XÂY DỰNG CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ CÓ PHÂN BIỆT TRÁCH NHIỆM KÝ TUẦN TỰ DỰA TRÊN BÀI TOÁN LOGARIT RỜI RẠC VÀ KHAI CĂN

CONSTRUCTING TWO SEQUENTIAL MULTISIGNATURE SCHEMES WITH DISTINGUISHED SIGNING AUTHORITIES BASED ON DISCRETE LOGARITHM PROBLEM AND MODULO ROOT PROBLEM

Đào Tuấn Hùng[1], Nguyễn Hiếu Minh[2]

[1]Phòng Thí nghiệm trọng điểm ATTT, Hà Nội; daotuanhung@gmail.com
[2]Học viện Kỹ thuật Mật mã, Hà Nội

Tóm tắt - Bài báo đề xuất hai lược đồ chữ ký số tập thể có phân biệt trách nhiệm với cấu trúc tuần tự dựa trên bài toán Logarit rời rạc và bài toán khai căn. Các lược đồ đề xuất có hiệu quả cao, giảm chi phí tính toán, chi phí trao đổi dữ liệu và dễ dàng áp dụng trong thực tiễn. Hơn nữa, các lược đồ đề xuất an toàn với các dạng tấn công dựa trên tính khó giải của hai bài toán khó và cung cấp chứng cứ tin cậy về quá trình ký. Sự khác nhau của lược đồ chúng tôi đề xuất với lược đồ của Hwang là ở phương pháp trao đổi dữ liệu trong quá trình sinh chữ ký. So sánh cho thấy các lược đồ mới cho phép giảm tính toán và chi phí trao đổi dữ liệu, thích hợp với các ứng dụng thực tế.

Từ khóa - chữ ký số; Logarit rời rạc; bài toán khai căn; chữ ký số tập thể; tấn công giả mạo; Schnorr

Abstract - This paper proposes two sequential multi-signature schemes with distinguished signing authorities based on discrete logarithm problem and modulo root problem. The proposed schemes have high efficiency in terms of small computation, communication costs and easy application. In addition, the proposed schemes are secure with known attack types because it is hard to solve these hard problems and provide internal integrity of multi-signature generation process. The difference between our schemes and Hwang et al.'s scheme is the method of data exchange during the multi-signature generation process. Comparisons show that the new schemes allow reducing computation and communication costs, so they can be used widely in practice.

Key words - digital signature; discrete logarithm problem; root problem; multi-signature scheme; forgery attack; Schnorr

1. Đặt vấn đề

Trong các giao dịch điện tử (chính phủ điện tử, thương mại điện tử, tiền điện tử…), chữ ký số tập thể được sử dụng khi cần thiết có nhiều hơn một bên tham gia để giao dịch được tiến hành. Các dạng chữ ký số tập thể thường xuyên được sử dụng trong thực tế nhằm chia quyền xác thực từ một sang nhiều người. Lược đồ chữ ký tập thể dạng ký tuần tự có phân biệt trách nhiệm cho phép nhóm người tham gia lần lượt theo trình tự kiểm tra chữ ký trước và ký phần văn bản của mình. Đây là mô hình áp dụng cho các ứng dụng yêu cầu trình tự phê duyệt và mỗi cá nhân ký chịu trách nhiệm trên chữ ký của mình trước khi chuyển sang cho người ký tiếp theo. Chữ ký số tập thể được giới thiệu đầu tiên do Itakura và Nakamura [1], tuy nhiên trong lược đồ này mọi cá nhân chịu trách nhiệm như nhau. Lược đồ ký số tập thể có phân biệt trách nhiệm đầu tiên được Harn đưa ra [2] dựa trên bài toán Logarit rời rạc. Sau đó, Huang [3] đã đề xuất hai lược đồ chữ ký số tập thể có phân biệt trách nhiệm cấu trúc tuần tự và song song dựa trên bài toán RSA và bài toán Logarit rời rạc. Tuy nhiên các lược đồ này được chứng minh không phải là các lược đồ an toàn như ở [4, 5].

Dựa trên độ khó của bài toán Logarit rời rạc, Diffie và Hellman [6] đã đề xuất lược đồ thỏa thuận khóa Diffie – Hellman nổi tiếng vào năm 1976. Kể từ đây, nhiều giao thức mật mã khác nhau [7-10] sở hữu tính bảo mật dựa trên bài toán DLP (Discrete Logarithm Problem) đã được đề xuất. Cũng chính sự quan tâm đến các ứng dụng này, DLP đã được các nhà toán học nghiên cứu một cách rộng rãi trong suốt hai mươi năm qua. Bên cạnh các bài toán khó khác, Moldovyan lần đầu giới thiệu bài toán khó khai căn [11] và nêu rõ nếu tham số được lựa chọn đúng thì đây sẽ trở thành một bài toán khó giải trong thời gian đa thức và có độ khó tương đương với bài toán DLP, nhưng sẽ có nhiều ưu điểm hơn khi được sử dụng để xây dựng các hệ thống mật mã.

Trong bài báo này, chúng tôi đề xuất phương pháp xây dựng hai lược đồ chữ ký số tập thể các lược đồ họ Schnorr [10] có phân biệt trách nhiệm cấu trúc tuần tự, dựa trên bài toán Logarit rời rạc và bài toán khai căn và chứng minh tính an toàn của các lược đồ đề xuất. Các lược đồ đề xuất cung cấp chứng cứ của những người tham gia ký và chống được tấn công giả mạo. Không người nào tham gia quá trình ký có thể tạo ra được chữ ký hợp lệ của cả nhóm.

2. Các bài toán khó sử dụng

Bài toán Logarit rời rạc [12]: Với p và q là hai số nguyên tố lớn thỏa mãn $q \mid p-1$, α là phần tử sinh của trường Z_q có bậc q. Bài toán Logarit rời rạc là với các giá trị cho trước (y, p, q, α), $y = \alpha^x \bmod p$,với $x \in Z_q$, tìm x.

Bài toán Khai căn modulo [11, 13]: Với p, q là hai số nguyên tố lớn $(|q| \geq 160)$ theo cấu trúc $p = Nq^2 + 1$, N là số nguyên chẵn sao cho $(|p| \geq 1024)$ bit. Bài khai căn modulo là với các giá trị cho trước (y, p, q) , $y = x^q \bmod p$,với $x \in Z_q$, tìm x. Bài toán khai căn modulo được tác giả Moldovyan trình bày và đưa ra một số cải tiến cho chữ ký số DSS ở [11].

3. Xây dựng lược đồ chữ ký số tập thể phân biệt trách nhiệm cấu trúc tuần tự dựa trên bài toán logarit rời rạc (lược đồ 1)

3.1. Quá trình chuẩn bị

Giả sử rằng nhóm *n* người ký là {U_1, U_2, …, U_n} muốn sinh chữ ký tập thể cho văn bản $M = m_1 \| m_2 \| ... \| m_n$. Các thành viên ký U_i chỉ được ký trên một phần văn bản m_i với $i = 1, 2, …, n$. Có một người quản lý đảm bảo trong quá trình ký. Người quản lý sắp xếp thành viên ký U_i chỉ được xem và ký cho phần văn bản m_i tương ứng. Lược đồ cho phép phân công trách nhiệm cá nhân kiểm tra và ký cho phần văn bản của mình trước khi người sau xác thực nội dung khác.

3.2. Quá trình tạo khóa

Bước 1: Người quản lý tạo ra một số nguyên tố lớn *p*, một ước số nguyên tố *q* với $q|(p-1)$, α là phần tử sinh của các nhóm Z^*_q và $\alpha \in Z^*_q$. *(α,p,q)* là các tham số được công khai và lựa chọn sử dụng hàm một chiều SHA-1.

Bước 2: Sinh nhóm khoá bí mật của người ký tương ứng là $x_1, x_2, …, x_n$ với điều kiện $1 < x_i < q$, $i = 1, 2, …, n$. Mỗi giá trị x_i được chọn ngẫu nhiên và chỉ được biết bởi người ký U_i.

Bước 3: $y_1, y_2, …, y_n$: khóa công khai của các thành viên thỏa mãn $y_i = \alpha^{x_i} \bmod p$ được tính và được công bố bởi người ký U_i. Thêm/xóa một thành viên *i* đòi hỏi phải thêm/xóa khóa công khai y_i tương ứng bởi người quản lý.

3.3. Quá trình tạo chữ ký tập thể

Lược đồ yêu cầu người quản lý và các thành viên ký phải trao đổi dữ liệu trong quá trình ký văn bản. Trước khi ký, quản lý đã sắp xếp dãy người ký theo đúng thứ tự văn bản ký. Người ký U_i chỉ được ký vào đoạn văn bản m_i đã định sẵn, do quản lý gửi cho mỗi thành viên.

Bước 1: Mỗi người ký U_i chọn ngẫu nhiên số $0 < k_i < q$ và tính toán giá trị: $r_i = \alpha^{k_i} \bmod p$. U_i thông báo r_i cho người quản lý. Người quản lý tính giá trị hàm băm *H*: $H = h(h(m_1) \| h(m_2) \| ... h(m_n))$, tính giá trị thống nhất chung cho phiên ký: $R = \prod_{i=1}^{n} r_i \bmod p$ và $\mathrm{E} = \mathrm{h}(\mathrm{H} \| \mathrm{R})$. Giá trị E được thông báo cho các thành viên ký.

Bước 2: Người ký đầu tiên U_1 tính hàm băm $h(m_1)$ và sinh chữ ký số $s_1 = k_1 - x_1 h(m_1) \mathrm{E}$. Sau đó U_1 gửi (r_1, s_1, $h(m_1)$) đến người ký thứ hai U_2 và quản lý. Tiếp theo mỗi người ký U_i với $i = 2, 3, …, n$ lần lượt thực thực hiện bước sau.

Bước 3: Mỗi thành viên U_i kiểm tra xác thực tính đúng đắn của người ký trước theo: $\alpha^{S_{i-1}} y_{i-1}^{h(m_{i-1})\mathrm{E}} = r_{i-1} \bmod p$. Nếu phương trình này thoả mãn thì chứng tỏ thành viên ký thứ $i - 1$ tức là U_{i-1} đúng là người ký trên các văn bản trước đó lần lượt $m_1, …, m_{i-1}$. U_i tính $s_i = k_i - x_i h(m_i) \mathrm{E}$. Sau đó, U_i gửi cho thành viên ký U_{i+1} và quản lý các tham số: (r_i, s_i, $h(m_i)$). Riêng U_n gửi các tham số (r_n, s_n, $h(m_n)$) cho quản lý.

Bước 4: Quản lý xác thực chữ ký của U_n theo công thức: $\alpha^{S_n} y_n^{h(m_n)\mathrm{E}} = r_n \bmod p$. Sau đó người quản lý tính giá trị: $S = \sum_{i=1}^{n} s_i \bmod q$. Cặp (*E*, *S*) là chữ ký số tập thể cho văn bản $M = m_1 \| m_2 \| ... \| m_n$. Sau đó tính khoá công khai chung của nhóm $Y = \prod_{i=1}^{n} y_i^{h(\mathrm{m}_i)} \bmod p$

3.4. Xác thực chữ ký số tập thể

Việc xác thực chữ ký (*E*, *S*) cho tập văn bản $M = m_1 \| m_2 \| ... \| m_n$ với khóa công khai nhóm Y được thực hiện như sau: Người xác thực tính $R' = \alpha^S Y^{\mathrm{E}} \bmod p$ và $H = h(h(m_1) \| h(m_2) \| ... h(m_n))$. Kiểm tra nếu E=h(H||R'), nếu biểu thức thỏa mãn, chữ ký là hợp lệ. Nếu không, chữ ký không hợp lệ hoặc văn bản gốc đã bị thay đổi. (Người xác thực có thể tính lại $Y = \Pi_{i=1}^{n} y_i^{h(\mathrm{m}_i)} \bmod p$ nếu muốn kiểm tra tính trách nhiệm của từng thành viên theo các giá trị khóa công khai của từng thành viên và văn bản tương ứng).

3.5. Pha xác thực bằng chứng

Tất cả các chữ ký cá nhân (r_i, s_i) có thể được sử dụng làm bằng chứng, cho biết thành viên U_i là người ký phần nội dung m_i, (r_i, s_i) theo biểu thức $\alpha^{S_i} y_i^{h(m_i)\mathrm{E}} = r_i \bmod p$ cùng với chữ ký hợp lệ (E,S) của bộ tài liệu. Nếu hai điều kiện được thỏa mãn, thành viên U_i được xác thực đã ký phần nội dung m_i vì công thức $\alpha^{S_i} y_i^{h(m_i)\mathrm{E}} = r_i \bmod p$ cho thấy mối quan hệ giữa toàn bộ tài liệu, phần nội dung m_i, và thành viên U_i.

3.6. Chứng minh tính đúng

Công thức kiểm tra chữ ký cá nhân :

$$\alpha^{S_{i-1}} y_{i-1}^{h(m_{i-1})\mathrm{E}} = \alpha^{k_{i-1} - x_{i-1} h(m_{i-1})\mathrm{E}} y_{i-1}^{h(m_{i-1})\mathrm{E}} =$$
$$\alpha^{k_{i-1}} \alpha^{-x_{i-1} h(m_{i-1})\mathrm{E}} y_{i-1}^{h(m_{i-1})\mathrm{E}} = r_{i-1} y_{i-1}^{-h(m_{i-1})\mathrm{E}} y_{i-1}^{h(m_{i-1})\mathrm{E}}$$
$$= r_{i-1} \bmod p$$

Chữ ký số (E, S) là một chữ ký số tập thể hợp lệ với văn bản cần ký $M = m_1 \| m_2 \| ... \| m_n$ với nhóm người ký có khóa công khai là $y_1, y_2, .., y_n$. Thật vậy, theo pha xác thực chữ ký tính giá trị R': $R' = \alpha^S Y^{\mathrm{E}} \bmod p$, ta có

$$\alpha^S Y^E = \alpha^{\sum_{i=1}^{n} s_i} Y^E = Y^E \alpha^{\sum_{i=1}^{n} (k_i - x_i h(m_i)\mathrm{E})} =$$
$$Y^E \alpha^{\sum_{i=1}^{n} k_i} \alpha^{\sum_{i=1}^{n} x_i h(m_i)E} = Y^E \prod_{i=1}^{n} \alpha^{k_i} \prod_{i=1}^{n} \alpha^{-x_i h(m_i)\mathrm{E}}$$
$$= Y^E \prod_{i=1}^{n} r_i \prod_{i=1}^{n} y_i^{-h(m_i)E} = Y^E R \prod_{i=1}^{n} y_i^{-h(m_i)E}$$
$$= Y^E R (\prod_{i=1}^{n} y_i^{h(m_i)})^{-E} = Y^E R Y^{-E} \bmod p = R$$
$$\Rightarrow R' = R \Rightarrow E = h(Y \| \mathrm{R}').$$

Như vậy, có thể khẳng định chữ ký số tập thể có phân biệt trách nhiệm ký tuần tự được xây dựng dựa trên bài toán Logarit rời rạc, được xây dựng như phần trên là đúng đắn và hợp lệ.

4. Xây dựng lược đồ chữ ký số tập thể có phân biệt trách nhiệm cấu trúc tuần tự dựa trên bài toán khai căn (lược đồ 2)

4.1. Quá trình chuẩn bị: Tương tự lược đồ 1.

4.2. Quá trình tạo khóa

Lược đồ sử dụng cấu trúc số nguyên tố $p = Nq^2 + 1$ với N là số tự nhiên chẵn, q là số nguyên tố lớn ($|q| \geq 160$ bít), và p là số nguyên tố lớn ($|p| \geq 1024$ bít). *(p,q)* là các tham số được công khai và lựa chọn sử dụng hàm một chiều SHA-1.

Bước 1: Người quản lý tạo ra một số nguyên tố lớn p, một ước số nguyên tố q theo cấu trúc $p = Nq^2 + 1$, như vậy ta có $q^2|(p-1)$.

Bước 2: Sinh nhóm khoá bí mật của người ký tương ứng là $x_1, x_2, \ldots, x_n$ với điều kiện $1 < x_i < q$, $i = 1, 2, \ldots, n$. Mỗi x_i được chọn ngẫu nhiên và chỉ được biết bởi người ký U_i.

Bước 3: Sinh nhóm khoá công khai $y_1, y_2, \ldots, y_n$ thoả mãn $y_i = x_i^q \bmod p$ được phân phối cho các thành viên U_i. Việc thêm hoặc loại bỏ một thành viên ký U_i cũng đòi hỏi việc thêm hoặc bỏ khoá công khai y_i tương ứng và nó được thực hiện bởi người quản lý.

4.3. Quá trình tạo chữ ký tập thể

Các yêu cầu tương tự lược đồ 1.

Bước 1: Mỗi người ký U_i chọn ngẫu nhiên số $0 < k_i < q$ và tính toán giá trị: $r_i = k_i^q \bmod p$. U_i thông báo r_i cho người quản lý. Người quản lý tính giá trị hàm băm H: $H = h(h(m_1) \| h(m_2) \| \ldots h(m_n))$, tính giá trị thống nhất chung cho phiên ký: $R = \prod_{i=1}^{n} r_i \bmod p$ và $E = h(H \| R)$. Giá trị E được thông báo cho các thành viên ký.

Bước 2: Người ký đầu tiên U_1 tính hàm băm $h(m_1)$ và sinh chữ ký số $s_1 = x_1^{h(m_1)E} k_1 \bmod q$ Sau đó U_1 gửi $(r_1, s_1, h(m_1))$ đến người ký thứ hai U_2 và quản lý.Tiếp theo mỗi người ký U_i với $i = 2, 3, \ldots, n$ lần lượt thực thực hiện bước sau.

Bước 3: Mỗi thành viên U_i kiểm tra xác thực tính đúng đắn của người ký trước bằng công thức:

$s_{i-1}{}^q = y_{i-1}{}^{h(m_{i-1})E} r_{i-1} \bmod p$. Nếu công thức này thoả mãn thì chứng tỏ thành viên ký thứ i - 1 tức là U_{i-1} là người ký trên các văn bản trước đó lần lượt $m_1 \ldots m_{i-1}$. U_i tính $s_i = x_i^{h(m_i)E} k_i \bmod q$. U_i gửi cho thành viên ký U_{i+1} và người quản lý các tham số: $(r_i, s_i, h(m_i))$. Riêng U_n gửi các tham số $(r_n, s_n, h(m_n))$ cho người quản lý.

Bước 4: Người quản lý xác thực chữ ký của U_n theo công thức: $s_n{}^q = y_n{}^{h(m_n)E} r_n \bmod q$. Sau đó người quản lý tính các giá trị: $S = \prod_{i=1}^{n} s_i \bmod q$. Cặp (E, S) là chữ ký số tập thể cho văn bản $M = m_1 \| m_2 \| \ldots \| m_n$ và công bố khóa công khai $Y = \prod_{i=1}^{n} y_i^{h(m_i)} \bmod p$

4.4. Xác thực chữ ký số tập thể

Việc xác thực chữ ký (E, S) cho tập văn bản $M = m_1 \| m_2 \| \ldots \| m_n$ với khóa công khai nhóm Y được thực hiện như sau:

Người xác thực tính $R' = S^q Y^{-E} \bmod p$ và $H = h(h(m_1) \| h(m_2) \| \ldots h(m_n))$. Kiểm tra nếu E=h(H||R'), nếu biểu thức thỏa mãn, thì chữ ký là hợp lệ. Nếu không, chữ ký không hợp lệ hoặc văn bản gốc đã bị thay đổi.

4.5. Xác thực bằng chứng

Tất cả các chữ ký cá nhân (r_i, s_i) có thể được sử dụng làm bằng chứng, cho biết thành viên U_i là người ký phần nội dung m_i, (r_i, s_i) theo biểu thức $s_i^q y_i^{h(m_i)E} = r_i \bmod p$ cùng với chữ ký hợp lệ (E,S) của bộ tài liệu. Nếu hai điều kiện được thỏa mãn, thành viên U_i được xác thực đã ký phần nội dung m_i vì công thức $s_i^q y_i^{h(m_i)E} = r_i \bmod p$ cho thấy mối quan hệ giữa toàn bộ tài liệu, phần nội dung m_i, và thành viên U_i.

4.6. Chứng minh tính đúng đắn của lược đồ đề xuất

Thật vậy, sử dụng biểu thức:

$R' = S^q Y^{-E} \bmod p$ ta có:

$$S'^q Y^{-E} = Y^{-E} \prod_{i=1}^{n} (x_i^{h(m_i)E k_i})^q =$$

$$Y^{-E} \prod_{i=1}^{n} y_i^{h(m_i)E} \prod_{i=1}^{n} k_i^q$$

$$= Y^{-E} Y^E \prod_{i=1}^{n} (k_i)^q = R \Rightarrow R' = R \Rightarrow E = h(Y \| R').$$

Như vậy, có thể khẳng định chữ ký số tập thể có phân biệt trách nhiệm ký tuần tự được xây dựng dựa trên bài toán khai căn được xây dựng như phần trên là đúng đắn và hợp lệ.

5. Phân tích các lược đồ đề xuất

Trong các lược đồ đã đề xuất của chúng tôi, vấn đề an toàn và bảo mật là chống lại những sự tấn công từ những người tham gia trong lược đồ quan trọng hơn những sự tấn công lược đồ từ bên ngoài.

5.1. Phân tích độ an toàn của các lược đồ đề xuất

A. Lược đồ 1

Dạng tấn công thứ nhất

Giả sử rằng $(n - 1)$ người ký cùng chia sẻ một chữ ký số tập thể (E, S) với người ký thứ n là kẻ tấn công đang cố gắng để tính khóa bí mật của người ký thứ n là x_n. Kẻ tấn công biết rằng các giá trị r_n và s_n được sinh ra bởi người ký thứ n. Những giá trị này thoả mãn công thức $\alpha^{S_n} y_n^{h(m_n)E} = r_n \bmod p$. Giá trị r_n được tạo ra bởi công thức $r_n = \alpha^{k_n} \bmod p$ với k_n là một số ngẫu nhiên, $k_n \in Z_q^*$. Việc tính khóa bí mật x_n đòi hỏi phải giải quyết bài toán logarit rời rạc, có nghĩa là phải giải quyết các vấn đề, cụ thể tính $k_n = \log_\alpha r_n$ và tính x_n theo s_n: $x_n = (k_n - s_n)(h(m_n)E)^{-1} \bmod p$ hoặc là tính x_n theo y_n:

$x_n = \log_\alpha y_n \bmod p$. Nếu những kẻ tấn công xác định giá trị k_n (hay x_n) đầu tiên, thì khi đó họ phải vượt qua bài toán logarit rời rạc và phán đoán đúng số ngẫu nhiên k_n. Ở đây, ta thấy tầm quan trọng của việc sử dụng bộ tạo ngẫu nhiên an toàn.

Dạng tấn công thứ hai

Giả sử *n* -1 người ký thử tạo ra chữ ký số của n người (*E*, *S*) với khoá chung là: $Y = Y' y_n^{h(m_n)} \bmod p$, với $Y' = \prod_{i=1}^{n-1} y_i^{h(m_i)} \bmod p$. Khi đó, *n*-1 người hợp sức cố gắng để tạo ra cặp (*E*, *S*) sao cho tính R'= $\alpha^S Y^E \bmod p$ và thỏa mãn biểu thức kiểm tra $E \equiv h(H \| R')$. Để làm được điều này, có thể chọn bất kỳ R, tính ra E theo $E = h(H \| R)$, và tìm S sao cho $\alpha^S = Y^{-E} R \bmod p$, điều này mâu thuẫn với giả thiết logarit rời rạc là bài toán khó. Hơn nữa $s_n = k_n - x_n h(m_n) E$, $r_i = \alpha^{k_i} \bmod p$, các giá trị này có liên quan thông qua E và giá trị ngẫu nhiên k_i. Vì vậy các cố gắng tấn công lược đồ đều quy về bài toán khó logarit rời rạc.

B. Lược đồ 2

Dạng tấn công thứ nhất

Giả sử rằng (*n* – 1) người ký cùng chia sẻ một chữ ký số tập thể (*E*, *S*) với người ký thứ *n* là những kẻ tấn công đang cố gắng để tính khóa bí mật của người ký thứ n là x_n. Kẻ tấn công biết rằng các giá trị r_n và s_n được sinh ra bởi người ký thứ *n*. Những giá trị này thoả mãn công thức: $s_n = x_n^{h(m_n)E} k_n \bmod q$. Giá trị r_n được tạo ra bởi công thức $r_n = {k_n}^q \bmod p$ với k_n số ngẫu nhiên, $k_n \in Z_q^*$. Do vậy việc tính khoá mật x_n thì phải giải quyết vấn đề khai căn modulo số nguyên tố *p*. Cụ thể là tính k_n như sau: $k_n = \sqrt[q]{r_n} \bmod p$. Sau đó tính $\chi_n = \sqrt[h(m_n)E]{s_n / k_n} \bmod p$. Hoặc là tính x_n theo công thức: $x_n = \sqrt[q]{y_n} \bmod p$. Để tính các giá trị trên kẻ tấn công đối diện vấn đề khó của bài toán khai căn và phán đoán số ngẫu nhiên lớn.

Dạng tấn công thứ hai

Giả sử *n* -1 người ký thử tạo ra chữ ký số của n người (*E*, *S*) với khoá chung là: $Y = Y' y_n^{h(m_n)} \bmod p$, với $Y' = \prod_{i=1}^{n-1} y_i^{h(m_i)} \bmod p$. Khi đó, *n*-1 người hợp sức cố gắng để tạo ra cặp (*E*, *S*) sao cho tính $R' = S^q Y^{-E} \bmod p$ và thỏa mãn biểu thức kiểm tra $E \equiv h(H \| R')$. Để làm được điều này, có thể chọn bất kỳ R, tính ra E theo $E = h(H \| R)$, và tìm S sao cho $S^q = Y^{-E} R \bmod p$, đây lại là bài toán khó khai căn modulo [11].

5.2. Đánh giá chất lượng của các lược đồ đề xuất

A. Chi phí tính toán

Để so sánh hiệu quả, chúng ta so sánh lược đồ đề xuất với lược đồ của Hwang. Để thuận tiện, chúng ta sử dụng các ký hiệu cho việc đánh giá hiệu năng: T_E là chi phí tính toán cho mô-đun có phép toán luỹ thừa mod *p*. T_M là chi phí tính toán cho mô-đun có phép toán nhân mod *p* (hoặc mod *q*). T_H là chi phí tính toán cho hàm băm H trên văn bản nào đó. Chú ý rằng một số khối tính toán với thời gian tính toán quá nhỏ so với T_E, T_M, T_H được bỏ qua. Chi phí tính toán cho lược đồ đề xuất là tổng chi phí tính toán cho nhóm sinh khóa công khai, sinh chữ ký số, xác thực chữ ký số (Chú ý: Những chi phí tính toán bởi *n* thành viên ký và người quản lý được xác định trước).

Chi phí tính toán lược đồ 1: nT_E ; $4nT_E$ + $6nT_M$ + $(n+1)T_H$; $(2+n)T_E$ + $(n+1)T_M$+nT_H.

Chi phí tính toán lược đồ 2: nT_E; $5nT_E$ + $(3n)T_M$ + $(n+1)T_H$; $(2+n)T_E$ + $(n+1)T_M$+nT_H.

Chi phí tính toán lược đồ của Hwang [18]: $2nT_E$ + nT_M; $(n+1)^2T_E$ + $4nT_E$ + $(n+1)^2T_M$ + $7nT_M$ + $(n^2 + 4n - 1)T_H$; $3T_E$ + T_M + T_H.

Bảng 1 chỉ ra sự so sánh chi phí tính toán giữa các lược đồ đề xuất và lược đồ của Hwang [14].

Bảng 1. *So sánh chi phí tính toán giữa các lược đồ chữ ký số tập thể*

Lược đồ	Tổng chi phí
Lược đồ 1	$(6n+3)T_E + (7n)T_M + (2n+1)T_H$
Lược đồ 2	$(7n + 2)T_E + (4n+1)T_M + (2n + 1)T_H$
Lược đồ Hwang [14]	$(6n + 3)T_E + (n + 1)^2T_E + (n + 1)^2T_M + (8n + 1)T_M + (n^2 + 4n)T_H$

Bảng 2. *So sánh kích thước chữ ký số*

Lược đồ	
Lược đồ 01	$\|E\| + \|S\|$
Lược đồ 02	$\|E\| + \|S\|$
Lược đồ của Hwang [14]	$\|R\| + \|S\|$

Bảng 3. *So sánh chi phí trao đổi dữ liệu giữa các lược đồ đề xuất và lược đồ của Hwang*

Lược đồ	Tổng
Lược đồ 01	6n
Lược đồ 02	6n
Lược đồ của Hwang [14]	$n^2 + n$

B. Kích thước chữ ký số của các lược đồ đề xuất

Cặp (*E*, *S*) là chữ ký số tập thể. Kích thước của lược đồ là $|E| + |S| \approx |q| + |q|$ giảm đáng kể so với Hwang [14] $|R| + |S| \approx |p| + |q|$. Nếu chọn q=160 bít, với hàm SHA-1 thì E kích thước 160 bít. Như vậy kích thước chữ ký xấp xỉ 320 bít tương đương kích thước chữ ký đơn cho dù số lượng người ký lớn hay nhỏ.

Bảng 2 chỉ ra sự so sánh kích thước chữ ký số giữa các lược đồ đề xuất và lược đồ của Hwang [14].

C. Chi phí trao đổi dữ liệu của các lược đồ đề xuất

Chi phí trao đổi dữ liệu của các lược đồ đề xuất được đo bằng tổng các trao đổi dữ liệu trong quá trình sinh chữ ký số tập thể (yêu cầu người quản lý và các thành viên ký

phải chấp hành trao đổi dữ liệu trong xử lý sinh chữ ký số tập thể). Bảng 3 chỉ ra rằng các lược đồ đề xuất giảm chi phí trao đổi dữ liệu so với lược đồ của Hwang [14].

6. Kết luận

Bài báo đã đề xuất hai lược đồ chữ ký số tập thể có phân biệt trách nhiệm với cấu trúc tuần tự dựa trên bài toán Logarit rời rạc và khai căn và có kích thước bằng chữ số đơn. Các lược đồ đề xuất đảm bảo tính an toàn thông qua độ khó giải của hai bài toán trên, và đã được chứng minh an toàn với một số các tấn công. Hơn nữa, các lược đồ đề xuất còn có hiệu quả về mặt tính toán và chi phí giao tiếp so với các nghiên cứu trước đó. Hai lược đồ đề xuất đảm bảo có thể được ứng dụng trong các mô hình thực tế.

TÀI LIỆU THAM KHẢO

[1] K.Itakura, K.Nakamura, "A public-key cryptosystem suitable for digital multisignatures", NEC Res. Dev, Vol.71, 1983, pp.1-8.

[2] L. Harn, "Digital multisignatures with distinguished signing authorities", Electr. Lett., 35(4), 1999, pp. 294-295.

[3] H. F. Huang, C. C. Chang, Multisignatures with distinguished signing authorities for sequential and broadcasting architectures, Computer Standard and Interfaces, 27(2), 2005, pp. 169-176.

[4] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of Two Multisignature Schemes with Distinguished Signing Authorities", International Conference on Hybrid Information Technology - Vol.2 (ICHIT'06), 2006, pp. 492-495.

[5] J. Zhang and V. Zou, "On the Security of Huang-Chang Multisignature Schemes", Int. *J. Network Security*, 5(1), 2007, pp. 62-65.

[6] W. Diffie, M. Hellman, New directions in cryptography, *IEEE transactions on Information Theory*, 22, 1976, pp. 644-654.

[7] N. FIPS, 186 digital signature standard, in, May, 1994.

[8] R. 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, 1994.

[9] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 10-18.

[10] C.-P. Schnorr, "Efficient signature generation by smart cards", *Journal of cryptology*, 4, 1991, pp. 161-174.

[11] N. A. Moldovyan, "Digital Signature Scheme Based on a New Hard Problem", *Computer Science Journal of Moldova*, vol. 16, No. 2, 2008, pp. 163-182.

[12] W. Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hall, 2005, pp. 592.

[13] N. H. Minh, N. A. Moldovyan, N. L. Minh, "New Multisignature Protocols Based on Randomized Signature Algorithms", IEEE, *International Conference on Research, Innovation and Vision for the Future in computing & Communication Technologies*, 2008, pp. 124-127.

[14] S.-J. Hwang, M.-S. Hwang, S.-F. Tzeng, "A new digital multisignature scheme with distinguished signing authorities", *Journal of Information Science and Engineering*, 19, 2003, pp. 881-887.

(BBT nhận bài: 22/12/2016, hoàn tất thủ tục phản biện: 02/02/2017)