\right) \bmod q$

b) Thuật toán kiểm tra chữ ký

Dữ liệu đầu vào: Thông điệp dữ liệu M, chữ ký (R,S), khóa công khai *y* của đối tượng ký.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước như sau:

1 - Tính: $E = H(M)$

2- Tính: $\overline{R} = \left(g^{S.E} \times y^{R.E} \bmod p\right) \bmod q$

3- Kiểm tra nếu: $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

3.2 Lược đồ cơ sở loại 2 - LD 2.02

3.2.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 2.01.

3.2.2 Phương pháp kết hợp hình thành chữ ký và mã hóa thông điệp dữ liệu

a) Thuật toán hình thành chữ ký và mã hóa thông điệp dữ liệu

Giả sử đối tượng gửi U_i có khóa bí mật là x_i, khóa công khai tương ứng là y_i; Đối tượng nhận U_i có khóa bí mật là x_i và khóa công khai là y_i. Để gửi thông điệp dữ liệu M cho đối tượng U_j, U_i thực hiện các bước như sau:

1- Tính: $k_i = H(x_i \parallel M)$, $R = g^{k_i} \bmod p$

2- Tính: $E = H(R \parallel M)$, $S = \left(k_i \times E^{-1} + x_i\right) \bmod q$

3- Tính: $C = M \times \left(y_j\right)^{k_i} \bmod p$

4- Gửi bản mã - chữ ký số (C,E,S) đến đối tượng nhận U_j.

b) Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký

Từ bản mã - chữ ký số (C,E,S) nhận được, đối tượng U_j sử dụng

khóa bí mật của mình (x_j) và khóa công khai (y_i) của đối tượng gửi (U_i) để giải mã và xác thực (nguồn gốc, tính toàn vẹn thông tin) thông điệp dữ liệu nhận được theo các bước như sau:

1- Tính giá trị $\bar{R}$ theo công thức: $\bar{R} = g^{S.E} \times (y_i)^E \bmod p$

2- Giải mã thông điệp dữ liệu: $\bar{M} = C \times (\bar{R})^{x_j} \bmod p$

3- Tính: $\bar{E} = H(\bar{R} \parallel \bar{M})$. Nếu: $\bar{E} = E$ thì $\bar{M} = M$ và (E,S) là chữ ký hợp lệ đối với M.

3.3 Lược đồ chữ ký số đơn - LD 2.03

3.3.1 Phương pháp hình thành các tham số hệ thống và khóa

Các tham số hệ thống, khóa của CA và khóa của các đối tượng ký được hình thành theo các bước như sau:

1- Hình thành các tham số hệ thống như lược đồ cơ sở LD 2.01.

2- Khóa bí mật (x_{ca}) của CA là một giá trị được chọn thỏa mãn: $1 < x_{ca} < q$, khóa công khai tương ứng (y_{ca}) của CA được tính theo công thức: $y_{ca} = g^{-x_{ca}} \bmod p$

3- Khóa bí mật (x_i) của thành viên U_i (i = 1,2,3,...) là một giá trị được chọn thỏa mãn: $1 < x_i < q$, khóa công khai y_i tương ứng được tính theo công thức: $y_i = g^{-x_i} \bmod p$

4- Công khai các giá trị: p, q, g, y_{ca} và y_i (i=1,2,3,...); giữ bí mật các giá trị: x_{ca}, x_i (i=1,2,3,...).

3.3.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

a) Thuật toán chứng nhận đối tượng ký

Dữ liệu vào: Khóa công khai y_i và thông tin nhận dạng ID_i của đối tượng ký U_i ($i = 1,2,3...$), khóa bí mật x_{ca} của CA.

Kết quả ra: (u_i,v_i) - chứng nhận của CA đối với U_i .

Thuật toán bao gồm các bước:

1- Tính: $k_i = H(x_{ca} \parallel y_i \parallel ID_i)$, $u_i = \left(g^{k_i} \bmod p\right) \bmod q$

2- Tính: $E = H(y_i \parallel ID_i)$, $v_i = \left(k_i \times E^{-1} + x_{ca} \times u_i\right) \bmod q$

b) Thuật toán kiểm tra tính hợp pháp của đối tượng ký

Dữ liệu vào: Khóa công khai y_i và ID_i của đối tượng U_i, (u_i,v_i), khóa công khai y_{ca} của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chứng nhận (u_i,v_i).

Thuật toán bao gồm các bước:

1- Tính: $E = H(y_i \parallel ID_i)$

2- Tính: $\bar{u}_i = \left(g^{v_i.E} \times (y_{ca})^{u_i.E} \bmod p\right) \bmod q$

3- Kiểm tra nếu $\bar{u}_i = u_i$ thì (u_i,v_i) hợp lệ, do đó tính hợp pháp của đối tượng ký U_i và tính toàn vẹn của y_i được công nhận.

3.3.3 Phương pháp hình thành và kiểm tra chữ ký tập thể

a) Thuật toán hình thành chữ ký tập thể

Dữ liệu đầu vào: Thông điệp dữ liệu M, khóa bí mật x_i của U_i, khóa bí mật x_{ca} của CA.

Kết quả đầu ra: chữ ký số tập thể (R,S).

Thuật toán bao gồm các bước như sau:

1- U_i tính: $R_i = g^{k_i} \bmod p$, với: $k_i = H(x_i \| M)$

2- CA tính: $R_{ca} = g^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

3- CA tính: $R = (R_i \times R_{ca} \bmod p) \bmod q$

4- U_i tính: $S_i = (k_i \times E^{-1} + x_i \times R) \bmod q$, với: $E = H(M)$

5- CA kiểm tra tính hợp lệ của chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu chữ ký cá nhân hợp lệ thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

6- CA tính: $S_{ca} = (k_{ca} \times E^{-1} + x_{ca} \times R) \bmod q$, với: $E = H(M)$

7- CA tính: $S = (S_i + S_{ca}) \bmod q$

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu M, chữ ký (R,S), khóa y_i của U_i, khóa y_{ca} của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước như sau:

1- Tính: $Y = (y_i \times y_{ca}) \bmod p$

2- Tính: $E = H(M)$

3- Tính: $\overline{R} = (g^{S.E} \times Y^{R.E} \bmod p) \bmod q$

4- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (R_i,S_i) là chữ ký cá nhân của thành viên U_i.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R_i,S_i).

Thuật toán bao gồm các bước:

1 - Tính: $\overline{R}_i = g^{S_i.E} \times (y_i)^{R.E} \bmod p$

2- Kiểm tra nếu $\overline{R}_i = R_i$ thì chữ ký cá nhân (R_i,S_i) hợp lệ. Ngược lại, nếu $\overline{R}_i \neq R_i$ thì (R_i,S_i) là giả mạo.

3.4 Lược đồ chữ ký số đơn và mã hóa - LD 2.04

3.4.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như Lược đồ LD 2.03.

3.4.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

a) Thuật toán chứng nhận đối tượng ký

Dữ liệu đầu vào: Khóa công khai y_i và ID_i của U_i ($i = 1,2,3...$), khóa bí mật x_{ca} của CA.

Kết quả đầu ra: chứng nhận (u_i,v_i) của CA đối với U_i .

Thuật toán bao gồm các bước:

1- Tính: $k_i = H(x_{ca} \| y_i \| ID_i)$, $t_i = g^{k_i} \bmod p$

2- Tính: $u_i = H(t_i \| y_i \| ID_i)$

3- Tính: $v_i = (k_i \times (u_i)^{-1} + x_{ca}) \bmod q$

b) Thuật toán kiểm tra tính hợp pháp của đối tượng ký

Dữ liệu vào: Khóa công khai y_i và ID_i của U_i, (u_i,v_i), khóa công khai y_{ca} của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chứng nhận (u_i,v_i).

Thuật toán bao gồm các bước như sau:

1- Tính: $\bar{t}_i = g^{v_i \cdot u_i} \times (y_{ca})^{u_i} \bmod p$

2- Tính: $\bar{u}_i = H(\bar{t}_i \| y_i \| ID_i)$

3- Kiểm tra nếu $\bar{u}_i = u_i$ thì (u_i,v_i) hợp lệ, do đó tính hợp pháp của đối tượng ký U_i và tính toàn vẹn của y_i được công nhận.

3.4.3 Phương pháp kết hợp hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

a) Thuật toán hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

Trường hợp 1:

Giả sử đối tượng U_i gửi thông điệp dữ liệu M cho đối tượng U_j. Ở đây, đối tượng U_i có khóa bí mật là x_i và khóa công khai là y_i, đối tượng U_j có khóa bí mật là x_j và khóa công khai là y_j.

Dữ liệu vào: Thông điệp dữ liệu M: $0 \le M < p$, khóa bí mật (x_i) của đối tượng U_i, khóa bí mật x_{ca} của CA và khóa công khai y_j của đối tượng U_j.

Kết quả đầu ra: (C,E,S) là bản mã - chữ ký số tập thể tương ứng với M.

Thuật toán bao gồm các bước như sau:

1- U_i tính: $R_i = g^{k_i} \bmod p$, với: $k_i = H(x_i \| M)$

2- CA tính: $R_{ca} = g^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

3- CA tính: $R = R_i \times R_{ca} \bmod p$

4- CA tính: $E = H(R \| M)$

5- U_i tính: $S_i = (k_i \times E^{-1} + x_i) \bmod q$

6- CA kiểm tra chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục ***c***). Nếu chữ ký cá nhân hợp lệ thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

7- CA tính: $S_{ca} = (k_{ca} \times E^{-1} + x_{ca}) \bmod q$

8- CA tính: $S = (S_i + S_{ca}) \bmod q$

9- U_i mã hóa thông điệp dữ liệu M: $C_i = M \times (y_j)^{k_i} \bmod p$

10- CA mã hóa C_i : $C = C_i \times (y_j)^{k_{ca}} \bmod p$

11- Gửi bản mã – chữ ký tập thể (C,E,S) tới đối tượng nhận U_j.

Trường hợp 2:

Giả sử đối tượng U_i gửi thông điệp dữ liệu M cho một nhóm *k* đối tượng: G_i ={ U_1, U_2, ... ,U_i, ... ,U_k}. Ở đây, đối tượng U_i có khóa bí mật là x_i, khóa công khai tương ứng là y_i và nhóm đối tượng G_i có các khóa bí mật là: {x_1, x_2, ... ,x_j, ... ,x_k} và các khóa công khai tương ứng là: { y_1, y_2, ... ,y_i, ... ,y_k}.

Dữ liệu vào: Thông điệp dữ liệu M: $0 \le M < p$, khóa bí mật x_i của đối tượng U_i, khóa bí mật x_{ca} của CA, các khóa công khai (y_1, y_2, ... ,y_j, ... ,y_k) của nhóm đối tượng G_i.

Kết quả đầu ra: bản mã - chữ ký số tập thể (C,E,S) tương ứng với M.

Thuật toán bao gồm các bước như sau:

1- U_i tính: $R_i = g^{k_i} \bmod p$, với: $k_i = H(x_i \| M)$

2- CA tính: $R_{ca} = g^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

3- CA tính: $R = R_i \times R_{ca} \bmod p$

4- CA hình thành phần thứ nhất E của chữ ký tập thể: $E = H(R \| M)$

5- U_i tính: $S_i = (k_i \times E^{-1} + x_i) \bmod q$

6- CA kiểm tra chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu chữ ký cá nhân hợp lệ thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

7- CA tính S_{ca} theo công thức: $S_{ca} = (k_{ca} \times E^{-1} + x_{ca}) \bmod q$

8- CA hình thành phần thứ hai S của chữ ký tập thể: $S = (S_i + S_{ca}) \bmod q$

9- Tính khóa công khai chung của nhóm G_j:

$$Y_j = \prod_{j=1}^{k} y_j \bmod p$$

10- U_i mã hóa thông điệp dữ liệu M: $C_i = M \times (Y_j)^{k_i} \bmod p$

11- CA mã hóa C_i theo công thức: $C = C_i \times (Y_j)^{k_{ca}} \bmod p$

12- Gửi bản mã – chữ ký tập thể (C,E,S) tới đối tượng nhận U_j.

b) Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký tập thể

Trường hợp 1:

Từ bản mã - chữ ký tập thể (C,E,S) nhận được, đối tượng U_j sử dụng khóa bí mật của mình (x_j), khóa công khai (y_i) của đối tượng gửi U_i và khóa công khai (y_{ca}) của CA để giải mã và kiểm tra nguồn gốc cũng như tính toàn vẹn của thông điệp dữ liệu theo các bước như sau:

1- Tính khóa công khai chung của CA và đối tượng ký:

$$Y = y_i \times y_{ca} \bmod p$$

2- Tính: $\overline{R} = g^{S.E} \times Y^E \bmod p$

3- Giải mã thông điệp dữ liệu: $\overline{M} = C \times (\overline{R})^{x_j} \bmod p$

4- Tính: $\overline{E} = H(\overline{R} \| \overline{M})$

5- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ với M.

Trường hợp 2:

Từ bản mã - chữ ký tập thể (C,E,S) nhận được, nhóm đối tượng G_j sử dụng khóa bí mật của mình $\{x_1, x_2, ... ,x_j, ... ,x_k\}$, khóa công khai của đối tượng gửi (y_i) và khóa công khai (y_{ca}) của CA để giải mã và kiểm tra nguồn gốc cũng như tính toàn vẹn của thông điệp dữ liệu nhận được. Mỗi thành viên U_i (j=1,2,.., k) của nhóm G_i thực hiện các bước như sau:

1- Tính khóa công khai chung của CA và đối tượng ký:

$$Y = y_i \times y_{ca} \bmod p$$

2- Tính: $\overline{R} = g^{S.E} \times Y^E \bmod p$

3- Tính giá trị $\overline{r}_j$ theo công thức: $\overline{r}_j = (\overline{R})^{x_j} \bmod p$

4- Gửi giá trị $\overline{r}_j$ cho các thành viên còn lại trong nhóm G_j bằng *Thuật toán hình thành chữ ký và mã hóa thông điệp dữ liệu* của lược đồ cơ sở LD 2.02.

5- Nhận các giá trị: $\overline{r}_1, \overline{r}_2, \ldots, \overline{r}_{j-1}, \overline{r}_{j+1}, \ldots, \overline{r}_k$ của các thành viên khác trong nhóm bằng *Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký* của lược đồ cơ sở LD 2.02.

6- Tính giá trị $\overline{R}_j$ theo công thức:

$$\overline{R}_j = \prod_{j=1}^{k} \overline{r}_j \bmod p$$

7- Giải mã thông điệp dữ liệu: $\overline{M} = C \times (\overline{R}_j) \bmod p$

8- Tính: $\overline{E} = H(\overline{R} \parallel \overline{M})$

9- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ tương ứng với M.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (R_i,S_i) là chữ ký cá nhân của thành viên U_i.

Kết quả ra: Khẳng định tính hợp lệ của (R_i,S_i).

Thuật toán bao gồm các bước:

1- Tính giá trị $\overline{R}_i$ theo công thức: $\overline{R}_i = g^{S_i.E} \times (y_i)^E \bmod p$

2- Kiểm tra nếu $\overline{R}_i = R_i$ thì chữ ký cá nhân (R_i,S_i) của U_i hợp lệ. Ngược lại, nếu $\overline{R}_i \neq R_i$ thì (R_i,S_i) là giả mạo.

3.5 Lược đồ đa chữ ký song song - LD 2.05

3.5.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như ở lược đồ LD 2.03.

3.5.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như ở lược đồ LD 2.03.

3.5.3 Phương pháp hình thành và kiểm tra chữ ký tập thể

Giả sử nhóm ký gồm *n* đối tượng: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $\{x_1, x_2, \ldots x_i, \ldots, x_n\}$ và các khóa công khai tương ứng: $\{y_1, y_2, \ldots y_i, \ldots, y_n\}$.

a) Thuật toán hình thành chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu cần ký M, các khóa bí mật (x_1, x_2,… x_i,…, x_n) của các thành viên nhóm G_i , khóa bí mật (x_{ca}) của CA.

Kết quả đầu ra: (R,S) - chữ ký tập thể tương ứng với M.

Thuật toán bao gồm các bước:

1- Hình thành phần thứ nhất của các chữ ký cá nhân (r_i) theo các bước:

1a- Các thành viên U_i ($i = \overline{1,n}$) tính giá trị r_i theo công thức:

$r_i = g^{k_i} \bmod p$, với: $k_i = H(x_i \| M)$

1b- Các thành viên U_i gửi giá trị r_i cho CA.

2- Hình thành phần thứ nhất (R) của chữ ký tập thể theo các bước:

2a- CA tính giá trị R_i theo công thức:

$$R_i = \prod_{i=1}^{n} r_i \bmod p$$

2b- CA tính: $R_{ca} = g^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

2c- CA hình thành phần thứ nhất của chữ ký tập thể:

$R = (R_i \times R_{ca} \bmod p) \bmod q$

3- Hình thành phần thứ hai của các chữ ký cá nhân (s_i) theo các bước:

3a- Các thành viên U_i ($i = \overline{1,n}$) tính giá trị s_i theo công thức:

$s_i = (k_i \times E^{-1} + x_i \times R) \bmod q$, với: $E = H(M)$

3b- Các thành viên U_i gửi giá trị s_i cho CA.

4- Hình thành phần thứ hai (S) của chữ ký tập thể theo các bước:

4a- CA kiểm tra tính hợp lệ của các chữ ký cá nhân bằng *Thuật toán kiểm tra chữ ký cá nhân*. Nếu tính hợp lệ của các chữ ký cá nhân được công nhận thì thực hiện các bước tiếp theo. Ngược lại, kết thúc việc hình thành chữ ký tập thể.

4b- CA tính giá trị S_i theo công thức:

$$S_i = \sum_{i=1}^{n} s_i \bmod q$$

4c- CA tính: $S_{ca} = (k_{ca} \times E^{-1} + x_{ca} \times R) \bmod q$

4d- CA hình thành phần thứ hai S của chữ ký tập thể: $S = (S_i + S_{ca}) \bmod q$

5- CA công khai (R,S) là chữ ký tập thể của nhóm G_i tương ứng với thông điệp dữ liệu M.

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu cần thẩm tra M, chữ ký tập thể (R,S), khóa công khai (y_1, y_2,… y_i,…, y_n) của các thành viên nhóm G_i , khóa công khai (y_{ca}) của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước như sau:

1- Tính khóa công khai chung của nhóm ký:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính khóa công khai chung của nhóm ký và CA: $Y = Y_i \times y_{ca} \bmod p$

3- Tính giá trị đại diện (E) của thông điệp dữ liệu cần thẩm tra (M):

$$E = H(M)$$

4- Tính giá trị $\overline{R}$ theo công thức: $\overline{R} = \left(g^{S.E} \times Y^{R.E} \bmod p\right) \bmod q$

5- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (r_i,s_i) là chữ ký cá nhân của thành viên U_i .

Kết quả ra: khẳng định tính hợp lệ của chữ ký (r_i,s_i).

Thuật toán bao gồm các bước:

1- Tính các giá trị $\overline{r_i}$ $(i = \overline{1,n})$ theo công thức: $\overline{r_i} = g^{s_i.E} \times (y_i)^{R.E} \bmod p$

2- Tính giá trị $\overline{R_i}$ theo công thức:

$$\overline{R_i} = \prod_{i=1}^{n} \overline{r_i} \bmod p$$

3- Kiểm tra nếu $\overline{R_i} = R_i$ thì chữ ký cá nhân (r_i,s_i) hợp lệ. Ngược lại, nếu $\overline{R_i} \neq R_i$ đã có sự giả mạo trong các chữ ký cá nhân (r_i,s_i).

3.6 Lược đồ đa chữ ký nối tiếp - LD 2.06

3.6.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 2.03.

3.6.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như ở lược đồ LD 2.03.

3.6.3 Phương pháp hình thành và kiểm tra chữ ký tập thể

Giả sử nhóm ký gồm *n* đối tượng: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $x_1, x_2, \ldots x_i, \ldots, x_n$ và các khóa công khai tương ứng là: $y_1, y_2, \ldots y_i, \ldots, y_n$.

a) Thuật toán hình thành chữ ký tập thể

Dữ liệu vào: Thông điệp dữ liệu cần ký M, khóa bí mật $(x_1, x_2, \ldots x_i, \ldots, x_n)$ của các thành viên nhóm ký G_i , khóa bí mật (x_{ca}) của CA.

Kết quả đầu ra: (R,S) - chữ ký số tập thể tương ứng với M.

Thuật toán bao gồm các bước như sau:

1- Hình thành phần thứ nhất của các chữ ký cá nhân (r_i) theo các bước:

1a- Thành viên U_i $(i = \overline{1,n})$ tính giá trị r_i theo công thức:

$$r_i = r_{i-1} \times g^{k_i} \bmod p, \text{ với: } r_0 = 1 \text{ và } k_i = H(x_i \| M)$$

1b- Thành viên U_i $(i = \overline{1,n})$ gửi giá trị r_i cho CA.

1c- CA kiểm tra nếu $i < n$ thì gửi r_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước hình thành phần thứ nhất của các chữ ký cá nhân (1a). Nếu $i = n$ thì $R_i = r_n$, CA chuyển sang thực hiện bước hình thành chữ ký tập thể tiếp theo (2).

2- Hình thành phần thứ nhất của chữ ký tập thể (R) theo các bước như sau:

2a- CA tính: $R_{ca} = g^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

2b- CA hình thành phần thứ nhất của chữ ký tập thể:

$R = (R_i \times R_{ca} \bmod p) \bmod q$

3- Hình thành phần thứ hai của các chữ ký cá nhân (s_i) theo các bước:

3a- CA gửi giá trị R cho các thành viên nhóm ký.

3b- Thành viên U_i ($i = \overline{1,n}$) tính:

$s_i = (s_{i-1} + k_i \times E^{-1} + x_i \times R) \bmod q$, với: $s_0 = 0$ và $E = H(M)$

3c- Thành viên U_i ($i = \overline{1,n}$) gửi giá trị s_i cho CA.

3d- CA kiểm tra chữ ký cá nhân (r_i,s_i) bằng *Thuật toán kiểm tra chữ ký cá nhân* (Mục c). Nếu chữ ký cá nhân hợp lệ thì thực hiện bước tiếp theo (3e). Ngược lại, kết thúc việc hình thành chữ ký tập thể.

3e- Nếu $i < n$: CA gửi s_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước hình thành phần thứ hai của chữ ký cá nhân (3b). Nếu $i = n$ thì $S_i = s_n$, CA chuyển sang thực hiện các bước hình thành chữ ký tập thể tiếp theo (4).

4- Hình thành phần thứ hai (S) của chữ ký tập thể theo các bước như sau:

4a- CA tính: $S_{ca} = (k_{ca} \times E^{-1} + x_{ca} \times R) \bmod q$, với: $E = H(M)$

4b- CA hình thành phần thứ 2 của chữ ký tập thể: $S = (S_i + S_{ca}) \bmod q$

5- CA công khai (R,S) là chữ ký tập thể của nhóm G_i tương ứng với M.

b) Thuật toán kiểm tra chữ ký tập thể

Dữ liệu đầu vào: Thông điệp dữ liệu M, chữ ký tập thể (R,S), khóa công khai (y_1, y_2, y_i,, y_n) của các thành viên nhóm ký G_i , khóa công khai (y_{ca}) của CA.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (R,S).

Thuật toán bao gồm các bước như sau:

1- Tính khóa công khai chung của nhóm ký theo công thức:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính khóa công khai chung của nhóm ký và CA: $Y = Y_i \times y_{ca} \bmod p$

3- Tính: $E = H(M)$

4- Tính: $\overline{R} = (g^{S.E} \times Y^{R.E} \bmod p) \bmod q$

5- Kiểm tra nếu $\overline{R} = R$ thì chữ ký (R,S) hợp lệ.

c) Thuật toán kiểm tra chữ ký cá nhân

Dữ liệu vào: (r_i,s_i) - chữ ký cá nhân của thành viên U_i.

Kết quả ra: Khẳng định tính hợp lệ của (r_i,s_i).

Thuật toán bao gồm các bước:

1- Tính giá trị $\overline{r_i}$ theo công thức:

$\overline{r_i} = g^{s_i.E} \times (Y_i)^{R.E} \bmod p$, với: $Y_i = (y_1 \times y_2 \times ... \times y_i) \bmod p$

2- Kiểm tra nếu: $\overline{r_i} = r_i$ thì chữ ký cá nhân (r_i,s_i) hợp lệ. Ngược lại, nếu $\overline{r_i} \neq r_i$

thì (r_i,s_i) là giả mạo.

3.7 Lược đồ đa chữ ký và mã hóa song song - LD 2.07

3.7.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 2.03.

3.7.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như lược đồ LD 2.04.

3.7.3 Phương pháp kết hợp hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

a) Thuật toán hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

Trường hợp 1:

Giả sử nhóm *n* đối tượng gửi: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $\{x_1, x_2, \ldots x_i, \ldots, x_n\}$ và các khóa công khai tương ứng là: $\{y_1, y_2, \ldots y_i, \ldots, y_n\}$; đối tượng nhận U_j có khóa bí mật là x_j và khóa công khai tương ứng là y_j. Dữ liệu đầu vào của thuật toán bao gồm: thông điệp dữ liệu M: $0 \le M < p$, khóa bí mật ($x_1, x_2, \ldots x_i, \ldots, x_n$) của các thành viên nhóm G_i, khóa bí mật (x_{ca}) của CA và khóa công khai (y_j) của đối tượng nhận U_j. Kết quả đầu ra của thuật toán là bản mã – chữ ký tập thể (C,E,S) tương ứng với M. Nhóm G_i mã hóa và ký tập thể thông điệp dữ liệu M theo các bước như sau:

1- Hình thành chữ ký (E,S) bằng *Thuật toán hình thành chữ ký tập thể* của lược đồ LD 2.05.

2- Mã hóa thông điệp dữ liệu (M) theo các bước:

2a- Thành viên U_i ($i = \overline{1,n}$) tính: $c_i = \left(y_j\right)^{k_i} \bmod p$, với: $k_i = H(x_i \| M)$

2b- Các thành viên gửi giá trị c_i ($i = \overline{1,n}$) cho CA.

2c- CA tính giá trị C_i theo công thức:

$$C_i = \prod_{i=1}^{n} c_i \bmod p$$

2d- CA tính: $C_{ca} = \left(y_j\right)^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

2e- CA hình thành bản mã: $C = M \times C_i \times C_{ca} \bmod p$

3- Gửi bản mã – chữ ký tập thể (C,E,S) cho đối tượng nhận U_j.

Trường hợp 2:

Giả sử nhóm đối tượng gửi: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $x_1, x_2, \ldots x_i, \ldots, x_n$ và các khóa công khai tương ứng là: $y_1, y_2, \ldots y_i, \ldots, y_n$; Nhóm đối tượng nhận: $G_j = \{U_1, U_2, \ldots U_j, \ldots, U_k\}$ có các khóa bí mật là: $x_1, x_2, \ldots x_j, \ldots, x_k$ và các khóa công khai tương ứng là: $y_1, y_2, \ldots y_j, \ldots, y_k$. Dữ liệu đầu vào của thuật toán bao gồm: thông điệp dữ liệu M: $0 \le M < p$, khóa bí mật ($x_1, x_2, \ldots x_i, \ldots, x_n$) của các thành viên nhóm G_i, khóa bí mật (x_{ca}) của CA và các khóa công khai ($y_1, y_2, \ldots y_j, \ldots, y_k$) của nhóm đối tượng nhận G_j. Kết quả đầu ra của thuật toán là bản mã – chữ ký tập thể (C,E,S) tương ứng với M. Nhóm G_i mã hóa và ký tập thể thông điệp dữ liệu M theo các bước như sau:

1- Hình thành chữ ký (E,S) bằng *Thuật toán hình thành chữ ký tập thể* của

LD 2.05.

2- Mã hóa thông điệp dữ liệu (M) theo các bước:

2a- Tính khóa công khai chung của nhóm G_j theo công thức:

$$Y_j = \prod_{j=1}^{k} y_j \bmod p$$

2b- Thành viên U_i ($i = \overline{1,n}$) tính: $c_i = (Y_j)^{k_i} \bmod p$

2c- Các thành viên gửi giá trị c_i ($i = \overline{1,n}$) cho CA.

2d- CA tính giá trị C_i theo công thức:

$$C_i = \prod_{i=1}^{n} c_i \bmod p$$

2e- CA tính: $C_{ca} = (Y_j)^{k_{ca}} \bmod p$

2g- CA hình thành bản mã: $C = M \times C_i \times C_{ca} \bmod p$

3- Gửi bản mã – chữ ký tập thể (C,E,S) cho nhóm đối tượng U_j.

b) Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký tập thể

Trường hợp 1:

Dữ liệu đầu vào của thuật toán bao gồm: bản mã – chữ ký tập thể (C,E,S), khóa công khai (y_1, y_2,… y_i,…, y_n) của các thành viên nhóm G_i, khóa công khai (y_{ca}) của CA và khóa bí mật (x_i) của đối tượng nhận U_i. Kết quả đầu ra của thuật toán là sự khẳng định về tính hợp lệ của bản mã – chữ ký tập thể (C,E,S) hay sự công nhận về nguồn gốc và tính toàn vẹn của thông điệp dữ liệu được bảo mật nội dung (M). Thuật toán bao gồm các bước như sau:

1- Tính khóa công khai chung của nhóm G_i:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính: $Y = Y_i \times y_{ca} \bmod p$

3- Tính: $\overline{R} = g^{S.E} \times Y^E \bmod p$

4- Giải mã thông điệp dữ liệu theo công thức: $\overline{M} = C \times (\overline{R})^{x_j} \bmod p$

5- Tính: $\overline{E} = H(\overline{R} \parallel \overline{M})$

6- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ với M.

Trường hợp 2:

Dữ liệu đầu vào của thuật toán bao gồm: bản mã – chữ ký tập thể (C,E,S), khóa công khai (y_1, y_2,… y_i,…, y_n) của các thành viên nhóm G_i, khóa công khai (y_{ca}) của CA và khóa bí mật (x_1, x_2,… x_i,…, x_k) của các thành viên nhóm đối tượng nhận G_i. Kết quả đầu ra của thuật toán là sự khẳng định về tính hợp lệ của bản mã - chữ ký tập thể (C,E,S) hay sự công nhận về nguồn gốc và tính toàn vẹn của thông điệp dữ liệu nhận được (M). Mỗi thành viên U_i (j=1,2,.., k) của nhóm G_i thực hiện các bước như sau:

1- Tính khóa công khai (Y_i) chung của nhóm G_i theo công thức:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính khóa công khai chung (Y) của nhóm G_i và CA: $Y = Y_i \times y_{ca} \bmod p$

3- Tính: $\overline{R} = g^{S.E} \times Y^E \bmod p$

4- Tính: $\overline{r}_j = (\overline{R})^{x_j} \bmod p$

5- Gửi giá trị $\overline{r}_j$ cho các thành viên còn lại trong nhóm G_j bằng *Thuật toán hình thành chữ ký và mã hóa thông điệp dữ liệu* của lược đồ cơ sở LD 2.02.

6- Nhận các giá trị: $\overline{r}_1, \overline{r}_2, \ldots, \overline{r}_{j-1}, \overline{r}_{j+1}, \ldots, \overline{r}_k$ của các thành viên khác trong nhóm bằng *Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký* của lược đồ cơ sở LD 2.02.

7- Tính giá trị $\overline{R}_j$ theo công thức:

$$\overline{R}_j = \prod_{j=1}^{k} \overline{r}_j \bmod p$$

8- Giải mã thông điệp dữ liệu theo công thức: $\overline{M} = C \times (\overline{R}_j) \bmod p$

9- Tính: $\overline{E} = H(\overline{R} \parallel \overline{M})$

10- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ với M.

3.8 Lược đồ đa chữ ký và mã hóa nối tiếp - LD 2.08

3.8.1 Phương pháp hình thành các tham số hệ thống và khóa

Tương tự như lược đồ LD 2.03.

3.8.2 Phương pháp chứng nhận và kiểm tra tính hợp pháp của các đối tượng ký

Tương tự như ở lược đồ LD 2.04.

3.8.3 Phương pháp kết hợp hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

a) Thuật toán hình thành chữ ký tập thể và mã hóa thông điệp dữ liệu

Trường hợp 1:

Giả sử nhóm đối tượng gửi: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $\{x_1, x_2, \ldots x_i, \ldots, x_n\}$ và các khóa công khai tương ứng là: $\{y_1, y_2, \ldots y_i, \ldots, y_n\}$; Đối tượng nhận U_i có khóa bí mật là x_i và khóa công khai tương ứng là y_i.

Dữ liệu đầu vào của thuật toán bao gồm: thông điệp dữ liệu M, khóa bí mật $\{x_1, x_2, \ldots x_i, \ldots, x_n\}$ của các thành viên nhóm G_i, khóa bí mật (x_{ca}) của CA và khóa công khai (y_i) của đối tượng nhận U_i. Kết quả đầu ra của thuật toán là bản mã – chữ ký tập thể (C,E,S) tương ứng với M. Nhóm G_i mã hóa và ký tập thể thông điệp dữ liệu M theo các bước như sau:

1- Hình thành chữ ký (E,S) bằng *Thuật toán hình thành chữ ký tập thể* của LD 2.06.

2- Mã hóa thông điệp dữ liệu theo các bước như sau :

2a- Thành viên U_i ($i = \overline{1,n}$) tính giá trị c_i theo công thức:

$c_i = c_{i-1} \times (y_j)^{k_i} \bmod p$, với: $c_0 = 1$ và $k_i = H(x_i \parallel M)$

2b- Thành viên U_i ($i = \overline{1,n}$) gửi giá trị c_i cho CA.

2c- CA kiểm tra nếu $i < n$ thì gửi c_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước (2a). Nếu $i = n$ thì $C_i = c_n$, CA chuyển sang thực hiện các bước tiếp theo.

2d- CA tính: $C_{ca} = (y_j)^{k_{ca}} \bmod p$, với: $k_{ca} = H(x_{ca} \| M)$

2e- CA hình thành bản mã: $C = M \times C_i \times C_{ca} \bmod p$

3- Gửi bản mã – chữ ký tập thể (C,E,S) cho đối tượng nhận U_j.

Trường hợp 2:

Giả sử nhóm đối tượng gửi: $G_i = \{U_1, U_2, \ldots U_i, \ldots, U_n\}$ có các khóa bí mật là: $\{x_1, x_2, \ldots x_i, \ldots, x_n\}$ và các khóa công khai tương ứng là: $\{y_1, y_2, \ldots y_i, \ldots, y_n\}$; Nhóm đối tượng nhận: $G_j = \{U_1, U_2, \ldots U_j, \ldots, U_k\}$ có các khóa bí mật là: $\{x_1, x_2, \ldots x_j, \ldots, x_k\}$ và các khóa công khai tương ứng là: $\{y_1, y_2, \ldots y_j, \ldots, y_k\}$.

Dữ liệu đầu vào của thuật toán bao gồm: thông điệp dữ liệu M: $0 \le M < p$, khóa bí mật ($x_1, x_2, \ldots x_i, \ldots, x_n$) của các thành viên nhóm G_i, khóa bí mật (x_{ca}) của CA và các khóa công khai ($y_1, y_2, \ldots y_i, \ldots, y_k$) của nhóm đối tượng nhận G_j. Kết quả đầu ra của thuật toán là bản mã – chữ ký tập thể (C,E,S) tương ứng với M. Nhóm G_i mã hóa và ký tập thể thông điệp dữ liệu M theo các bước như sau:

1- Hình thành chữ ký (E,S) bằng *Thuật toán hình thành chữ ký tập thể* của LD 2.06.

2- Mã hóa thông điệp dữ liệu (M) theo các bước:

2a- Tính khóa công khai chung của nhóm G_j theo công thức:

$$Y_j = \prod_{j=1}^{k} y_j \bmod p$$

2b- Thành viên U_i ($i = \overline{1,n}$) tính: $c_i = c_{i-1} \times (Y_j)^{k_i} \bmod p$ với: $c_0 = 1$

2c- Thành viên U_i ($i = \overline{1,n}$) gửi giá trị c_i cho CA.

2d- CA kiểm tra nếu $i < n$ thì gửi c_i cho thành viên tiếp theo U_{i+1} để tiếp tục thực hiện bước (2a). Nếu $i = n$ thì $C_i = c_n$, CA chuyển sang thực hiện các bước tiếp theo.

2e- CA tính giá trị C_{ca} theo công thức: $C_{ca} = (Y_j)^{k_{ca}} \bmod p$

2g- CA hình thành bản mã: $C = M \times C_i \times C_{ca} \bmod p$

3- Gửi bản mã – chữ ký tập thể (C,E,S) cho nhóm đối tượng U_j.

b) Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký tập thể

Trường hợp 1:

Dữ liệu đầu vào của thuật toán bao gồm: bản mã – chữ ký tập thể (C,E,S), khóa công khai ($y_1, y_2, \ldots y_i, \ldots, y_n$) của các thành viên nhóm G_i, khóa công khai (y_{ca}) của CA và khóa bí mật (x_i) của đối tượng nhận U_i. Kết quả đầu ra của thuật toán là sự khẳng định về tính hợp lệ của chữ ký (E,S) hay sự công nhận về nguồn gốc và tính toàn vẹn của thông điệp dữ liệu nhận được. Thuật toán bao gồm các bước như sau:

1- Tính khóa công khai chung của nhóm G_i:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính khóa công khai chung của nhóm G_i và CA: $Y = Y_i \times y_{ca} \bmod p$

3- Tính: $\overline{R} = g^{S.E} \times Y^E \bmod p$

4- Giải mã thông điệp dữ liệu: $\overline{M} = C \times (\overline{R})^{x_j} \bmod p$

5- Tính: $\overline{E} = H(\overline{R} \parallel \overline{M})$

6- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ với M.

Trường hợp 2:

Dữ liệu vào: bản mã – chữ ký tập thể (C,E,S), khóa công khai (y_1, y_2,… y_i,…, y_n) của các thành viên nhóm G_i, khóa công khai (y_{ca}) của CA và khóa bí mật (x_1, x_2,… x_j,…, x_k) của các thành viên nhóm đối tượng nhận G_i.

Kết quả đầu ra: khẳng định tính hợp lệ của chữ ký (E,S).

Để giải mã và xác thực thông điệp dữ liệu nhận được mỗi thành viên U_j (j=1,2,.., k) của nhóm G_i thực hiện các bước như sau:

1- Tính khóa công khai chung của nhóm G_i:

$$Y_i = \prod_{i=1}^{n} y_i \bmod p$$

2- Tính khóa công khai chung của nhóm G_i và CA: $Y = Y_i \times y_{ca} \bmod p$

3- Tính: $\overline{R} = g^S \times Y^E \bmod p$

4- Tính: $\overline{r}_j = (\overline{R})^{x_j} \bmod p$

5- Gửi giá trị $\overline{r}_j$ cho các thành viên còn lại trong nhóm G_j bằng *Thuật toán hình thành chữ ký và mã hóa thông điệp dữ liệu* của lược đồ cơ sở LD 2.02.

6- Nhận các giá trị: $\overline{r}_1, \overline{r}_2, \ldots, \overline{r}_{j-1}, \overline{r}_{j+1}, \ldots, \overline{r}_k$ của các thành viên khác trong nhóm bằng *Thuật toán giải mã thông điệp dữ liệu và kiểm tra chữ ký* của lược đồ cơ sở LD 2.02.

7- Tính giá trị $\overline{R}_j$ theo công thức:

$$\overline{R}_j = \prod_{j=1}^{k} \overline{r}_j \bmod p$$

8- Giải mã thông điệp dữ liệu: $\overline{M} = C \times (\overline{R}_j) \bmod p$

9- Tính: $\overline{E} = H(\overline{R} \parallel \overline{M})$

10- Kiểm tra nếu $\overline{E} = E$ thì $\overline{M} = M$ và (E,S) là chữ ký hợp lệ với M.

3.4 Kết luận Chương 3

Các kết quả đã đạt được ở Chương 3 bao gồm 8 lược đồ chữ ký số mới, trong đó có 2 lược đồ cơ sở được phát triển từ hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94. Các lược đồ cơ sở được sử dụng để xây dựng 6 lược đồ chữ ký tập thể theo mô hình đã được đề xuất ở Chương 1.

KẾT LUẬN

1. Những kết quả đã đạt được của Luận án:

- Đề xuất mô hình ứng dụng chữ ký số nhằm đáp ứng các yêu cầu về chứng thực các thông điệp dữ liệu trong các giao dịch điện tử, có thể áp dụng phù hợp trong các tổ chức xã hội, cơ quan hành chính nhà nước, các doanh nghiệp,...
- Xây dựng 12 lược đồ chữ ký số, trong đó có 3 lược đồ cơ sở (LD 1.01, LD 2.01, LD 2.02) phát triển từ các hệ mật RSA, ElGamal và chuẩn chữ ký GOST R34.10-94 của Liên bang Nga, 9 lược đồ chữ ký tập thể theo mô hình ứng dụng mới đề xuất, bao gồm 3 lược đồ chữ ký số đơn (LD 1.02, LD 2.03, LD 2.04) và 6 lược đồ đa chữ ký số (LD 1.03, LD 1.04, LD 2.05, LD 2.06, LD 2.07, LD 2.08) trong đó một số lược đồ có khả năng hỗ trợ bảo mật thông tin (LD 2.04, LD 2.07, LD 2.08).

2. Những đóng góp mới của Luận án:

- *Mô hình chữ ký số tập thể*: đây là mô hình ứng dụng chữ ký số nhằm đáp ứng yêu cầu xác thực nguồn gốc và tính toàn vẹn cho các thông điệp dữ liệu ở nhiều cấp độ khác nhau, ứng dụng phù hợp trong các tổ chức xã hội, các cơ quan hành chính nhà nước, các doanh nghiệp,... Kết quả này được thể hiện ở công trình số [4] của Luận án.
- *Lược đồ cơ sở LD 1.01*: là một thuật toán chữ ký số được phát triển trên cơ sở hệ mật RSA, thuật toán này có một số ưu điểm như:

+ Cho phép nhiều thực thể ký cùng sử dụng chung một *modulo n*.

+ Cho phép xây dựng lược đồ chữ ký tập thể ở cả 2 dạng lược đồ chữ ký số đơn và lược đồ đa chữ ký thuận tiện hơn so với lược đồ chữ ký RSA.

Kết quả này được thể hiện ở công trình số [5] của Luận án.

- *Lược đồ cơ sở LD 2.01*: được phát triển từ chuẩn chữ ký số GOST R34.10-94 của Liên bang Nga, lược đồ này có ưu điểm so với các lược đồ thuộc họ El Gamal là chỉ cần sử dụng một khóa bí mật duy nhất để hình thành chữ ký, do đó đã khắc phục được yếu điểm của các lược đồ họ ElGamal khi khóa thứ hai bị sử dụng lặp lại. Kết quả này được thể hiện ở công trình số [6] của Luận án.
- *Lược đồ cơ sở LD 2.02*: là sự kết hợp lược đồ cơ sở LD 2.01 và thuật toán mật mã El Gamal nhằm bảo đảm đồng thời các yêu cầu về bảo mật và xác thực thông tin. Kết quả này được thể hiện ở công trình số [8] của Luận án.
- *Các lược đồ chữ ký số tập thể*: được phát triển từ các lược đồ cơ sở theo mô hình ứng dụng mới đề xuất, nhằm đáp ứng các yêu cầu chứng thực các thông điệp dữ liệu trong các giao dịch điện tử áp dụng trong các tổ chức xã hội, cơ quan hành chính nhà nước, các doanh nghiệp,... Kết quả này được thể hiện ở công trình số [4,5,6,8] của Luận án.