Nghiên cứu xây dựng lược đồ chữ ký số tập thể

Research and Construction of Digital Multi-Signature Schemes

Lưu Hồng Dũng

Abstract: *This paper proposed two new digital signature schemes has the option of using keys as follows: use a unique key; use two keys, both of which key value does not change; use two keys, primary key is fixed, subkey change with each time to sign. The paper also offers analysis on the safety of the proposed schemes, has shown the ability to apply it in practice.*

I. ĐẶT VẤN ĐỀ

Chữ ký số (Digital Signature) được sử dụng để chứng thực các văn bản trong các giao dịch điện tử, nhằm đáp ứng các yêu cầu về: tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm [1,2]. Ở các lược đồ chữ ký số như ElGamal, Schnorr, chuẩn chữ ký số DSS của Mỹ hay GOST R34.10-94 của Liên bang Ngay,... khóa bí mật được sử dụng với mục đích: xác thực và chống giả mạo chữ ký. Do đó nó phải được giữ cố định đối với mọi văn bản ký, nhưng việc phải được giữ cố định sẽ làm cho nó có thể bị bẻ một cách dễ dàng. Để chống lại việc bẻ khóa, các lược đồ dạng trên phải sử dụng một khóa bí mật thứ hai, khóa này cần phải được thay đổi theo từng văn bản ký, hơn nữa giá trị của nó cho mỗi lần ký không được trùng với các giá trị đã sử dụng ở những lần ký trước đó. Như vậy, có thể nói rằng các lược đồ nói trên thuộc dạng sử dụng khóa một lần, trước mỗi lần ký đều phải sinh khóa mới, trên thực tế giá trị của khóa thứ 2 trước mỗi lần ký được tạo ra bởi một bộ sinh số ngẫu nhiên. Bài báo này đề xuất một giải pháp mà có thể đưa các lược đồ trên về dạng sử dụng một khóa cho nhiều lần ký khác nhau, điều đó có thể giúp cho việc triển khai thực hiện được thuận tiện hơn mà không làm giảm độ an toàn của các lược đồ này.

II. XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ

Các lược đồ chữ ký số được đề xuất ở đây xây dựng trên cơ sở bài toán logarit rời rạc tương tự như các hệ chữ ký số Elgamal [3], chuẩn chữ ký số DSS của Mỹ [4], hay chuẩn chữ ký số của Liên bang Nga GOST R34.10-94 [5]. Trong đó, lược đồ chữ ký tập thể được phát triển từ lược đồ chữ ký cơ sở có dạng như sau:

1. Lược đồ chữ ký cơ sở - LD 1.01

1.1. Thuật toán hình thành và kiểm tra chữ ký số

a) Hình thành các tham số công khai:

+ Phát sinh cặp số nguyên tố p và q đủ lớn và: $q|(p-1)$.

+ Phát sinh $g = \alpha^{(p-1)/q} \bmod p$, là phần tử sinh có bậc q của nhóm Z_p^*, nghĩa là: $1 < g < p$ và: $g^q \equiv 1 \bmod p$. Ở đây: $\alpha \in Z_p^*$.

Các giá trị *(p, q, g)* là các tham số công khai trong quá trình hình thành và kiểm tra chữ ký.

b) Hình thành khóa công khai:

Thủ tục hình thành khóa công khai bao gồm các bước thực hiện sau:

1- Khóa bí mật x là một giá trị được chọn ngẫu nhiên trong khoảng: $1 < x < q-1$.

2- Khóa công khai được tính theo công thức:

$$y = g^{-x} \bmod p .$$

3- Công khai y.

c) Hình thành chữ ký số:

Thủ tục hình thành chữ ký được thực hiện theo các bước như sau:

1- Chọn k thỏa mãn: $1 < x < q-1$.Tính ***r*** theo công thức:

$$r = g^{h(k\|M)} \bmod p;$$

2- Thành phần thứ nhất ***e*** của chữ ký được tính theo công thức :

$$e = h(r \| M) \bmod q$$

3- Thành phần thứ hai ***s*** của chữ ký được tính theo công thức:

$$s = h(k \| M) + x.e \bmod q$$

4- Cặp giá trị (e, s) là chữ ký vào văn bản *M*.

Chú ý:

+ *h()* là hàm băm kháng va chạm mạnh. Ví dụ: nếu chọn |*q*| = 160 bit thì hàm băm có thể chọn là SHA-1.

+ Toán tử || là phép nối xâu.

d) Kiểm tra chữ ký số:

Thủ tục kiểm tra được thực hiện qua các bước sau:

1- Tính:

$$r' = g^s.y^e \bmod p;$$

2- Tính:

$$e' = h(r' \| M) \bmod q$$

3- Kiểm tra nếu: *e' = e* thì tính hợp lệ của chữ ký và tính toàn vẹn của văn bản cần thẩm tra được công nhận. Ngược lại, chữ ký đã bị giả mạo hoặc nội dung văn bản đã bị sửa đổi.

1.2. Tính đúng đắn của lược đồ được đề xuất

Tính đúng đắn của lược đồ được đề xuất ở đây là sự phù hợp giữa thuật toán hình thành chữ ký với thuật toán xác minh chữ ký. Điều cần chứng minh là: Phù hợp với lược đồ LD 1.01 tồn tại tồn tại đẳng thức: $e' = e$.

Chứng minh:

Từ tính hợp lệ của chữ ký *(e,s)* ta có:

$$\begin{aligned} r' &= g^s.y^e \bmod p \\ &= g^{h(k\|M)+x.e \bmod q}.(g^{-x})^e \bmod p \\ &= g^{h(k\|M)}.g^{x.e}.g^{-x.e} \bmod p \\ &= g^{h(k\|M)} \bmod p = r \end{aligned}$$

Từ tính toàn vẹn của văn bản *M* suy ra:

$$\begin{aligned} e' &= h(r' \| M) \bmod q \\ &= h(r \| M) \bmod q = e \end{aligned}$$

Đây là điều cần chứng minh.

1.3. Mức độ an toàn của lược đồ mới đề xuất

Ở lược đồ mới đề xuất, có thể thấy rằng công thức tính thành phần thứ hai (*s*) của chữ ký tương tự như GOST R34.10-94 hay lược đồ chữ ký Schnorr. Tuy nhiên, ở lược đồ mới đề xuất đã sử dụng giá trị $h(k \| M)$ thay cho *k* như trong lược đồ chữ ký Schnorr hay thay cho $k.h(M)$ trong GOST R34.10-94. Vì vậy, nếu giá trị $h(k \| M)$ tương đương với giá trị *k* trong lược đồ chữ ký Schnorr hay tương đương với $k.h(M)$ trong GOST R34.10-94 thì mức độ an toàn của lược đồ mới đề xuất sẽ hoàn toàn tương đương với 2 lược đồ chữ ký kia.

Ta xét việc chọn *k* theo 3 phương án như sau:

- Chọn k = x: Trường hợp này ta có lược đồ chỉ sử dụng một khóa với một lần chọn duy nhất. Dễ dàng thấy rằng, giá trị $h(k \| M)$ là sự kết hợp của 3 yếu tố: bí mật (khóa mật ***x***), ngẫu nhiên (văn bản cần ***M***) và một chiều (hàm băm ***h()***) nên giá trị $h(x \| M)$ hoàn toàn thỏa mãn các yêu cầu thay thế cho giá trị *k* được sinh ra bằng một thuật toán sinh số ngẫu nhiên. Một điều rõ ràng là không ai có thể tính được giá trị này ngoài người ký (chỉ người ký mới biết khóa mật ***x***), giá trị này thay đổi theo từng văn bản ký và quan trọng nhất: nó là duy nhất đối với mọi văn bản (mỗi văn bản chỉ được ký một lần), hơn nữa với số lượng văn bản cần ký *M* không đủ lớn thì không thể tính được $(x \| M)$ từ $h(x \| M)$ (tấn công hàm băm theo kiểu "ngày sinh") để từ đó có thể tính ra ***x***.
- Chọn $k \neq x$ nhưng cũng chỉ cần chọn một lần duy nhất và giữ cố định như *x*. Cách này hoàn toàn tương tự như cách thứ nhất.
- Chọn ngẫu nhiên *k* bằng cách sử dụng một bộ sinh số ngẫu nhiên tương tự như trong DSS hay GOST R34.10-94,...thì giá trị $h(x \| M)$ hoàn toàn tương đương với *k* về khía cạnh an toàn.

Ta thấy rằng, do thành phần ***r*** được tính theo công thức:

$$r = g^{h(k\|M)} \bmod p$$

nên để tính $h(k \| M)$ từ ***r***, rồi từ đó tính khóa ***x***, theo công thức:

$$s = h(k \| M) + x.e \bmod q$$

kẻ tấn công buộc phải giải bài toán logarit rời rạc.

Mặt khác, với công thức tính thành phần thứ hai **s** của chữ ký:

$$s = h(k \| M) + x.e \bmod q$$

kẻ tấn công cũng không thể giải được hệ phương trình:

$$s_1 = h(k \| M_1) + x.e_1 \bmod q$$

$$s_2 = h(k \| M_2) + x.e_2 \bmod q$$

cho dù giá trị của k được giữ nguyên, để từ đó có thể tính được khóa bí mật *x*. ở đây: (e_1, s_1) và (e_2, s_2) là chữ ký tương ứng với 2 văn bản M_1 và M_2.

Như vậy, để ký vào các văn bản khác nhau người ký cần chọn một cặp khóa (x, k), trong đó khóa chính ***x*** được giữ cố định, khóa phụ ***k*** có thể là cố đinh hoặc thay đổi theo từng văn bản ký. Trường hợp, nếu chọn *k* thay đổi theo từng văn bản ký thì cũng không cần thiết phải sử dụng bộ sinh số ngẫu nhiên như ở các lược đồ khác, vì lược đồ này cho phép sử dụng các giá trị của *k* trùng nhau mà không làm giảm độ an toàn của lược đồ. Hơn nữa nếu chọn $k = x$ thì lược đồ chỉ cần duy nhất 1 khóa bí mật mà không làm giảm mức độ an toàn, nếu so sánh với các lược đồ như Schnorr hay GOST R34.10-94.

2. Lược đồ chữ ký tập thể- LD 1.02

Giả thiết rằng nhóm người có thẩm quyền ký gồm *n* thành viên, để ký vào văn bản *M*. Cần lưu ý rằng, trong lược đồ này đại diện nhóm không nhất thiết và nói chung không phải là một thành viên trong nhóm, trên thực tế vai trò của đại diện nhóm có thể do một cơ quan chuyên trách đảm nhiệm.

2.1. Thuật toán hình thành và kiểm tra chữ ký

a) Hình thành các tham số công khai:

Các giá trị *(p, q, g)* là các tham số công khai được hình thành tương tự như ở lược đồ LD 1.01

b) Hình thành khóa công khai tập thể:

Thủ tục hình thành khóa công khai tập thể bao gồm các bước như sau:

1- Mỗi thành viên chọn khóa bí mật x_i thỏa mãn: $1 < x_i < q - 1]$ và tính khóa công khai cá nhân tương ứng:

$$y_i = g^{-x_i} \bmod p \text{ , i = 1, 2, ..., n.}$$

2- Khóa công khai tập thể được đại diện nhóm tính theo công thức:

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

3- Công khai Y.

Chú ý:

Để chống giả mạo trong việc hình thành khóa công khai tập thể Y thì các khóa công khai cá nhân y_i cần phải được công khai trong nhóm và mọi thành viên của nhóm ký đều phải tham gia tính khóa công khai tập thể Y, chỉ khi nào có sự xác nhận của tất cả các thành viên thì Y mới được công bố làm khóa công khai tập thể của nhóm ký.

c) Hình thành chữ ký tập thể:

Thủ tục hình thành chữ ký tập thể bao gồm các bước như sau:

1 - Mỗi thành viên chọn k_i thỏa mãn $1 < k_i < q - 1]$ và tính thành phần thứ nhất của chữ ký cá nhân theo công thức:

$$r_i = g^{h(k_i \| M)} \bmod p \text{ , i = 1, 2, ..., n.}$$

rồi gửi cho đai diện. Ở đây: *h()* là hàm băm được chọn đủ an toàn, chẳng hạn: SHA-1 và toán tử || là phép nối 2 xâu.

2- Đại diện nhóm tính:

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

rồi tính thành phần thứ nhất của chữ ký tập thể:

$$E = h(R \| M) \bmod q$$

Sau đó đại diện nhóm gửi giá trị *E* cho các thành viên trong nhóm

3- Các thành viên trong nhóm tính phần thứ hai của chữ ký cá nhân theo công thức:

$$s_i = h(k_i \| M) + x_i.E \bmod q \text{ , i = 1, 2, ..., n.}$$

rồi gửi s_i cho đại diện nhóm. Cặp giá trị (r_i, s_i) là

chữ ký cá nhân của thành viên thứ *i* vào văn bản *M*.

4- Sau khi nhận được tất cả chữ ký cá nhân (r_i, s_i) của các thành viên, đại diện nhóm kiểm tra sự hợp lệ của các chữ ký này bằng cách tính:

$$r_i^{'} = y_i^E . g^{s_i} \bmod p \text{ , i = 1, 2, ..., n.}$$

và:

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

Kiểm tra nếu: $R' = R$ thì tính hợp lệ các chữ ký cá nhân của các thành viên được công nhận, đại diện nhóm sẽ tính thành phần thứ hai của đa chữ ký theo công thức:

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

5- Phát hành (E, S) cùng văn bản *M*.

Chú ý:

+ Để chống giả mạo trong việc tính R thì các giá trị r_i cần phải được công khai trong nhóm và mọi thành viên của nhóm ký đều phải tham gia tính R, chỉ khi nào có sự xác nhận của tất cả các thành viên thì R mới được sử dụng để tính thành phần thứ nhất E của chữ ký tập thể..

+ Có thể sử dụng cặp (R, S) làm chữ ký của nhóm lên M thay cho cặp (E, S). Tuy nhiên cần lưu ý đến độ dài của chữ ký trong 2 trường hợp như sau: Giả sử chọn |p| = 1024 bit và |q| = 160 bit, khi đó nếu chọn cặp (R, S) là chữ ký thì độ dài của chữ ký sẽ là: |p| + |p| = 1024 bit + 1024 bit = 2048 bit. Còn nếu chọn cặp (E, S) làm chữ ký thì độ dài của chữ ký trong trương hợp này là: |p| + |q| = 1024 bit + 160 bit = 1184 bit. Rõ ràng việc chọn cặp (E, S) làm chữ ký đã giúp cho độ dài của chữ ký được rút ngắn đáng kể.

+ Tương tự như lược đồ LD 1.01, lược đồ được đề xuất ở đây có 3 phương án sử dụng khóa như sau:

- Sử dụng một khóa duy nhất: khi chọn $k_i = x_i$, i = 1, 2,...,n.
- Sử dụng 2 khóa với giá trị được chọn khác nhau, nhưng đều được giữ cố định.
- Sử dụng 2 khóa: trong đó khóa thứ nhất (x_i) được giữ cố định, còn khóa thứ hai (k_i) thay đổi ở mỗi lần ký như các lược đồ hiện tại (DSS, GOST R34.10-94,...) đang dùng.

d) Kiểm tra đa chữ ký số:

Thủ tục kiểm tra được thực hiện qua các bước sau:

1- Từ cặp *(E,S)* nhận được tính:

$$R'' = g^S . Y^E \bmod p$$

2- Tính:

$$E' = h(R'' \| M) \bmod q$$

3- Kiểm tra nếu: $E' = E$ thì chữ ký là hợp lệ và tính toàn vẹn của văn bản được bảo đảm. Ngược lại, chữ ký đã bị giả mạo hoặc nội dung của văn bản đã bị thay đổi.

2.2. Tính đúng đắn của lược đồ mới xây dựng

Tính đúng đắn của lược đồ mới đề xuất thể hiện qua tính đúng đắn của thủ tục kiểm tra chữ ký cá nhân và tính đúng đắn của thủ tục kiểm tra chữ ký tập thể như sau:

a) Tính đúng đắn của thủ tục kiểm tra chữ ký cá nhân

Tính đúng đắn của thủ tục kiểm tra chữ ký cá nhân là sự phù hợp giữa phương pháp hình thành chữ ký cá nhân với phương pháp kiểm tra tính hợp lệ của chữ ký cá nhân mà lược đồ đã đề xuất. Điều cần chứng minh ở đây là:

Với:

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

trong đó: $r_i^{'} = s^{s_i} . y_i^E \bmod p$, i = 1, 2, ..., n.

Nếu: $R' = R$ thì chữ ký cá nhân của tất cả các thành viên trong nhóm là hợp lệ. Nói cách khác là không có bất kỳ sự giả mạo nào trong các chữ ký cá nhân của các thành viên trong nhóm.

Chứng minh:

Thật vậy, theo định nghĩa:

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

và:

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

Vì vậy, nếu $R' = R$ thì: $r_i' = r_i$ với: i = 1,2,...n.

Giả sử thành phần thứ 2 của chữ ký cá nhân cần thẩm tra là: $s_i = h(k_i' \| M') + x_i'.E \bmod q$

Nên:

$$\begin{aligned} r_i' &= g^{s_i}.y_i^E \bmod p \\ &= g^{h(k_i'\|M')+x_i'.E \bmod q}.g^{-x_i.E} \bmod p \\ &= g^{h(k_i'\|M')}.g^{x_i'.E}.g^{-x_i.E} \bmod p \end{aligned}$$

Nếu: $(r_i' = r_i)$ với: i = 1,2,...n. thì:

$$\begin{aligned} & g^{h(k_i'\|M')}.g^{x_i'.E}.g^{-x_i.E} \bmod p \\ & = g^{h(k_i\|M)} \bmod p \end{aligned} \quad (1)$$

Từ (1) suy ra:

$x_i' = x_i$, $k_i' = k_i$ và M' = M.

Như vậy (r_i, s_i) thực sự là chữ ký cá nhân của thành viên thứ *i*, nói cách khác chữ ký này là hợp lệ.

b) Tính đúng đắn của thủ tục kiểm tra chữ ký tập thể

Tính đúng đắn của thủ tục kiểm tra chữ ký tập thể là sự phù hợp giữa phương pháp hình thành chữ ký tập thể với phương pháp kiểm tra tính hợp lệ của chữ ký tập thể và tính toàn ven của văn bản được ký mà lược đồ đã đề xuất. Điều cần chứng minh ở đây là:

Với:

$$R'' = g^S.Y^E \bmod p$$

và:

$$E' = h(R''\| M) \bmod q$$

Nếu: $E' = E$ thì chữ ký là hợp lệ và tính toàn vẹn của văn bản cần thẩm tra được bảo đảm.

Chứng minh:

Theo định nghĩa ta có:

$$E = h(R \| M) \bmod q$$

và:

$$E' = h(R''\| M) \bmod q$$

Nếu $E' = E$ thì suy ra:

$$h(R''\| M) \bmod q = h(R \| M) \bmod q \quad (2)$$

Từ (2) suy ra văn bản cần thẩm tra cũng chính là văn bản được ký hay tính toàn vẹn của văn bản được bảo đảm và: $R'' = R$.

Xét thành phần S của chữ ký cần thẩm tra, theo định nghĩa S sẽ có dạng:

$$\begin{aligned} S &= \sum_{i=1}^{n} s_i \bmod q \\ &= \sum_{i=1}^{n} h(k_i'\| M) + x_i'.E \bmod q \\ &= \sum_{i=1}^{n} h(k_i'\| M) \bmod q + \sum_{i=1}^{n} x_i'.E \bmod q \end{aligned}$$

Nên:

$$\begin{aligned} R'' &= g^S.Y^E \bmod p \\ &= g^{\sum_{i=1}^{n} h(k_i'\|M) \bmod q + \sum_{i=1}^{n} x_i'.E \bmod q}.(g^{-\sum_{i=1}^{n} x_i \bmod q})^E \bmod p \\ &= g^{\sum_{i=1}^{n} h(x_i'\|M) \bmod q}.g^{\sum_{i=1}^{n} x_i'.E \bmod q}.g^{-\sum_{i=1}^{n} x_i.E \bmod q} \bmod p \end{aligned}$$

Mặt khác, theo định nghĩa ta có:

$$R = \prod_{i=1}^{n} r_i \bmod p = g^{\sum_{i=1}^{n} h(x_i\|M) \bmod q} \bmod p$$

Vì vậy, nếu $R'' = R$ thì:

$$\begin{aligned} & g^{\sum_{i=1}^{n} h(k_i'\|M) \bmod q}.g^{\sum_{i=1}^{n} x_i'.E \bmod q}.g^{-\sum_{i=1}^{n} x_i.E \bmod q} \bmod p \\ & = g^{\sum_{i=1}^{n} h(k_i\|M) \bmod q} \bmod q \end{aligned}$$

Từ đây suy ra:

$x_i' = x_i$ và $k_i' = k_i$, với: i = 1,2,....n.

Như vậy (E,S) hợp lệ, đây là điều cần phải chứng minh.

2.3. Mức độ an toàn của lược đồ mới xây dựng

Mức độ an toàn của các lược đồ chữ ký số được đánh giá bằng khả năng chống lại các kiểu tấn công khác nhau:

- Tấn công bằng cách tính khóa mật.
- Tấn công theo kiểu giả mạo chữ ký.

Ở kiểu tấn công thứ nhất, kẻ tấn công phải giải bài toán logarith rời rạc mà khả năng thành công là rất thấp nếu các tham số *(p, q)* được lựa chọn thích hợp. Ở kiểu tấn công thứ 2, tồn tại một số phương pháp giả mạo như sau:

Phương pháp thứ nhất:

Xét trường hợp kẻ mạo danh muốn giả mạo chữ ký của thành viên thứ *m* trong nhóm, Do không biết (x_m, k_m) kẻ mạo danh sẽ phải thực hiện như sau:

1- Chọn $k_m^* \in [1, q-1]$ thay cho k_m của thành viên thứ *m* và tính:

$$r_m^* = g^{h(k_m^* \| M)} \bmod p;$$

2- Khi đó thành phần R sẽ là :

$$R = r_1.r_2...r_m^*...r_n \bmod p$$

và E sẽ là: $E = h(R \| M) \bmod q$

3- Kẻ mạo danh giả thành phần thứ 2 trong chữ ký cá nhân của thành viên thứ *m* như sau:

$$s_m^* = h(k_m^* \| M) + x_m^*.E \bmod q$$

Ở đây x_m^* là giá trị giả mạo.

4- Thành phần S của chữ ký tập thể khi đó sẽ là:

$$S = s_1 + s_2 + ... + s_m^* + ... + s_n \bmod q$$

Cặp (E, S) là chữ ký tập thể lên văn bản *M*, mà trong đó có chứa chữ ký giả mạo (r_m^*, s_m^*).

Khi thẩm tra chữ ký, thủ tục kiểm tra sẽ phát hiện sự giả mạo này như sau:

Theo định nghĩa, ta có:

$$S = \sum_{i=1}^{n} s_i \bmod q = h(k_1 \| M) + h(k_2 \| M) + ...$$
$$+ h(k_n \| M) + (x_1 + x_2 + ... + x_n).E \bmod q$$
$$= \sum_{i=1}^{n} h(k_i \| M) + \sum_{i=1}^{n} (x_1 + x_2 + ... + x_n).E \bmod q$$

Nên:

$$R'' = g^S.Y^E \bmod p =$$
$$g^{h(k_1\|M)+h(k_2\|M)+...+h(k_m^*\|M)+...+h(k_n\|M)+(x_1+x_2+...+x_m^*+...+x_n).E}.$$
$$g^{(-x_1-x_2-...-x_m-...-x_n).E} \bmod p =$$
$$g^{h(k_1\|M)+h(k_2\|M)+...+h(k_m^*\|M)+...+h(k_n\|M)}.$$
$$g^{(x_1+x_2+...+x_m^*+...+x_n).E}.g^{-(x_1+x_2+...+x_m+...+x_n).E} \bmod p =$$
$$= R.g^{x_m^*}.g^{-x_m} \bmod p \neq R$$

Do đó: $E' = h(R'' \| M) \bmod q \neq h(R \| M)$

hay: $E' \neq E$

Như vậy là chữ ký không hợp lệ và việc giả mạo đã bị thủ tục kiểm tra phát hiện. Tuy nhiên, cũng cần phải thấy rằng việc giả mạo như trên chỉ thực hiện được khi kẻ mạo danh là đại diện nhóm. Trong trường hợp kẻ mạo danh không phải là đại diện nhóm thì việc giả mạo sẽ bị phát hiện bởi thủ tục kiểm tra tính hợp lệ của chữ ký cá nhân như sau:

$$r_m^{'} = y_m^E.g^{s_m} \bmod p$$
$$= (g^{-x_m})^E.g^{h(k_m^*\|M)+x_m^*.E \bmod q} \bmod p$$
$$= g^{-x_m.E}.g^{h(k_m^*\|M)}.g^{x_m^*.E} \bmod p$$
$$= r_j^*.g^{-x_m.E}.g^{x_m^*.E} \bmod p \neq r_m^*$$

Do đó: $R' = \prod_{i=1}^{n} r_i^{'} \bmod p \neq R$

Việc giả mạo đã bị phát hiện do không thỏa mãn điều kiện của thủ tục kiểm tra chữ ký cá nhân.

Phương pháp thứ hai:

Giả sử kẻ mạo danh là thành viên thứ nhất muốn giả mạo chữ ký của thành viên thứ *m* trong nhóm. Kẻ mạo danh sẽ thực hiện các bước sau:

1- Tính khóa công khai cá nhân:

$$y_1 = y_m^{-1} \bmod p$$

2- Tính thành phần thứ nhất của chữ ký cá nhân: $r_1 = r_m^{-1} \bmod p$

3- Tính thành phần thứ 2 của chữ ký cá nhân: $s_1 = -s_m \bmod q$

Do đó:

$$Y = y_1.y_2...y_m...y_n \bmod p$$
$$= y_2...y_{m-1}.y_{m+1}...y_n \bmod p$$
$$R = r_1.r_2...r_m...r_n \bmod p$$
$$= r_2...r_{m-1}.r_{m+1}...r_n \bmod p$$
$$S = s_1 + s_2 + ... + s_m + ... + s_n \bmod p$$
$$= s_2 + ... + s_{m-1} + s_{m+1} + ... + s_n \bmod p$$

Chữ ký *(E,S)* được tạo ra hoàn toàn phù hợp với thủ tục kiểm tra. Thật vậy, khi tính R'' bằng công thức: $R'' = g^S.Y^E \bmod p$, ta sẽ có:

$$R'' = g^{(s_2+s_3+...+s_{m-1}+s_{m+1}+...+s_n)}.$$
$$(y_2.y_3...y_{m-1}.y_{m+1}...y_n)^E \bmod p$$
$$= g^{s_2}.g^{s_3}...g^{s_{m-1}}.g^{s_{m+1}}...g^{s_n}.$$
$$(g^{-x_2}.g^{-x_3}...g^{-x_{m-1}}.g^{-x_{m+1}}...g^{-x_n})^E \bmod p$$
$$= g^{h(k_2\|M)+x_x.E}.g^{h(k_3\|M)+x_3.E}...g^{h(k_{m-1}\|M)+x_{m-1}.E}.$$
$$g^{h(k_{m+1}\|M)+x_{m+1}.E}...g^{h(k_n\|M)+x_n.E}.g^{-x_2.E}.g^{-x_3.E}...$$
$$g^{-x_{m-1}.E}.g^{-x_{m+1}.E} \bmod p = g^{h(k_2\|M)}.g^{h(k_3\|M)}...$$
$$g^{h(k_{m-1}\|M)}.g^{h(k_{m+1}\|M)}...g^{h(k_n\|M)} \bmod p$$
$$= r_2.r_3...r_{m-1}.r_{m+1}...r_n \bmod p = R$$

Nếu văn bản không bị sửa đổi, ta có:

$$E' = h(R''\| M') \bmod q$$
$$= h(R \| M) \bmod q = E$$

Chữ ký đã được xác nhận là hợp lệ. Bằng cách đó thành viên thứ nhất đã mạo danh được thành viên thứ *m*, và nói chung là có thể mạo danh được bất kỳ thành viên nào trong nhóm ký. Hơn nữa, phương pháp giả mạo này có thể áp dụng cho bất kỳ lược đồ chữ ký tập thể nào.

Về mặt toán học, phương pháp giả mạo này là hoàn toàn đúng. Tuy nhiên, ta hãy xét tính thực tiễn của nó, ở đây có 2 vấn đề:

Thứ nhất, việc tính khóa công khai cá nhân của kẻ mạo danh: $y_1 = y_m^{-1} \bmod p$ là không thể thực hiện được nếu có một cơ chế kiểm tra chặt chẽ khi hình thành khóa công khai tập thể *Y*. Giả sử việc tính khóa công khai cá nhân của kẻ mạo danh (y_1) như trên không bị phát hiện thì kẻ mạo danh cũng chỉ có thể thực hiện giả mạo được với thành viên thứ *m*, mà không thể giả mạo với các thành viên khác được, vì khóa công khai tập thể *Y* sau khi đã được công bố thì không thể tùy ý thay đổi theo từng văn bản ký.

Thứ hai, ta thấy rằng điều kiện tiên quyết để phương pháp này thực hiện được là kẻ mạo danh phải biết được chữ ký cá nhân của thành viên mà chúng muốn giả mạo chữ ký. Chính điều đó đã hạn chế khả năng ứng dụng của phương pháp này trong thực tiễn. Vì rằng, kẻ mạo danh chỉ có thể biết được chữ ký cá nhân của những thành viên mà chúng muốn giả mạo chữ ký khi họ đã đồng ý ký vào văn bản và gửi chữ ký cá nhân của mình cho nhóm. Nhưng giả mạo chữ ký của thành viên đã ký vào văn bản là một việc làm vô nghĩa và không đúng với bản chất của sự giả mạo. Hơn nữa, không thể lấy chữ ký cá nhân của một thành viên lên văn bản này để giả mạo chữ ký của họ với các văn bản khác được, vì thành phần *s* của chữ ký cá nhân phụ thuộc vào giá trị băm (bản tóm lược) của văn bản được ký, khi nội dung văn bản bị thay đổi thì chữ ký cá nhân của các thành viên mà chúng muốn mạo danh không còn phù hợp để tạo chữ ký cho văn bản đã bị sửa đổi nữa, điều đó đồng nghĩa với việc kẻ giả mạo không có được chữ ký cá nhân của những thành viên mà chúng muốn mạo danh, do đó không thể thực hiện việc giả mạo theo phương pháp này được.

Phương pháp thứ 3:

Ta cũng xét trường hợp kẻ mạo danh là thành viên thứ nhất muốn giả mạo chữ ký của thành viên thứ *m* trong nhóm. Kẻ mạo danh sẽ thực hiện các bước sau:

1- Tính thành phần thứ nhất của chữ ký cá nhân:

$$r_1 = g^{h(k_1\|M)}.r_m \bmod p$$

2- Tính thành phần thứ 2 của chữ ký cá nhân:

$$s_1 = h(k_1 \| M) + x_1.E + s_m \bmod q$$

Do đó:

$$R = r_1.r_2...r_{m-1}.r_{m+1}...r_n \bmod p$$
$$= g^{h(k_1\|M)}.g^{h(k_2\|M)}...g^{h(k_{m-1}\|M)}.$$
$$.g^{h(k_m\|M)}.g^{h(k_{m+1}\|M)}....g^{h(k_n\|M)} \bmod p$$
$$= \prod_{i=1}^{n} r_i \bmod p$$

Và:

$$S = s_1 + s_2 + ... + s_{m-1} + s_{m+1}... + s_n \bmod p$$
$$= h(k_1 \| M) + x_1.E + h(k_2 \| M) + x_2.E + ...$$
$$+ h((k_{m-1} \| M) + x_{m-1}.E + h(k_m \| M) + x_m.E +$$
$$+ h(k_{m+1} \| M) + x_{m+1}.E + ...$$
$$+ h(k_n \| M) + x_n.E \bmod q$$
$$= \sum_{i=1}^{n} h(k_i \| M) + x_i.E \bmod q = \sum_{i=1}^{n} s_i \bmod q$$

Điều đó cho thấy rằng, nhóm ký vẫn tạo ra được chữ ký hợp lệ với đầy đủ *n* thành viên mà không cần

sự có mặt của thành viên thứ *m*. Tuy nhiên, phương pháp giả mạo này đã thực hiện không đúng với yêu cầu của lược đồ đưa ra. Xem xét lại công thức tính R và S của lược đồ: $R = \prod_{i=1}^{n} r_i \bmod p$

và: $S = \sum_{i=1}^{n} s_i \bmod q$

Các công thức trên đã chỉ ra một cách rõ ràng rằng, chữ ký tập thể phải được tạo ra từ *n* chữ ký cá nhân của các thành vên trong nhóm và nó chỉ được tạo ra khi có đầy đủ số lượng chữ ký cá nhân của các thành viên. Ở mức thực thi bằng chương trình, việc tính R và S có thể được thực hiện bằng các vòng lặp như sau:

```
    R := 1;
For i := 1 to n do
    R := R *  ri ;
Hay:
    S:=0;
    i := 1;
While (i <=n) do
  Begin
     S := S + si ;
     i := i +1 ;
  End
```

Rõ ràng là 2 vòng lặp trên không thể kết thúc được nếu không có đủ số lượng chữ ký cá nhân của các thành viên trong nhóm, nghĩa là chữ ký tập thể không được tạo ra nếu không đủ số lượng thành viên tham gia ký. Như vậy, nếu ở mức giao thức và mức thực thi (bằng phần cứng hay phần mềm) có cơ chế kiểm soát tốt việc thực hiện các yêu cầu mà lược đồ đã chỉ ra thì phương pháp giả mạo trên sẽ không thể áp dụng được.

Phương pháp này có ưu điểm là kẻ mạo danh không cần phải tính khóa công khai cá nhân của mình theo khóa công khai cá nhân của thành viên mà chúng muốn mạo danh như ở phương pháp thứ hai, điều đó làm cho phương pháp giả mạo này phù hợp với thực tế hơn. Tuy nhiên, về bản chất phương pháp này cũng giống như phương pháp thứ hai, kẻ mạo danh chỉ thực hiện giả mạo được chữ ký của những thành viên trong nhóm khi chúng biết được chữ ký cá nhân mà chúng đang muốn giả mạo. Trường hợp dù có được chữ ký cá nhân ở những lần ký trước đó của thành viên mà chúng đang muốn giả mạo thì kẻ mạo danh cũng không thể áp dụng phương pháp giả mạo này được. Ta xét một trường hợp cụ thể, mà ở đó kẻ mạo danh có thể là n-1 thành viên muốn giả mạo chữ ký của thành viên thứ *n* trong nhóm. Kẻ mạo danh được chọn là một thành viên, chẳng hạn thành viên thứ 1, kẻ mạo danh chọn cho mình (r_1,s_1) của lần ký mới này như sau:

1- Tính thành phần thứ nhất của chữ ký cá nhân: $r_n' = (r_n)^{r_1} \bmod p$

2- Tính thành phần thứ 2 của chữ ký cá nhân: $s_n' = s_n.r_1 \bmod q$

Với lưu ý: ở đây người giả mạo chỉ cần lấy r_n , s_n cũ của lần 1 lần ký trước đó mà thành viên m đã ký (có mang thông tin về x_n), chứ không phải của lần ký này.

Nhóm n-1 người thay cặp $(r_n'$, $s_n')$ mới qua mặt người thứ n, còn n-1 thành viên, cả thứ 1, vẫn không thay đổi. *Hệ ký vẫn tỏ ra đủ n thành viên, có sử dụng khóa công khai Y vẫn hợp lý, hệ (R',S',Y,g) mới vẫn hợp lệ, tạo được sự thuyết phục rằng m thành viên đã ký vào văn bản, và hậu quả như thế nào?*

Ta biết rằng, trước khi hình thành chữ ký tập thể, thì chữ ký cá nhân của các thành viên phải được kiểm tra về tính hợp, trong trường hợp này, chữ ký cá nhân của thành viên thứ n được kiểm tra như sau :

1- Tính: $r_n'' = g^{s_n'}.y_n^E \bmod p$

2- Kiểm tra nếu $r_n'' = r_n'$ thì (r_n', s_n') là hợp lệ, ngược lại (r_n', s_n') là giả mạo.

Theo giả thiết: $r_n' = (r_n)^{r_1} \bmod p$

Và: $s_n' = s_n.r_1 \bmod q$

Ở đây: r_n và s_n là chữ ký cá nhân của thành viên thứ n trong 1 lần ký trước nào đó mà kẻ mạo danh (ở đây là thành viên thứ 1) có được.

Do: $s_n = h(k_n \| M^*) + x_n.E^* \bmod q$

Nên: $s_n' = (h(k_n \| M^*) + x_n.E^*).r_n \bmod q$

Cần lưu ý rằng, văn bản của lần ký hiện tại là M và thành phần thứ nhất của chữ ký tập thể tương ứng là E, còn M* là văn bản của lần ký trước nào đó và E* thành phần thứ nhất của chữ ký tập thể tương ứng M*.

Vì vậy:

$$r_n'' = g^{s_n'}.y_n^E \bmod p$$
$$= g^{(h(k_n\|M^*)+x_n.E^*).r_1}.(g^{-x_n})^E \bmod p$$
$$= g^{h(k_n\|M^*).r_1}.g^{x_n.E^*.r_1}.g^{-x_n.E} \bmod p$$
$$= (r_n)^{r_1}.g^{x_n.E^*.r_1}.g^{-x_n.E} \bmod p$$
$$= r_n'.g^{x_n.E^*.r_1}.g^{-x_n.E} \bmod p$$

Kết quả cho thấy là: $r_n'' \neq r_n'$, như vậy là sự giả mạo đã bị phát hiện trước khi hình thành chữ ký tập thể. Chúng ta lại giả sử rằng, sự giả mạo này không bị phát hiện (nếu đại diện nhóm cũng tham gia vào việc giả mạo này), khi đó chữ ký tập thể sẽ được hình thành như sau:

$$R = r_1.r_2...r_n' \bmod p = r_1.r_2...(r_n)^{r_1} \bmod p$$
$$= g^{h(k_1\|M)}.g^{h(k_2\|M)}....g^{h(k_n^*\|M^*).r_1} \bmod p$$
$$= g^{\sum_{i=1}^{n-1} h(k_i\|M) \bmod q}.g^{h(k_n^*\|M^*)} \bmod p$$
$$E = h(R \| M) \bmod q$$
$$S = s_1 + s_2... + s_n' \bmod q$$
$$= s_1 + s_2... + s_n.r_1 \bmod q$$
$$= h(k_1 \| M) + x_1.E + h(k_2 \| M) + x_2.E + ...$$
$$+ h(k_n^* \| M^*) + x_n.E^* \bmod q$$
$$= (\sum_{i=1}^{n-1} h(k_i \| M) + h(k_n^* \| M^*)) \bmod q$$
$$+ (E.\sum_{i=1}^{n-1} x_i + x_n.E^*) \bmod q$$

Ký hiệu k_n * để chỉ rằng đây là giá trị của *k* của thành viên n trong lần ký trước. Việc kiểm tra tính hợp lệ của chữ ký và tính toàn vẹn của văn bản đươc thực hiện như sau:

1- Tính: $R'' = g^S.Y^E \bmod p$

và: $E' = h(R'' \| M) \bmod q$

2- Kiểm tra nếu: $E' = E$ thì chữ ký là hợp lệ và tính toàn vẹn của văn bản cần thẩm tra được bảo đảm.

Từ (E,S) cần thẩm tra, ta tính R'' như sau:

$$R'' = g^S.Y^E \bmod p = g^{\sum_{i=1}^{n-1} h(k_i\|M) \bmod q}.g^{h(k_n^*\|M^*)}.$$
$$.g^{E.\sum_{i=1}^{n-1} x_i}.g^{x_n.E^*}.(g^{-\sum_{i=1}^{n} x_i})^E \bmod p$$
$$= g^{\sum_{i=1}^{n-1} h(k_i\|M) \bmod q}.g^{h(k_n^*\|M^*)}.g^{x_n.E^*}.g^{-x_n.E} \bmod p$$

Do đó:

$$E' = h(R'' \| M) \bmod q =$$
$$= h((g^{\sum_{i=1}^{n-1} h(k_i\|M) \bmod q}.g^{h(k_n^*\|M^*)}.$$
$$g^{n_n(E^*-E)} \bmod p) \| M) \bmod q$$

Trong khi đó:

$$E = h(R \| M) \bmod q$$
$$= h((g^{\sum_{i=1}^{n-1} h(k_i\|M) \bmod q}.$$
$$g^{h(k_n^*\|M^*)} \bmod p) \| M) \bmod q$$

Như vậy là: $E' \neq E$ nên tính hợp lệ của chữ ký và tính toàn vẹn của văn bản cần thẩm tra đã không được công nhận.

Có thể xem xét thêm một tình huống ứng dung phương pháp tấn công giả mạo này. Trong ví dụ này, các khóa công khai y_m của các thành viên giả thiết không thay đổi sau một số lần ký, và N-1 thành viên muốn qua mặt thành viên thứ N, giả sử là A, họ trao cho một thành viên trong nhóm, giả sử là B, ví dụ người đại diện là không trung thực trong nhóm, tấn công A như sau: Giả sử lần ký mới này, văn bản là M' có giá trị hàm băm H(M')=m', còn văn bản lần trước M có hàm băm H(M)=m.

Người B sẽ thực hiện:

a) Do q nguyên tố rất lớn, nên với xác suất hầu chắc chắn, xảy ra (m', q)=1 nên tồn tại $m'^{-1} \bmod q$.

b) chọn t tùy ý sao cho 0< t < q để t nguyên tố cùng nhau với q, p. Từ đó hệ phương trình đồng dư Trung hoa sau (i) có nghiệm:

$r'_N = (r_N)^t \bmod p$ (i1)

$r'_N = r_N.\ t.m.m'^{-1} \bmod q$ (i2)

Từ (i2) suy ra:

(ii) $r'_N.m' = r_N.\ t.m. \bmod q$

Chi tiết hơn, chẳng hạn nếu có x_N lẻ, $(-1)^{xN} \bmod p = -1$ và $g^{(p-1)/2} = -1 \bmod p$ (khi p =3 mod 4), nghĩa là thay vào (i1) với t=(p-1)/2 sẽ có $r'_N=(r_N)^t = -1 \bmod p$, ta có thể lấy đơn giản $r'_N = p-1$ thỏa phương trình (i).

Bây giờ B lấy hệ biểu diễn (*):

(iii) $r'_N = (r_N)^t \bmod p$,

$s'_N = s_N.t \bmod q$,

c) Trước hết, giả thiết trường hợp đơn giản nhất là với hệ N chữ ký mới lần này cho văn bản M', N-1 thành viên vẫn được phép sử dụng các giá trị cũ $r_1,..,r_{N-1}$, (chỉ $s_1,...,s_{N-1}$ là thay đổi), còn thành viên thứ N (bị qua mặt bởi N-1 thành viên kia) bị thay bởi cặp (r'_N,s'_N) bởi thành viên B nào đó, khi đó với hai lần ký- hiện tại và trước đây ta có:

(iv) $E' = r_1.r_2...r_{N-1}.r'_N. m' \bmod q$

và $E = r_1.r_2...r_{N-1}r_N. m \bmod q$

Ta sẽ kiểm chứng hệ thức sau vẫn thỏa mãn:

(v) $r'_N = g^{s'_N} . y_N^{E'} \bmod p$

- Trước hết, do (ii) và (iv) ta có

(vi) $E' = E.t \bmod q$,

- Sử dụng đẳng thức này và (iii), do

$s_N=k_N+x_N.E \bmod q$ của lần ký trước, ta được:

$s'_N = s_N.t = (k_N+ x_N.E).t \bmod q$

$= k_N.t + x_N.E' \bmod q$,từ đó:

$r'_N = (r_N)^t = g^{k_N.t} = g^{s'_N - x_N.E'}$

$= g^{s'_N} . y_N^{E'} \bmod p$, do vậy yêu cầu (v) thỏa mãn.

- Và nếu cần - từ 1 cặp (r'_N,s'_N) này, người B đi lấy tham số chữ ký khác qua mặt A theo kiểu tấn công thứ 3, sẽ có thể lấy cặp (r'_N,s'_N) khác nữa - cho cùng lần ký mới này. Từ đó suy ra cách mà sơ đồ vẫn hoạt động mà không cần có thành viên N.

Đây cũng là ví dụ về cách áp dụng tấn công (kiểu thứ 3) thoạt đầu có vẻ là đúng đắn, tuy nhiên nếu xem xét kỹ thì chúng ta sẽ thấy rằng nó chỉ có ý nghĩa toán học thuần túy. Bởi vì trong trường hợp này, phương pháp chỉ thành công được với giả thiết: **" ... trường hợp đơn giản nhất là với hệ N chữ ký mới lần này cho văn bản M', N-1 thành viên vẫn được phép sử dụng các giá trị cũ r_1, ..., r_{N-1}, (chỉ s_1, ..., s_{N-1} là thay đổi),.."**. Nhưng đây lại là một giả thiết rất không thực tế. Vì rằng, việc sử dụng **r** cũ thì cũng đồng nghĩa với việc dùng lại giá trị cũ của **k**, chỉ cần như thế thôi thì kẻ tấn công đã tìm ngay được **x** rồi, mà không cần dùng đến phương pháp nào nữa cả.

Từ những phân tích trên đây có thể thấy rằng lược đồ mới xây dựng là an toàn với các kiểu tấn công giả mạo đã biết trên thực tế.

III. KẾT LUẬN

Các lược đồ chữ ký số được đề xuất trong bài báo, ngoài phương án sử dụng 2 khóa như các lược đồ hiện tại, còn cho phép giữ cố định giá trị cho khóa thứ 2 hay chỉ sử dụng một khóa duy nhất khi ký vào các văn bản khác nhau mà tính an toàn của lược đồ vẫn được đảm bảo. Điều đó rất có ý nghĩa khi một người ký tham gia vào nhiều nhóm khác nhau và mỗi nhóm phải ký nhiều văn bản khác nhau. Hơn nữa, việc sử dụng một khóa cho các lần ký khác nhau sẽ cho phép việc triển khai ứng dụng lược đồ trong thực tế được thuận tiện hơn.

Bài báo cũng đưa ra những phân tích về mức độ an toàn của các lược đồ được đề xuất, cho thấy khả năng ứng dụng chúng là hoàn toàn có thể trên thực tế.

TÀI LIỆU THAM KHẢO.

[1] D.R STINSON, *Cryptography: Theory and Practice*, CRC Press 1995.

[2] WENBO MAO, *"Modern Cryptography: Theory and Practice"*, Prentice Hall PTR, 2003, p. 648.

[3] T. ElGamal. *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory. 1985, Vol. IT-31, No. 4. pp.469–472.

[4] National Institute of Standards and Technology, NIST FIPS PUB 186-3. *Digital Signature Standard*, U.S. Department of Commerce,1994.

[5] GOST R 34.10-94. Russian Federation Standard. Information Technology. *Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm*. Government Committee of the Russia for Standards, 1994 (in Russian).

[6] K. ITAKURA and K. NAKAMURA, *"A public key cryptosystem suitable for digital multisignatures"*,

NEC Research and Development, Vol. 71, 1983, pp 1-8.

[7] TATSUAKI OKAMOTO, *"A digital multisignature scheme using bijective public-key cryptosystems"*, ACM Trans. Comput. Syst., Vol.6, No. 8, 1988, pp 432–441.

[8] M. BURMESTER, Y. DESMEDT, H. DOI, M. MAMBO, E. OKAMOTO, M. TADA and Y. YOSHIFUJI, *"A structured ElGamal-type multisignature scheme"*, Proceedings of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000), Springer-Verlag, 2000, pp. 466-483.

[9] JUN ZHANG, "*Cryptographic Analysis of the Two Structured Multi-signature Schemes"*, Journal of Computational Information Systems 6:9 (2010) 3127-3135.

Nhận bài ngày:18/05/2011

SƠ LƯỢC VỀ TÁC GIẢ

LƯU HỒNG DŨNG

Sinh năm 1966.

Tốt nghiệp Đại học chuyên ngành Vô tuyến điện tử năm 1989 và Cao học ngành Kỹ thuật Điện tử và Thông tin liên lạc năm 2000 tại Học viện Kỹ thuật Quân sự.

Hiện là giảng viên Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự.

Lĩnh vực nghiên cứu: An toàn và bảo mật thông tin, An ninh mạng máy tính.

Email: luuhongdung@gmail.com