DOI: 10.15625/vap.2020.00148

CHỮ KÝ SỐ TẬP THỂ CHO CÁC NHÓM KÝ

Nguyễn Kim Tuấn[1], Hồ Ngọc Duy[2], Hồ Lê Viết Nin[1]

[1]Khoa Công nghệ Thông tin, Trường Đại học Duy Tân, Việt Nam
[2]Phòng Công nghệ Thông tin, Bộ Quốc phòng, Việt Nam

nkimtuan@duytan.edu.vn, duyho@gmail.com, holevietnin@duytan.edu.vn

TÓM TẮT: *Trong bài báo này, chúng tôi đề xuất hai dạng mới của lược đồ chữ ký số tập thể. Đó là: 1) Chữ ký số tập thể được chia sẻ bởi một tập các nhóm ký và 2) Chữ ký số tập thể được chia sẻ bởi nhiều nhóm ký và nhiều cá nhân ký. Lược đồ thứ 2 thực chất là sự mở rộng của lược đồ thứ 1. Cả hai lược đồ này đều được xây dựng dựa trên độ khó của bài toán logarit rời rạc. Một trong những ưu điểm của các lược đồ được đề xuất là có thể triển khai trên nền các Hạ tầng khóa công khai (Public key Infrastructure) đang tồn tại.*

Từ khóa: *Chữ ký số nhóm, Chữ ký số tập thể, Nhóm ký, Hạ tầng khóa công khai.*

I. GIỚI THIỆU

Chữ ký số (Digital signature - DS) hiện đang được sử dụng khá phổ biến trong lĩnh vực công nghệ thông tin, đặc biệt là trong các ứng dụng hoạt động trên không gian mạng, mà ở đó có yêu cầu cao về tính xác thực, tính toàn vẹn và tính chống chối bỏ trách nhiệm. Về nguyên lý, các giao thức chữ ký số (Digital Signature Protocol - DSP) được xây dựng dựa trên hoạt động của hệ mật mã khóa công khai (Public key cryptography). Theo đó, người ký, là người sở hữu cặp khóa, sử dụng khóa bí mật (private key) để tạo ra chữ ký trên tài liệu số của họ. Và người kiểm tra, là người nhận chữ ký này, sẽ sử dụng khóa công khai (public key) của người ký để kiểm tra tính hợp lệ của chữ ký mà họ nhận được. Tuy nhiên, để đáp ứng yêu cầu xác thực của các ứng dụng thực tế khác nhau người ta đã đề xuất nhiều loại giao thức DS: Giao thức chữ ký số đơn/cá nhân (Individual digital signature protocol) [1]; Giao thức chữ ký số mù (Blind digital signature protocol) [2, 3, 4, 5]; Giao thức chữ ký số tập thể (Collective digital signature protocol) [8]; Giao thức chữ ký số nhóm (Group digital signature protocol) [9],… Các giao thức chữ ký số nhóm thường được sử dụng trong các ứng dụng mà ở đó người nhận chỉ cần biết rằng chữ ký là đến từ một nhóm ký.

Chữ ký số tập thể là loại chữ ký được hình thành với sự tham gia của tất cả thành viên trong một tập người ký đã được khai báo (tập thể ký). Điều này có nghĩa, chữ ký số tập thể trên một tài liệu số M được công nhận là hợp lệ khi M được ký bởi mỗi người ký trong tập thể ký đó. Private key của mỗi người trong tập thể ký được sử dụng để tạo ra chữ ký số của tập thể ký này. Trong khi đó, public key của họ được sử dụng bởi thủ tục kiểm tra chữ ký để xác minh sự hợp lệ của chữ ký mà tập thể ký này tạo ra. Ưu điểm của loại chữ ký này là: Có thể cài đặt nó dựa vào các giao thức chữ ký số cá nhân đang được triển khai trên các hạ tầng khóa công khai sẵn có. Và dễ dàng triển khai theo các chuẩn chữ ký số đã được công bố như: Chuẩn DSS của Mỹ [12], chuẩn GOST R 34.10-2012 của Nga [13].

Chữ ký số nhóm là loại chữ ký được hình thành trên danh nghĩa của một nhóm những người ký, gọi tắt là nhóm ký (signing group), nhưng thực tế thì nó được sinh ra chỉ bởi một thành viên ẩn danh của nhóm ký này. Điều này cũng có nghĩa, mặc dầu chữ ký số nhóm trên một tài liệu số M là chỉ do một thành viên trong nhóm tạo ra nhưng việc xác minh tính hợp lệ của chữ ký sau này phải dựa vào các tham số công khai của nhóm ký, cụ thể ở đây là public key của nhóm ký. Mỗi nhóm ký được điều hành bởi một người đứng đầu, gọi là người quản lý nhóm (group manager). Người này phải là một thành viên hoặc một đối tác tin cậy của nhóm ký. Nhiệm vụ chính của họ là tạo ra các tham số bí mật, mà các thành viên nhóm sử dụng để tạo ra chữ ký nhóm của mỗi nhóm. Và chỉ có người này mới có thể tiết lộ được danh tính của thành viên đã sinh ra chữ ký nhóm lên tài liệu số M.

Trong thực tế có những tài liệu số cần được xử lý và cần được ký bởi nhiều nhóm ký khác nhau. Trong trường hợp này, chữ ký cuối cùng có thể là sự "kết nối" của các chữ ký nhóm của mỗi nhóm ký. Như vậy, độ dài chữ ký và việc xác minh chữ ký sau này phụ thuộc rất lớn vào số lượng nhóm ký tham gia vào quá trình tạo ra chữ ký này. Đây là điều mà các lược đồ xác thực dựa trên chữ ký số không mong muốn. Chúng tôi nghĩ, nếu kết hợp được những ưu điểm của chữ ký số nhóm và chữ ký số tập thể thì ta có tạo ra một dạng chữ ký số đơn nhưng đáp ứng được cho bài toán thực tế này: Mặc dầu chữ ký cuối cùng là một chữ ký số đơn, nhưng nó đại diện cho các nhóm ký và có cơ sở để bên kiểm tra chữ ký tin rằng chữ ký đã được ký bởi mỗi nhóm ký đã tham gia vào quá trình xử lý tài liệu ban đầu.

Trong bài báo, chúng tôi đề xuất một *"Lược đồ chữ ký tập thể được chia sẻ bởi các nhóm ký"* để cung cấp khả năng xác thực cho bài toán này. Thực tế cũng có những tài liệu số cần được xử lý và cần được ký bởi nhiều nhóm ký và nhiều cá nhân ký khác nhau, vì vậy chúng tôi đề xuất một dạng lược đồ chữ ký tập thể kết hợp để đáp ứng bài toán vừa nêu: *"Lược đồ chữ ký tập thể được chia sẻ bởi nhiều nhóm ký và nhiều cá nhân ký"*. Dạng lược đồ này cũng cung cấp khả năng sinh ra một chữ ký số đơn trên tài liệu số M nhưng bên kiểm tra có cơ sở tin rằng là nó đã được ký bởi nhiều nhóm ký và nhiều cá nhân ký khác nhau.

Các lược đồ mà chúng tôi đề xuất ở đây được phát triển trên cơ sở của lược đồ chữ ký số nhóm, nó vẫn đảm bảo khả năng cho phép nhóm ký sinh ra một chữ ký đơn trên tài liệu số nào đó, nhưng kích thước của chữ ký không phụ thuộc vào số lượng người ký, số lượng nhóm ký và số lượng người ký cá nhân.

II. CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ ĐỀ XUẤT

A. Giao thức chữ ký số nhóm

Đầu tiên, chúng tôi dựa vào giao thức chữ ký số nhóm được mô tả trong [9] để đề xuất một giao thức chữ ký số nhóm được xây dựng dựa trên độ khó tính toán của bài toán logarit rời rạc theo modulo số nguyên tố. Đây là loại chữ ký nhóm gồm 3 thành phần (U, E, S) và việc hình thành chữ ký được điều hành bởi người quản lý nhóm. Cụ thể như sau:

Các tham số được sử dụng trong giao thức bao gồm: 1) Một số nguyên tố đủ lớn *p* (độ dài của p > 2464 bít), sao cho *q*|*p - 1* (độ dài của q ≥ 256 bít) và 2) Một số α có bậc bằng *q modulo p*. Mỗi người ký thứ i của nhóm ký sinh ra khóa riêng (private key) x_i (|x| ≥ 256 bit) và khóa công khai (public key) yi được tính theo công thức $y_i = \alpha^{x_i} \bmod p$.

Public key Y của người quản lý nhóm, được tính theo công thức: $Y = \alpha^X \bmod p$, trong đó X là private key của người quản lý nhóm. Y cũng chính là public key của nhóm nên nó sẽ được sử dụng để kiểm tra tính xác thực của chữ ký nhóm.

Giả sử có một nhóm gồm *m* thành viên, muốn ký lên tài liệu M. Mỗi thành viên thứ i trong nhóm có *public key* là $y_i = \alpha^{x_i} \bmod p$ và *private key* tương ứng là x_i, với i = 1, 2,…, m. Giao thức chữ ký nhóm được mô tả như sau:

- ***Thủ tục sinh chữ ký nhóm:***

Bước 1: Người quản lý nhóm thực hiện các công việc sau:

- Sử dụng một hàm băm F_H nào đó (có thể là MD5, SHA) để tính giá trị băm của tài liệu M:

$$H = F_H(M) \tag{1}$$

- Tính các hệ số mặt nạ λ_i, và rồi gửi λ_i đến mỗi thành viên tương ứng ("||" là toán tử nối xâu):

$$\lambda_i = F_H\left(H \,\|\, y_i \,\|\, F_H\left(H \,\|\, y_i \,\|\, X\right)\right) \tag{2}$$

- Tính thành phần đầu tiên của chữ ký, thành phần U:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p \tag{3}$$

Bước 2: Mỗi thành viên thứ i (i = 1, 2,…, m) của nhóm ký thực hiện các công việc sau:

- Sinh số ngẫu nhiên k_i < q và rồi tính R_i theo công thức:

$$R_i = \alpha^{k_i} \bmod p \tag{4}$$

- Gửi R_i đến người quản lý nhóm.

Bước 3: Người quản lý nhóm thực hiện các công việc sau:

- Sinh số ngẫu nhiên K < q và rồi tính giá trị R như sau:

$$R' = \alpha^K \bmod p \tag{5}$$

$$R = R' \prod_{i=1}^{m} R_i \bmod p = \alpha^{K+\sum_{i=1}^{m} k_i} \bmod p \tag{6}$$

- Tính thành phần thứ hai của chữ ký, thành phần E:

$$E = F_H\left(M \,\|\, R \,\|\, U\right) \tag{7}$$

- Gửi E đến tất cả các thành viên của nhóm ký (tham gia quá trình hình thành chữ ký ngay từ ban đầu)

Bước 4: Mỗi thành viên thứ i (i = 1, 2,…, m) của nhóm ký thực hiện các công việc sau:

- Sinh số ngẫu nhiên k_i < q và rồi tính S_i theo công thức:

$$S_i = k_i - x_i \lambda_i E \bmod q \tag{8}$$

- Gửi S_i đến người quản lý nhóm (cặp giá trị (R_i, S_i) được xem là chữ ký của thành viên i của nhóm ký).

Bước 5: Người quản lý nhóm thực hiện các công việc sau:

- Kiểm tra tính đúng của mỗi S_i theo biểu thức:

$$R_i = y_i^{\lambda_i E} \alpha^{S_i} \bmod p \quad (9)$$

- Nếu tất cả S_i đều thỏa biểu thức trên thì tiếp tục tính giá trị chia sẻ của nhóm ký:

$$S' = K - XE \bmod q \quad (10)$$

- Tính thành phần thứ ba (cuối cùng) của chữ ký nhóm, thành phần S:

$$S = S' + \sum_{i=1}^{m} S_i \bmod q \quad (11)$$

Như vậy một chữ ký nhóm gồm 3 thành phần (U, R, S) đã được hình thành trên tài liệu M, nó đại diện cho nhóm ký. Bên nhận sẽ sử dụng public key Y của nhóm ký này để kiểm tra tính hợp lệ của chữ ký trên M.

Có thể thấy, thành phần D trong công thức (11), $D = \sum_{i=1}^{m} S_i \bmod q$, đóng vai trò như "tiền chữ ký nhóm" của nhóm ký. Chỉ khi nào tính hợp lệ của nó được xác nhận bởi người quản lý nhóm thì nó mới có thể đóng góp vào việc tạo ra thành phần đầu tiên (S) của chữ ký nhóm của nhóm ký.

Tham số ngẫu nhiên R trong công thức (6) được xem như chữ ký tập thể sử dụng một lần (the single-use collective signature), nó được hình thành từ các R_i (single-use public key của mỗi người ký cá nhân) và R' (single-use public key của người quản lý nhóm). Tính "sử dụng một lần" ở đây giúp nhóm ký có thể tạo ra các chữ ký khác nhau trên các tài liệu khác nhau, dù họ vẫn sử dụng cùng một cặp khóa public key và private key ban đầu.

- ***Thủ tục kiểm tra chữ ký nhóm:***

Người kiểm tra chữ ký thực hiện các công việc sau:

- Sử dụng hàn băm F_H để tính giá trị băm của tài liệu M:

$$H = F_H(M) \quad (12)$$

- Sử dụng public key Y của nhóm ký và chữ ký nhận được (U, R, S) để tính giá trị R*:

$$R^* = (UY)^E \alpha^S \bmod p \quad (13)$$

- Và rồi tính giá trị E* theo công thức:

$$E^* = F_H(M \,||\, R^* \,||\, U) \quad (14)$$

- So sánh E* và E. Nếu E* = E: Kết luận, chữ ký nhận được là hợp lệ và tài liệu số M nhận được là đảm bảo tính toàn vẹn. Ngược lại: Kết luận, chữ ký nhận được là không hợp lệ (bị giả mạo) hoặc tài liệu không đảm bảo tính toàn vẹn.

- ***Chứng minh tính đúng của giao thức chữ ký:***

Tính đúng của một giao thức chữ ký là sự phù hợp giữa phương pháp hình thành chữ ký với phương pháp kiểm tra tính hợp lệ của chữ ký và tính toàn vẹn của văn bản được ký. Tính đúng đắn của giao thức chữ ký nhóm được đề xuất này thể hiện qua việc kiểm tra tính đúng đắn của thủ tục kiểm tra chữ ký của mỗi thành viên tham gia vào chữ ký nhóm (S_i) và tính đúng đắn của thủ tục kiểm tra chữ ký nhóm.

a) Tính đúng đắn của thủ tục kiểm tra chữ ký thành viên: Ở đây ta chỉ cần chứng mình sự tồn tại của biểu thức (9).

Ta thấy:

$$= (\alpha^{x_i})^{\lambda_i E} . \alpha^{k_i - x_i \lambda_i E} \ mod\ p$$

$$= \alpha^{x_i \lambda_i E} . \alpha^{k_i} . \alpha^{-x_i \lambda_i E} \ mod\ p$$

$$= \alpha^{k_i} \ mod\ p$$

$$= R_i$$

Đây là điều cần chứng minh.

b) Tính đúng đắn của thủ tục kiểm tra chữ ký nhóm: Ở đây ta cần chứng mình R* theo công thức (13) = R theo công thức (6), vì khi đó tất nhiên E* theo công thức (4) = E theo công thức (7).

Ta thấy: $R^* = (UY)^E \ \alpha^S \ mod\ p$

$$= \left(\prod_{i=1}^{m} y_i{}^{\lambda_i} \alpha^X\right)^E . \alpha^{K - XE + \sum_{i=1}^{m} S_i}$$

$$= \alpha^{(\sum_{i=1}^{m} x_i \lambda_i + X)E} . \alpha^{K - XE + \sum_{i=1}^{m} (k_i - x_i \lambda_i E)}$$

$$= \alpha^{(\sum_{i=1}^{m} x_i \lambda_i E)} . \alpha^{XE}\ \alpha^K . \alpha^{-XE} . \alpha^{\sum_{i=1}^{m} k_i} . \alpha^{-(\sum_{i=1}^{m} x_i \lambda_i E)}$$

$$= \alpha^K . \alpha^{\sum_{i=1}^{m} k_i}$$

$$= \alpha^{K + \sum_{i=1}^{m} k_i}$$

$$= R$$

Đây là điều cần chứng minh.

Giao thức chữ ký nhóm được đề xuất ở trên được sử dụng làm giao thức cơ sở để chúng tôi phát triển hai lược đồ chữ ký số tập thể mới đề xuất. Các lược đồ này cũng được phát triển dựa trên chiến lược 2 bước: Đầu tiên là hình thành "tiền chữ ký tập thể" giữa các nhóm ký. Sau đó là hình thành chữ ký tập thể chung cho các nhóm ký hoặc chung cho các nhóm ký và các cá nhân ký.

B. Lược đồ chữ ký số tập thể được chia sẻ bởi các nhóm ký:

Giả sử có *g* nhóm ký, muốn ký lên tài liệu M. Public key của mỗi nhóm ký thứ j (với j = 1, 2,…, g) được tính theo công thức (15), trong đó X_j là khóa bí mật (private key) của người quản lý nhóm của nhóm thứ j:

$$Y_j = \alpha^{X_j} \bmod p \tag{15}$$

Cũng giả sử nhóm ký thứ j bao gồm m_j người ký cá nhân, được chỉ định, đóng vai trò đại diện trong việc hình thành chữ ký của nhóm ký này. 6

Lược đồ chữ ký tập thể được chia sẻ bởi các nhóm ký được mô tả như sau:

- ***Thủ tục sinh chữ ký tập thể:***

Bước 1: Người quản lý nhóm của mỗi nhóm ký thứ j (j = 1, 2,…, g) thực hiện các công việc sau:

- Tạo ra các tham số mặc nạ cho λ_{ji} cho những người ký của nhóm j (theo công thức (2)).
- Tính U_j và R_j (i = 1, 2,…, m_j) của nhóm ký thứ j theo công thức (16) và (17):

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \bmod p \tag{16}$$

và

$$R_j = R_j' \prod_{i=1}^{m_j} R_{ji} \bmod p \tag{17}$$

Đây là hai giá trị (chữ ký nhóm tập thể và tham số ngẫu nhiên) mà nhóm ký thứ j chia sẻ với các nhóm ký khác để tạo chữ ký tập thể được chia sẻ bởi các nhóm ký.

- Gửi U_j và R_j đến tất cả người quản lý nhóm của các nhóm khác.

Bước 2: Mỗi người quản lý nhóm đều phải tiến hành tính U, R và rồi tính E:

$$U = \prod_{j=1}^{g} U_j \bmod p \tag{18}$$

$$R = \prod_{j=1}^{g} R_j \bmod p = \alpha^{\sum_{j=1}^{g} K_j} \bmod p \tag{19}$$

$$E = F_H\left(M \,||\, R \,||\, U\right) \tag{20}$$

Như vậy thành phần thứ nhất (U) và thành phần thứ hai (E) của chữ ký tập thể cho g nhóm ký đã được hình thành.

Bước 3: Mỗi người quản lý nhóm, của nhóm thứ j, thực hiện các công việc sau:

- Tính thành phần chữ ký chia sẻ của nhóm j:

$$S_j = S'_j + \sum_{i=1}^{m_j} S_{ji} \bmod q \tag{21}$$

Ở đây, S_{ji} là chữ ký chia sẻ của người ký cá nhân thứ i trong nhóm thứ j.

- Gửi S_j cho những người quản lý nhóm khác

Bước 4: Mỗi người quản lý nhóm có thể kiểm tra tính đúng của mỗi chữ ký chia sẻ S_j bằng cách kiểm tra biểu thức:

$$R_j = \left(U_j Y_j\right)^E \alpha^{S_j} \bmod p \tag{22}$$

Nếu tất cả S_j đều thỏa mãn biểu thức này thì thành phần thứ ba của chữ ký tập thể sẽ được tính theo công thức:

$$S = \sum_{j=1}^{g} S_j \bmod q \tag{23}$$

Vậy chữ ký tập thể gồm 3 thành phần (U, E, S) được sinh ra ở trên đại diện cho chữ ký tập thể trên tài liệu M mà nó được chia sẻ bởi g nhóm ký khác nhau.

- ***Thủ tục kiểm tra chữ ký tập thể:***

Từ chữ ký nhận được, thủ tục kiểm tra chữ ký thực hiện các bước sau:

Bước 1: Tính public key tập thể được chia sẻ bởi tất cả các nhóm ký:

$$Y_{\text{col}} = \prod_{j=1}^{g} Y_j \bmod p = \alpha^{\sum_{j=1}^{g} X_j} \bmod p \tag{24}$$

Bước 2: Tính giá trị R*:

$$R^* = \left(UY_{\text{col}}\right)^E \alpha^S \bmod p \tag{25}$$

Bước 3: Tính giá trị E*:

$$E^* = F_H\left(M \parallel R^* \parallel U\right) \tag{26}$$

Bước 4: So sánh E* với E. Nếu E* = E: Kết luận, chữ ký nhận được là hợp lệ và tài liệu M nhận được là đảm bảo tính toàn vẹn. Ngược lại: Kết luận, chữ ký nhận được là không hợp lệ (có thể bị giả mạo) hoặc tài liệu không đảm bảo tính toàn vẹn.

C. Lược đồ chữ ký số tập thể chia sẻ cho nhiều nhóm ký và nhiều người ký cá nhân

Lược đồ chữ ký tập thể được chúng tôi đề xuất sau đây cho phép nhiều nhóm ký và nhiều người ký cá nhân cùng ký lên một tài liệu M. Lược đồ này được xây dựng hoàn toàn tương tự lược đồ chữ ký tập thể được chia sẻ bởi các nhóm ký vừa được mô tả ở trên. Nhưng ở đây, chúng tôi xem mỗi người ký cá nhân như là một nhóm ký mà ở đó chỉ có một người ký (người ký cá nhân), tức là với mỗi cá nhân ký thứ j thì giá trị U_j của họ được cho = 1.

Thủ tục sinh chữ ký cũng sẽ thực hiện tương tự như trên, nhưng:

- Với các nhóm ký thì các giá trị U_j, R_j, S_j sẽ được tính theo công thức (16), (17), (21).
- Với những người ký cá nhân thì:

  Giá trị U_j được cho bằng 1: $U_j = 1$

  Giá trị R_j được tính theo công thức sau:

$$R_j = \alpha^{k_j} \bmod p \text{ ; (thay vì sử dụng công thức (17))}$$

  Giá trị S_j được tính theo công thức sau (x_j là private key của người ký cá nhân thứ j):

$$S_j = k_j - x_j E \bmod q \text{ ; (thay vì sử dụng công thức (21))}$$

Thủ tục kiểm tra chữ ký cũng thực hiện tương tự như trên. y_j ($y_j = \alpha^{x_j} \bmod p$) của mỗi người ký cá nhân sẽ cũng được sử dụng để tính public key của chữ ký tập thể , Y_{col} (theo công thức (24)), như Y_j của các nhóm ký khác.

Lược đồ chữ ký này đảm bảo rằng, chỉ khi nào có tất cả những người quản lý nhóm tham gia thì thủ tục tiết lộ chữ ký tập thể mới được thực hiện (việc xác định cá nhân ký trong mỗi nhóm ký được thực hiện trong phạm vi nhóm ký đó).

III. THẢO LUẬN

Công thức (2) và (3) cho thấy: Thành phần đầu tiên của chữ ký nhóm (U) chứa thông tin về tất cả những người ký nhóm đã ký tham gia vào việc hình thành chữ ký nhóm trên trên tài liệu M; Chỉ người quản lý nhóm mới có thể "mở" (open) chữ ký nhóm, sử dụng giá trị U, vì chỉ có người này mới có khóa bí mật X để có thể tính được giá trị λ_i. Đây được xem là ưu điểm của giao thức chữ ký nhóm này.

Việc sử dụng các tham số ngẫu nhiên k_i và K để tạo ra các sing-use public key của mỗi thành viên nhóm (tính R_i theo công thức (4)) và của người quản lý nhóm (tính R' theo công thức (5)) giúp hạn chế các cuộc tấn công theo cách đoán khóa bí mật hoặc giả mạo chữ ký. Trong trường hợp này, nếu kẻ tấn công muốn giả mạo, muốn tính được R, rồi tới E, thì nó phải hoặc đoán được k_i và K, trong khi được chon ngẫu nhiên. Hoặc tính được k_i và K, thì phải giải được bài toán logarit rời rạc. Rõ ràng mức độ thành công là rất thấp.

Thủ tục sinh chữ ký nhóm cho thấy, chỉ khi nào chữ ký cá nhân (S_i) của tất cả thành viên trong nhóm ký được kiểm tra và được công nhận bởi người quản lý nhóm thì "tiền chữ ký nhóm" mới được tính ($D = \sum_{i=1}^{m} S_i \bmod q$). Sau đó người quản lý nhóm mới xây dựng thành phần thứ ba (S) của chữ ký nhóm cho nhóm ký (công thức (11)). Điều này cho thấy, mức độ an toàn của chữ ký nhóm được đảm bảo, vì chỉ có thành viên của nhóm ký mới có S_i hợp lệ và vì một thành viên trong nhóm ký cũng không thể giả mạo chữ ký của thành viên khác trong cùng nhóm (xem công thức (8) và (9)).

Công thức (11) và (18) cho thấy, thành phần U của chữ ký tập thể chứa thông tin về tất cả thành viên nhóm, của mỗi nhóm ký đã tham gia vào việc hình thành chữ ký trên tài liệu M. Thủ tục định danh (tiết lộ chữ ký nhóm do ai ký) trong trường hợp này được thực hiện tương tự như định danh chữ ký nhóm mô tả trong [9]. Cũng cần chú ý rằng, để tiết lộ được cá nhân ký thì phải có sự tham gia của người quản lý nhóm của nhóm mà cá nhân đó là thành viên. Điều này cũng cho thấy độ phức tạp tính toán của thủ tục sẽ tăng cao khi mà số lượng nhóm ký tham gia hình thành chữ ký tăng lên. Đây là điều chúng tôi tiếp tục nghiên cứu.

Lược đồ chữ ký tập thể được đề xuất vẫn đảm bảo hai bước trong việc xác mình chữ ký: Ban đầu là xác minh chữ ký chia sẻ S_j của mỗi nhóm ký, trong thủ tục hình thành chữ ký. Sau đó là kiểm tra chữ ký được hình thành bởi các nhóm ký, trong thủ tục kiểm tra chữ ký. Điều đáng lưu ý ở thủ tục cuối này là sử dụng public key tập thể Y_{col} được tính theo công thức (24) chứ không phải public key của các nhóm ký.

IV. KẾT LUẬN

Trong bài báo này, chúng tôi đề xuất hai dạng mở rộng của chữ ký số tập thể, cả hai vẫn là một chữ ký số đơn nhưng: i) Được chia sẻ bởi nhiều nhóm ký khác nhau. Loại chữ ký này có kích thước cố định, hoàn toàn độc lập với số lượng nhóm ký tham gia vào việc tạo ra chữ ký và chứa đầy đủ thông tin về những gì liên quan đến việc hình thành chữ ký. ii) Được chia sẻ bởi nhiều nhóm ký và nhiều cá nhân ký khác nhau. Chúng tôi đã mô tả chi tiết về việc xây dựng lược đồ chữ ký của dạng thứ nhất (i). Lược đồ chữ ký của dạng thứ hai (ii) chỉ là sự thay đổi lược đồ thứ nhất, bằng cách, xem mỗi người ký cá nhân là một nhóm ký mà ở đó chỉ có 1 thành viên, giá trị U được gán bằng 1.

Cũng như các giao thức chữ ký số tập thể và chữ ký số nhóm được mô tả ở [5, 6] và [9, 15], các giao thức của chúng tôi cũng có thể được triển khai vào thực tế dựa trên các hệ thống PKI đang sẵn có. Chữ ký chúng tôi đề xuất được xây dựng một cách độc lập với các chuẩn chữ ký số đang có.

Các lược đồ chữ ký được đề xuất ở đây đều được xây dựng dựa trên độ khó tính toán của bài toán logarit rời rạc trên trường hữu hạn GF(p) nên về nguyên tắc nó vẫn đảm bảo mức độ an toàn cần thiết như các lược đồ chữ ký số Elgamal, DSS, GOST R34.10-94… Tuy nhiên, chúng tôi đang cố gắng rút ngắn chữ số xuống còn 2 thành phần E và S như trong các chuẩn chữ ký số [1, 12, 13]. Hy vọng rằng, các lược đồ chữ ký của chúng tôi nếu được xây dựng dựa trên bài toán đường cong Elliptic thì độ dài của chữ ký có thể giảm xuống, nhưng độ an toàn và hiệu năng của lược đồ có thể tăng lên. Đây là hướng nghiên cứu trong tương lai của chúng tôi.

V. TÀI LIỆU THAM KHẢO

[1] National Institute of Standards and Technology, "Digital Signature Standard", FIPS Publication 186-3, 2009.

[2] Chaum D., "Blind Signatures for Untraceable Payments", Advances in Cryptology: Proc. of CRYPTO'82, Plenum Press, pp. 199-203, 1983.

[3] Camenisch J. L., Piveteau J.-M., Stadler M. A., "Blind Signatures Based on the Discrete Logarithm Problem", In: Advances in Crypology - EUROCRYPT'94 Proc, Lecture Notes in Computer Science, Vol. 950. Springer-Verlag, Berlin Heidelberg New York, pp. 428-432, 1995.

[4] Minh N. H., Binh D. V., Giang N. T., Moldovyan N. A., "Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems", Applied Mathematical Sciences.,6, pp. 6903-6910, 2012.

[5] Moldovyan N. A., "Blind Signature Protocols from Digital Signature Standards", Int. Journal of Network Security, 13, pp. 22-30, 2011.

[6] Moldovyan N. A., "Blind Collective Signature Protocol", Computer Science Journal of Moldova,19, pp. 80-91, 2011.

[7] Moldovyan N. A., Moldovyan A. A., "Blind Collective Signature Protocol Based on Discrete Logarithm Problem", Int. Journal of Network Security, 11, pp. 106-113, 2010.

[8] Pieprzyk J., HardjonoTh., Seberry J., "Fundamentals of Computer Security", Springer-Verlag. Berlin (2003).

[9] Moldovyan A. A., Moldovyan N.A., "Group signature protocol based on masking public keys", Quasigroups and related systems, 22, pp. 133-140, 2014.

[10] Seetha R., Saravanan R., **"**Digital Signature Schemes for group communication: A Survey", International Journal of Applied Engineering Research, 11, pp. 4416-4422, 2016.

[11] Enache A.-C., "About Group Digital Signatures", Journal of Mobile, Embedded and Distributed Systems, IV, pp. 193-202, 2012.

[12] International Standard ISO/IEC 14888-3:2006(E), "Information technology - Security techniques - Digital Signatures with appendix - Part 3: Discrete logarithm based mechanisms".

[13] GOST R 34.10-2001. Russian Federation Standard. Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature. Government Committee of the Russia for Standards, (in Russian), 2012.

[14] Rajasree R. S., "Generation of Dynamic Group Digital Signature", International Journal of Computer Applications, 98, pp. 1-5, 2014.

[15] Moldovyan N. A., Nguyen Hieu Minh, Dao Tuan Hung, Tran Xuan Kien, "Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism", International Journal of Emerging Technology and Advanced Engineering, 6, pp. 1-5, 2016.

[16] Moldovyan N. A., "Digital Signature Scheme Based on a New Hard Problem", Computer Science Journal of Moldova. 16, pp. 163-182, 2008.

COLLECTIVE DIGITAL SIGNATURE FOR SIGNING GROUPS

Tuan Nguyen Kim, Duy Ho Ngoc, Nin Ho Le Viet, Long Nguyen Van

ABSTRACT: *In this paper, we propose two new types of collective digital signature scheme. They are: 1) The collective digital signature is shared by a set of signing groups and 2) The collective digital signature is shared by many signing groups and many individual signers. The second scheme is actually an extension of the first one. Both schemes are built on the difficulty of the discrete logarithm problem. The main advantage of the schemes we propose is that they can be implemented on existing public key infrastructures (PKI).*

Keywords: *Group Digital Signature, Collective Digital Signature, Signing Group, Public key Infrastructure (PKI).*