MỘT THUẬT TOÁN CHỮ KÝ XÂY DỰNG DỰA TRÊN TÍNH KHÓ CỦA VIỆC GIẢI ĐỒNG THỜI HAI BÀI TOÁN PHÂN TÍCH SỐ VÀ LOGARIT RỜI RẠC

A SIGNATURE ALGORITHM BASED ON DIFFICULTY OF SIMULTANEOUS SOLVING INTEGER FACTORIZATION AND DISCRETE LOGARITHM PROBLEM

Phạm Văn Hiệp[1], Nguyễn Hữu Mộng[2], Lưu Hồng Dũng[2]

[1]Trường Đại học Công nghiệp Hà Nội; hieppv@haui.edu.vn

[2]Học viện Kỹ thuật Quân sự; nghm06@yahoo.com, luuhongdung@gmail.com

Tóm tắt - Bài báo đề xuất xây dựng lược đồ chữ ký số mới dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên vành Zn. Lược đồ mới được xây dựng với mục đích nhằm nâng cao độ an toàn của thuật toán chữ ký số, đồng thời có thể rút gọn kích thước của chữ ký số. Lược đồ mới đề xuất chỉ bị phá vỡ khi đồng thời giải được các bài toán trên. Ngoài ra, bài báo cũng đã giải quyết tồn tại của một số lược đồ hiện nay, đó là kích thước chữ ký do chúng sinh ra khá lớn nên tốc độ xử lý chậm và làm giảm hiệu quả thực hiện của các lược đồ. Với lược đồ mới được đề xuất thì việc rút gọn kích thước của chữ ký sẽ nâng cao hiệu quả thực hiện của lược đồ trong các ứng dụng thực tế.

Từ khóa - lược đồ; chữ ký số; thuật toán chữ ký số; bài toán logarit rời rạc; số nguyên.

Abstract - The article proposes new digital signature schemes based on difficulty of simultaneous solving integer factorization and discrete logarithm problem. The new schema is designed to improve the security of digital signature algorithms and reduce the size of digital signatures. Schema security is only broken when concurrently solving these problems. In addition, the article has solved the problem of the existence of some current schemas. That is the size of the signatures due to their large size, resulting in slower processing times and reduced efficiency of the schemas. With the proposed new scheme, the shortened size of signatures will enhance effective implementation of the scheme in actual application.

Key words - schema; digital signature; digital signature algorithm; discrete logarithm problem; integer factoring problem.

1. Đặt vấn đề

Phát triển các lược đồ chữ ký số với mục đích nâng cao độ an toàn cho thuật toán là một hướng nghiên cứu được nhiều người quan tâm. Trong [1 - 9] các tác giả đã đề xuất một số lược đồ chữ ký xây dựng trên đồng thời hai bài toán khó. Đáng chú ý nhất trong đó là 2 lược đồ đề xuất bởi [8] và [9]. Trong [8] và một số kết quả trước đó, các lược đồ chữ ký đề xuất ở đây được xây dựng dựa trên tính khó của việc giải bài toán logarit rời rạc trên Z_p với p là số nguyên tố có dạng: $p = 2n + 1$, trong đó n là tích của hai số nguyên tố lớn sao cho việc phân tích n thành nhân tử là khó thực hiện. Để phá vỡ các lược đồ này cần phải giải được đồng thời bài toán phân tích n thành tích của hai thừa số nguyên tố p, q (*bài toán phân tích số*) và bài toán logarit rời rạc theo *modulo p và q* là các nhân tử của n (*bài toán logarit rời rạc trên* Z_p). Tuy nhiên, các lược đồ này vẫn tồn tại nhược điểm là kích thước chữ ký do chúng sinh ra khá lớn nên tốc độ xử lý chậm. Ngoài ra, việc sử dụng hai khóa công khai là không phù hợp với các hệ thống hiện tại. Trong [9], các tác giả đã giải quyết vấn đề rút gọn độ dài chữ ký, song điều đó cũng làm giảm đáng kể hiệu quả thực hiện của các lược đồ này.

Trong bài báo này, nhóm tác giả đề xuất một lược đồ chữ ký xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p nhằm nâng cao độ an toàn cho thuật toán và đảm bảo kích thước chữ ký nhỏ, mà không cần phải sử dụng giải pháp như trong [9, 10], từ đó nâng cao hiệu quả thực hiện của lược đồ trong các ứng dụng thực tế.

2. Xây dựng lược đồ chữ ký trên hai bài toán khó

2.1. Các bài toán cơ sở

2.1.1. Bài toán phân tích số

Bài toán phân tích số được phát biểu như sau: Cho số n ϵ N, hãy tìm biểu diễn: $n = p_1^{e_1}.p_2^{e_2}...p_i^{e_i}...p_k^{e_k}$, với: $e_i \geq 1$ và p_i là các số nguyên tố.

Một trường hợp riêng của bài toán phân tích số được ứng dụng để xây dựng hệ mật RSA [11] mà ở đó n là tích của hai số nguyên tố p và q. Khi đó, bài toán phân tích số hay còn gọi là bài toán $IFP_{(n)}$ được phát biểu như sau:

Bài toán $IFP_{(n)}$: Với mỗi số nguyên dương n, hãy tìm số nguyên tố p hoặc q thỏa mãn phương trình sau:

$$p.q = n$$

Giải thuật cho bài toán $IFP_{(n)}$ có thể được viết như một thuật toán tính hàm IFP(.) với biến đầu vào là n, còn giá trị hàm là p hoặc q của phương trình sau:

$$p = IFP(n)$$

Hoặc:

$$q = IFP(n)$$

Trong hệ mật RSA, bài toán phân tích số được sử dụng trong việc hình thành cặp khóa công khai/bí mật cho mỗi thực thể ký. Với việc giữ bí mật các tham số (p, q) thì việc tính được khóa bí mật (d) từ khóa công khai (e) và *modulo n* là một bài toán khó nếu p, q được chọn đủ lớn và mạnh. Hiện tại bài toán trên vẫn được coi là bài toán khó do chưa có giải thuật thời gian đa thức hay đa thức xác suất cho nó và hệ mật RSA là một minh chứng thực tế cho tính khó giải của bài toán này. Trong thực tế, các tham số p, q có thể chọn theo X9.31 hay FIPS 186 – 4 của Hoa Kỳ cho hệ mật RSA [12].

2.1.2. Bài toán logarit trên Z_p

Cho cặp số nguyên dương (p, g) với p là số nguyên tố, còn g là một phần tử của nhóm Z_p^*. Khi đó, bài toán logarit rời rạc trên Z_p hay còn gọi là bài toán $DLP_{(p, g)}$ được phát biểu như sau:

Bài toán $DLP_{(p, g)}$: Với mỗi số nguyên dương $y \in Z_p^*$, hãy tìm *x* thỏa mãn phương trình sau:

$$g^x \bmod p = y$$

Giải thuật cho bài toán $DLP_{(p, g)}$ có thể được viết như một thuật toán tính hàm $DL_pP(.)$ với biến đầu vào là *y*, còn giá trị hàm là *x* của phương trình sau:

$$x = DL_pP(y)$$

Bài toán $DLP_{(p, g)}$ là cơ sở để xây dựng nên hệ mật Elgamal, việc sử dụng rộng rãi của hệ mật Elgamal [13] và các biến thể của nó trong thực tế hiện nay cũng là một minh chứng cho tính khó giải của bài toán này.

2.1.3. Bài toán logarit trên Z_n

Cho cặp số nguyên dương (n, g) với *n* là tích hai số nguyên tố *p* và *q* sao cho bài toán phân tích số là khó giải trên Z_n, còn *g* là một phần tử của nhóm Z_n^*. Khi đó, bài toán logarit rời rạc trên Z_n hay còn gọi là bài toán $DLP_{(n, g)}$ được phát biểu như sau:

Bài toán $DLP_{(n, g)}$: Với mỗi số nguyên dương $y \in Z_n^*$, hãy tìm *x* thỏa mãn phương trình sau:

$$g^x \bmod n = y$$

Giải thuật cho bài toán $DLP_{(n, g)}$ có thể được viết như một thuật toán tính hàm $DL_nP(.)$ với biến đầu vào là *y*, còn giá trị hàm là *x* của phương trình sau:

$$x = DL_nP(y)$$

Ở dạng lược đồ chữ ký mới được đề xuất, mỗi thành viên của hệ thống tự chọn cho mình bộ tham số (n, g) và khóa bí mật *x* thỏa mãn: $1 < x < \varphi(n)$ và tính khóa công khai theo:

$$y = g^x \bmod n$$

Tương tự bài toán phân tích số $IFP_{(n)}$, bài toán $DLP_{(n, g)}$ cũng là cơ sở để xây dựng nên hệ mật RSA. Hiện tại chưa có giải thuật hiệu quả (thời gian đa thức hay đa thức xác suất) cho $DLP_{(n, g)}$, vì thế tính khó của việc giải bài toán logarit rời rạc trên Z_n có thể đặt ra với giả thiết là giải thuật cho bài toán này phải được thực hiện thông qua việc giải hai bài toán: bài toán phân tích *n* thành tích của hai số nguyên tố *p, q* (*bài toán phân tích số*) và bài toán logarit rời rạc theo *modulo p và q* là các nhân tử của *n* (*bài toán logarit rời rạc trên Z_p*). Như vậy, ý tưởng của giải pháp cho $DLP_{(n, g)}$ nằm ở chỗ nếu như độ khó để giải bài toán phân tích số là đủ lớn, thì độ khó để giải được bài toán $DLP_{(n, g)}$ sẽ là tích các độ khó của việc giải hai bài toán $IFP_{(n)}$ và bài toán $DLP_{(p, g)}$, với giả thiết xác suất xảy ra việc giải được đồng thời cả hai bài toán này là nhỏ, nên khả năng giải được bài toán $DLP_{(n, g)}$ là thấp.

2.2. Lược đồ mới đề xuất

Lược đồ mới đề xuất ở đây được phát triển trên cơ sở kết hợp đồng thời hai bài toán phân tích số và bài toán logarit rời rạc trên Z_p nhằm nâng cao độ an toàn của thuật toán chữ ký số, đồng thời có thể rút ngắn kích thước của chữ ký do lược đồ này sinh ra. Lược đồ mới đề xuất bao gồm các thuật toán hình thành tham số và khóa, thuật toán ký và kiểm tra chữ ký như sau:

2.2.1. Thuật toán hình thành tham số và khóa

Mỗi đối tượng ký trong hệ thống hình thành các tham số và khóa theo các bước như sau:

Thuật toán 1.1: Hình thành tham số và khóa.

Input: lp, lq – độ dài (tính theo bit) của số nguyên tố p, q.

Output: n, m, g, y, x_1, x_2.

Bước 1: Chọn 1 cặp số p, q nguyên tố với *len*(p) = *lp*, *len*(q) = *lq* sao cho bài toán phân tích số trên Z_n là khó giải.

Bước 2: Tính $n = p.\ q$ và $\varphi(n) = (p - 1).(q - 1)$.

Bước 3: Chọn p_1, q_1 là các số nguyên tố thỏa mãn $p_1|(p-1)$, $q_1|(q-1)$ và $p_1 \nmid (q-1)$, $q_1 \nmid (p-1)$

Bước 4: Tính $m = p_1.\ q_1$.

Bước 5: Chọn *g* là phần tử sinh của nhóm Z_n^* có bậc là *m* ($ord_g = m$), được tính theo

$g = \alpha^{\frac{\phi(n)}{m}} \bmod n$ và thỏa mãn $\gcd(g, n) = 1$, với $\alpha \in (1, n)$.

Bước 6: Chọn khóa bí mật thứ nhất x_1 trong khoảng (1, *m*).

Bước 7: Tính khóa công khai theo

$$y = (g)^{-x_1} \bmod n \quad (1)$$

Kiểm tra nếu: $y \geq \varphi(n)$ hoặc $\gcd(y, \phi(n)) \neq 1$ thì thực hiện lại từ Bước [6].

Bước 8: Tính khóa bí mật thứ hai theo

$$x_2 = y^{-1} \bmod \varphi(n) \quad (2)$$

Bước 9: Chọn hash function H: $\{0,1\}^* \rightarrow Z_h$, với h < n

Chú thích:

+ *len(.)* là hàm tính độ dài (theo bit) của một số;

+ Khóa công khai là *y*, khóa bí mật là (x_1, x_2) ;

+ Các tham số công khai là *n*, *g*; các tham số bí mật là: *p, q, p_1, q_1*, *m* và $\varphi(n)$.

2.2.2. Thuật toán ký

Thuật toán 1.2: Sinh chữ ký.

Input: n, g, m, x_1, x_2, M – bản tin cần ký.

Output: (E, S) – chữ ký

Bước 1: Chọn ngẫu nhiên giá trị *k* trong khoảng (*1, m*).

Bước 2: Tính giá trị *R* theo $R = g^k \bmod n$.

Bước 3: Tính thành phần thứ nhất của chữ ký theo

$$E = H(M \| R).$$

Bước 4: Tính thành phần thứ 2 của chữ ký theo

$$S = x_2 \times (k + x_1 \times E) \bmod m \quad (3)$$

Chú thích:

+ Toán tử "||" là phép nối 2 xâu bit.

2.2.3. Thuật toán kiểm tra

Thuật toán 1.3: Kiểm tra chữ ký.

Input: n, g, y, M – bản tin cần thẩm tra.

Output: (E, S) = true/false

Bước 1: Tính giá trị $\overline{R} = \left(g^S\right)^y \times (y)^E \bmod n$.

Bước 2: Tính giá trị: $\overline{E} = H(M \parallel \overline{R})$.

Bước 3: Nếu $\overline{E} = E$

thì (E, S) = *true*, ngược lại (E, S) = *false*.

Chú thích:

+ (E, S) = *true*: chữ ký hợp lệ, bản tin M được xác thực về nguồn gốc và tính toàn vẹn;

+ (E, S) = *false*: chữ ký hoặc/và bản tin bị giả mạo.

2.2.4. Tính đúng đắn của lược đồ mới đề xuất

Với các tham số và khóa được hình thành bởi **Thuật toán 1.1**, chữ ký (E, S) được sinh bởi **Thuật toán 1.2**, giá trị $\overline{E}$ được tạo bởi **Thuật toán 1.3** thì điều cần chứng minh ở đây là $\overline{E} = E$.

Thật vậy, do:

$$\begin{aligned}\overline{R} &= \left(g^S\right)^y \times (y)^E \bmod n \\ &= \left(g^{x_2.(k+x_1.E)} \bmod n\right)^y + \left(g^{-x_1} \bmod n\right)^E \bmod n \\ &= g^{(k+x_1.E).x_2.y} \times g^{-x_1.E} \bmod n = g^k \bmod n \\ &= R\end{aligned}$$

Suy ra điều cần chứng minh:

$$\overline{E} = H(M \parallel \overline{R}) = H(M \parallel R) = E$$

2.2.5. Ví dụ

Lược đồ mới đề xuất được minh họa bằng một ví dụ số như sau:

Sinh tham số và khóa (**Thuật toán 1.1**):

- Giá trị của p:

665420877979266637753312028002848613429272388001623144316752060268286403233932088225590750773394676644919414338465462495737551298755144622628204386189897 7.

- Giá trị của q:

845266763185109717517847868226466782189584328305935912907342209292896975762425806936582514876140983666110027689186190450926239552709811964296335159814273 7.

- Giá trị của p_1:

812141537786172241964572155002667002931252078421.

- Giá trị của q_1:

127418689836153951558896888393999215610802338170 7.

- Giá trị của n:

562458151685328562760856012755937409170516274881576189639674599726875512828697027190727478632309975263236214662743348388678978357861420315659185161717531270144365462047583719601216155009182885805901118435197678725718008599327362959612603532628788208787288305210831746140407838520377113964735249022311202800 49.

- Giá trị của m:

103482010706233385444343660125758834765808762075841633300915765154024740197809319682270878084464 7.

- Giá trị của g:

123054903129868507930321981147284150924908118149855205028134694949082443859284635229187912283722016298247234842452720930217545736171000644563598486755300616644790460654542967698114848748348688075508834056662024847686700185254472975825961969072278544638622485113804725445119978951440207808020617175737210694 52.

- Giá trị của x_1:

104441466614944086009696831821604447423731443578 3.

- Giá trị của y:

531661203794303973702004012747864649078810888411502543508893175695409620249787957980191524956734999549124343679209085135866500629771784432903658361177912981582592352261401879241682250428637006743275773012588944383896311543223143974313828336473272271991560779829574451292823374274758425910771084941581505855634 7.

- Giá trị của x_2:

530074211399657135695574133157250693366250855240668108639071440010768026008844251456762987034550135357874979458934503090077070165594919290357475598699631683976389365666861886686974704864045775277836981088596970207159495201356189285760233862477922063667966233493633384033652507190182766897048809769667019147 5.

Sinh chữ ký (**Thuật toán 1.2**):

Input: n, g, m, x_1, x_2, M.

Output: (E, S).

- Bản tin M: M = "*THIS IS A NEW DIGITAL SIGNATURE ALGRITHM*"

- M được mã hóa bằng chuỗi số:

840007200073000830003200073000830003200065000320007800069000870003200068000730007100073000840006500076000320008300073000710007800065000840008500082000690003200065000760007100082000730008400072000 77.

- Giá trị của k:

690106512842560511386991966503156369472934257177.

- Giá trị của R tính được:

840663895186853831166965961244814549950978355836680535003311897572284417793542576444591124899095895127382459565641404282896535669902625819889154908137967990822408152475683073710506139569686001072633760487263497766933003741488786939889557396664791581838426355495608928811327457970817167124936392533617750947 2.

- Giá trị của E tính được:

300145922958083012796549685211220698317918477983.

- Giá trị của S tính được:

221700019441850739139835627511419197779684132363648607038688055358057098996108751901616842162763.

Kiểm tra chữ ký (**Thuật toán 1.3**):

Input: n, g, y, M.

- Giá trị của M cần thẩm tra: M = "*THIS IS A NEW DIGITAL SIGNATURE ALGRITHM*"

- M được mã hóa bằng chuỗi số:

840007200073000830003200073000830003200065000320007800069000870003200068000730007100073000840006500076000320008300073000710007800065000840008500082000690003200065000760007100082000730008400072000 77.

- Giá trị của $\overline{R}$ tính được:

840663895186853831166965961244814549950978355836680535003311897572284417793542576444591124899095895127382459565641404282896535669902625819889154908137967990822408152475683073710506139569686001072633760487263497766933003741488786939889557396664791581838426355495608928811327457970817167124936392533616177509472.

- Giá trị của $\overline{E}$ tính được:

300145922958083012796549685211220698317918477983.

- Như vậy, $\overline{E} = E$, chữ ký được công nhận là hợp lệ.

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

a. Tấn công khóa bí mật

Ở lược đồ mới đề xuất, khóa bí mật của một đối tượng ký là cặp (x_1, x_2), tính an toàn của lược đồ sẽ bị phá vỡ hoàn toàn khi cặp khóa này có thể tính được bởi một hay các đối tượng không mong muốn. Từ **Thuật toán 1.1** cho thấy, để tìm được x_2 cần phải tính được tham số $\varphi(n)$, nghĩa là phải giải được $IFP_{(n)}$, còn để tính được x_1 cần phải giải được $DLP_{(n, g)}$. Như vậy, để tìm được cặp khóa bí mật này, kẻ tấn công cần phải giải được đồng thời hai bài toán $IFP_{(n)}$ và $DLP_{(n, g)}$ đã chỉ ra ở trên. Tuy nhiên, việc giải được $DLP_{(n, g)}$ là khó tương đương với việc giải đồng thời hai bài toán $IFP_{(n)}$ và $DLP_{(p, g)}$. Vì thế, có thể dẫn ra rằng, tính an toàn về khóa của lược đồ mới đề xuất được đảm bảo bởi tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p.

b. Tấn công giả mạo chữ ký

Từ điều kiện của **Thuật toán 1.3**, một cặp (E,S) bất kỳ sẽ được coi là chữ ký hợp lệ của đối tượng sở hữu các tham số công khai (n,g,y) lên bản tin M nếu thỏa mãn:

$$E = H\left(M \,\|\, \left(\left(g^S\right)^\gamma \times (y)^E \bmod n\right)\right) \quad (4)$$

Từ (4) cho thấy, việc tìm cặp (E, S) bằng cách chọn trước một trong hai giá trị rồi tính giá trị còn lại đều khó hơn việc giải $DLP_{(n, g)}$. Hơn nữa, nếu H(.) được chọn là hàm băm có độ an toàn cao (SHA 256/512,...) thì việc chọn ngẫu nhiên cặp (E, S) thỏa mãn (4) hoàn toàn không khả thi trong các ứng dụng thực tế.

2.2.7. Tính hiệu quả của lược đồ mới đề xuất

Tính hiệu quả của lược đồ chữ ký có thể đánh giá qua chi phí thực hiện của các thuật toán ký, kiểm tra chữ ký và kích thước chữ ký mà lược đồ sinh ra. Ở mục này, tính hiệu quả của lược đồ mới đề xuất sẽ được đánh giá và so sánh với các kết quả trong [9].

a. Kích thước chữ ký

Kích thước chữ ký do lược đồ mới đề xuất tạo ra sẽ được so sánh với kích thước chữ ký của các lược đồ trong [9] với cùng bộ tham số đã được lựa chọn.

Trong [9], các lược đồ chữ ký sử dụng *modulo n* được tạo ra từ hai số nguyên tố q và q': $n = q \times q'$. Với |q| = |q'| = 512 bit, nên |n| = 1024 bit. Hàm băm được lựa chọn có kích thước giá trị đầu ra là 160 bit, vì thế kích thước chữ ký do các lược đồ này tạo ra là: |E| + |S| = 160 bit + 1024 bit = 1184 bit.

Khi áp dụng phương pháp rút ngắn kích thước chữ ký theo [10] với các tham số $|q| \approx |q'| \geq 512$ bit, $|n| \geq 1024$ bit, $|p| \geq 1024$ bit, $|\gamma| = 160$ bit và $|\partial| = 160$ bit. Ở đây, $p = 2n+1$ và $\gamma = \gamma'.\gamma''$, với $\gamma' | (q-1)$, $\gamma'' | (q'-1)$, $\gamma'' \nmid (q-1)$, $\gamma' \nmid (q'-1)$. Khi đó, chữ ký do các lược đồ trong [9] tạo ra là bộ ba tham số (k,g,v) và sẽ có kích thước là $|k| + |g| + |v| \geq 480$ bit.

Ở lược đồ mới đề xuất, các tham số (p, q, n) là tương đương với (q, q', n) trong [9], còn các tham số (p_1, q_1, m) của lược đồ mới đề xuất và $(\gamma', \gamma'', \gamma)$ trong [9] cũng có vai trò tương đương nhau. Nếu chọn kích thước các tham số tương tự như ở các lược đồ trong [9] thì kích thước chữ ký do lược đồ mới đề xuất tạo ra là |E| + |S| = 160 bit + 160 bit = 320 bit.

Nhận xét:

Từ các kết quả trên cho thấy, với bộ tham số đã lựa chọn, chữ ký do lược đồ mới đề xuất tạo ra có kích thước nhỏ hơn 3 lần so với kích thước chữ ký do các lược đồ trong [9] tạo ra và nhỏ hơn 1,5 lần khi các lược đồ này áp dụng phương pháp rút gọn chữ ký theo [10].

b. Chi phí thực hiện

Chi phí thực hiện hay chi phí tính toán của các thuật toán ký và kiểm tra chữ ký có thể được đánh giá thông qua số phép toán cần thực hiện hay tổng thời gian cần thực hiện các phép toán để hình thành và kiểm tra chữ ký, ở đây quy ước sử dụng các ký hiệu:

T_{exp}: thời gian thực hiện phép toán mũ modulo.

T_h: thời gian thực hiện hàm băm.

T_{mul}: thời gian thực hiện phép nhân modulo.

T_{inv}: thời gian thực hiện phép nghịch đảo modulo.

T_{sr} : thời gian thực hiện phép khai căn bậc 2 modulo.

Chú ý:

Thuật toán sinh tham số và khóa chỉ cần thực hiện một lần duy nhất với mọi đối tượng ký. Vì thế, chi phí tính toán cho thuật toán sinh tham số và khóa có thể bỏ qua khi tính toán chi phí thực hiện lược đồ ký.

+ Thời gian thực hiện của lược đồ chữ ký mới đề xuất:

Thời gian thực hiện thuật toán ký: $(T_{exp} + T_h + 2T_{mul})$.

Thời gian thực hiện thuật toán kiểm tra: $(2T_{exp} + T_h + 2T_{mul})$.

+ Thời gian thực hiện của lược đồ chữ ký thứ nhất trong [9]:

Thời gian thực hiện thuật toán ký: $(T_{exp} + T_h + T_{mul} + T_{sr})$.

Thời gian thực hiện thuật toán kiểm tra: $(3T_{exp} + T_h + T_{mul})$.

Chú ý:

Để tính được thành phần S của chữ ký theo $S^2 = k - x.E \bmod n$ [9], thì $(k - x.E)$ phải là đồng dư bậc 2 modulo n. Điều đó không luôn xảy ra với mọi giá trị k được chọn ở bước thứ nhất của thuật toán ký. Nói cách khác, để tạo được giá trị S, các bước của thuật toán ký có thể sẽ phải thực hiện nhiều lần, giả sử số lần cần phải thực hiện là N, khi đó thời gian thực hiện thuật toán ký của lược đồ thứ nhất trong [9] sẽ là $N.(T_{exp} + T_h + T_{mul} + T_{sr})$.

+ Thời gian thực hiện của lược đồ chữ ký thứ hai trong [9]:

Thời gian thực hiện thuật toán ký: $(2T_{exp} + T_h + T_{mul})$.

Thời gian thực hiện thuật toán kiểm tra: $(3T_{exp} + T_h + T_{mul})$.

Chú ý:

Để rút ngắn độ dài chữ ký theo phương pháp [10] thì các lược đồ trong [9] cần phải thực hiện bổ sung một số phép tính lũy thừa, nhân, nghịch đảo modulo nữa. Vì thế, chi phí thực hiện các lược đồ này sẽ tăng đáng kể so với các kết quả đã chỉ ra trên đây [9].

Nhận xét:

Các kết quả trên cho thấy hiệu quả thực hiện của lược đồ mới đề xuất cao hơn các lược đồ trong [9] cả hai trường hợp áp dụng và không áp dụng phương pháp rút ngắn kích thước chữ ký theo [10].

3. Kết luận

Trong bài báo này, nhóm tác giả đề xuất một lược đồ chữ ký số mới xây dựng trên cơ sở kết hợp đồng thời hai bài toán phân tích số và logarit rời rạc trên Z_p nhằm nâng cao độ an toàn của thuật toán chữ ký số. Tính an toàn của lược đồ này được đảm bảo bằng tính khó của việc giải đồng thời hai bài toán nói trên, nghĩa là tính an toàn của lược đồ mới đề xuất chỉ bị phá vỡ khi đồng thời giải được các bài toán này. Ngoài ra, lược đồ mới đề xuất có kích thước nhỏ hơn và hiệu quả thực hiện cũng cao hơn so với một số lược đồ [9, 10] đã được đề cập trong bài báo. Điều này sẽ giúp cho việc nâng cao hiệu quả thực hiện của lược đồ trong các ứng dụng thực tế.

TÀI LIỆU THAM KHẢO

[1] Eddie Shahrie Ismail, Tahat N.M.F., Rokiah. R. Ahmad, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms", *Journal of Mathematics and Statistics*, 12(3), 04/2008, pp. 222-225.

[2] Swati Verma1, Birendra Kumar Sharma, "A New Digital Signature Scheme Based on Two Hard Problems", *International Journal of Pure and Applied Sciences and Technology*, 5(2), 2011, pp. 55-59.

[3] Sushila Vishnoi, Vishal Shrivastava, "A New Digital Signature Algorithm Based on Factorization and Discrete Logarithm Problem", *International Journal of Computer Trends and Technology*, Vol. 3, Issue 4, 2012, pp. 653-657.

[4] Shimin Wei, "Digital Signature Scheme Based on Two Hard Problems", *International Journal of Computer Science and Network Security*, Vol. 7, No. 12, December 2007, pp. 207-209.

[5] Qin Yanlin, Wu Xiaoping, "New Digital Signature Scheme Based on both ECDLP and IFP", *Computer Science and Information Technology*, *2nd IEEE International Conference*, 8-11 Aug. 2009, pp. 348-351.

[6] Q. X. WU, Y. X. Yang and Z. M. HU, "New Signature Schemes Based on Discrete Logarithms and Factoring", *Journal of Beijing University of Posts and Telecommunications*, Vol. 24, January 2001, pp. 61-65.

[7] Z. Y. Shen and X. Y. Yu, "Digital Signature Scheme Based on Discrete Logarithms and Factoring", *Information Technology*, Vol. 28, June 2004, pp. 21-22.

[8] N. H. Minh, D. V. Binh, N. T. Giang and N. A. Moldovyan, "Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems", *Applied Mathematical Sciences*, Vol. 6, No. 139, 2012, pp. 6903-6910.

[9] Binh V. Do, Minh H. Nguyen, Nikolay A. Moldovyan, "Digital Signature Schemes from Two Hard Problems", *Multimedia and Ubiquitous Engineering*, *Lecture Notes in Electrical Engineering 240*, May 9-11, 2013, pp. 817-825.

[10] Moldovyan NA, "Short Signatures from Difficulty of Factorization Problem", *Int J Netw Secur*, 8(1), 2009, pp. 90-95.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Commun. of the ACM*, 21, 1978, pp. 120-126.

[12] National Institute of Standards and Technology, NIST FIPS PUB 186-4, *Digital Signature Standard*, U.S. Department of Commerce, 2013.

[13] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, Vol. IT-31, No. 41985, 2009, pp. 469-472.

(BBT nhận bài: 16/5/2018, hoàn tất thủ tục phản biện: 24/6/2018)