ISSN 2354-0575

MỘT DẠNG LƯỢC ĐỒ CHỮ KÝ SỐ TỔNG QUÁT

Nguyễn Hữu Mộng
Trường Đại học Sư phạm Kỹ thuật Hưng Yên

Ngày tòa soạn nhận được bài báo: 05/02/2018
Ngày phản biện đánh giá và sửa chữa: 06/03/2018
Ngày bài báo được xét duyệt đăng: 09/03/2018

Tóm tắt:

Bài viết trình bày một lược đồ tổng quát cho chữ ký số. Tính tổng quát của lược đồ phụ thuộc vào sự tuỳ biến của một số hàm số nguyên như các tham số sinh các chữ ký số. Từ lược đồ tổng quát bằng cách tuỳ biến các hàm số nguyên ta có thể thu được các lược đồ cụ thể khác nhau. Bài viết còn nhấn mạnh đến các khía cạnh toán học và đặc biệt là tính đúng đắn của các thuật toán. Tính đúng đắn của lược đồ nói chung thể hiện ở chỗ từ các chữ ký nhận được và văn bản nhận được ta có thể xác thực được tính toàn vẹn và tính nguồn gốc của văn bản nhận được.

Từ khoá: *Lược đồ, chữ ký số, RSA, số nguyên tố lớn, hàm ơle, khoá công khai, khoá bí mật.*

1. Đặt vấn đề

Từ khi ra đời đến nay thuật toán RSA [1] được sử dụng rộng rãi trên thế giới với mục đích bảo mật tối đa một văn bản được gửi đi. Sự mở rộng và phát triển thuật toán này cho việc xác thực một văn bản đã được hưởng ứng và thực hiện mạnh mẽ trong nước và trên thế giới những năm gần đây [2,3,..,17]. Hàng loạt các cơ quan xác thực ra đời để cung cấp các chữ ký số cho các khách hàng khác nhau.

Thuật toán RSA về mặt toán học là rất chặt chẽ và chính xác, do đó, nó có tính bảo mật cao. Tính bảo mật của thuật toán RSA dựa vào tính khó của bài toán phân tích số và bài toán khai căn theo modulo. Do vậy, khi phát triển thuật toán này cho việc gửi các văn bản lớn bắt buộc phải thay đổi một số trật tự trong thuật toán cũng như các phương pháp tạo ra chữ ký. Về mặt hình thức thì một lược đồ chữ ký số áp dụng cho việc xác thực văn bản có các bước cơ bản sau đây:

- Lựa chọn các tham số: các khoá bí mật và các khoá công khai.
- Hình thành chữ ký – ký lên văn bản.
- Kiểm tra chữ ký – xác thực chữ ký.

Tất cả các lược đồ được đề xuất gần đây cơ bản vẫn duy trì theo các bước trên chỉ khác nhau về phương pháp ký và tất nhiên là khác nhau cả phương pháp kiểm tra. Một lược đồ mới đề xuất đều phải có phương pháp ký mới và phương pháp kiểm tra tương thích. Bản chất của một lược đồ chữ ký số là người nhận văn bản sử dụng các khoá công khai để kiểm tra tính xác thực của văn bản, tức là, kiểm tra nội dung văn bản có bị thay đổi không và văn bản có đến từ người gửi chữ ký không?.

Trong bài viết này, chúng tôi đưa ra một lược đồ mới tổng quát bằng cách sử dụng một số hàm nguyên để hình thành chữ ký nhưng vẫn đảm bảo được tính xác thực của chữ ký số. Từ lược đồ tổng quát này, bằng cách tuỳ biến các hàm nguyên ta có thể thu được nhiều lược đồ cụ thể theo mong muốn của người dùng. Ngoài ra, bài viết còn đề cập đến các khía cạnh toán học của các vấn đề đặt ra có ảnh hưởng đến quá trình tạo các khoá, chữ kí và quá trình kiểm tra tính xác thực của chữ ký.

2. Lược đồ tổng quát

Giả sử A cần gửi cho B một văn bản M và A muốn B nhận đúng văn bản và do A gửi. Muốn vậy, A thực hiện như sau:

- A tạo các khoá bí mật và công khai.
- A băm văn bản M được m.
- A sử dụng các khoá và m tạo ra chữ kí số.
- A gửi văn bản và chữ ký số cho B.
- B nhận được văn bản và chữ ký: B băm văn bản nhận được và thu được m'.
- B sử dụng các khoá công khai để tính m từ chữ ký nhận được.
- Nếu $m = m'$ thì tính xác thực đúng đắn, nếu không không xác thực được.

Cụ thể quá trình này được thể hiện bằng các thuật toán sau đây:

2.1. Thuật toán chọn các tham số và khóa

1^0. Chọn hai số nguyên tố lớn p, q.

2^0. Tính $n = pq, \phi(n) = (p-1)(q-1)$.

3^0. Chọn một số nguyên t thoả mãn các điều kiện: $1 < t < \phi(n)$; $\gcd(t, \phi(n)) = 1$.

4^0. Chọn một số x trong khoảng $(1, n)$ và nguyên tố cùng nhau với n, tức là,

$1 < x < n$, $\gcd(x,n) = 1$.

5^0. Tính giá trị

$$y = x^t \bmod n \qquad (1)$$

Ghi chú:

1) Giá trị x, p, q, $\phi(n)$ được giữ bí mật (các khoá bí mật), còn y, t, n làm khoá công khai.

2) Các số nguyên tố lớn p, q có thể chọn từ trước để giảm thời gian triển khai lược đồ. Các số nguyên tố p, q có thể chọn bằng nhiều phương pháp khác nhau ví dụ như phương pháp Rabin – Miller, Lehmann, Strong Primes, v.v.. Ta có thể sử dụng thuật toán sinh số nguyên tố mạnh – RSA (thuật toán D. M. Gordon) [18] để nâng cao tính chống tấn công làm lộ khoá bí mật.

3) Việc chọn các số nguyên t và x có thể thực hiện được bằng thuật toán Euclid mở rộng. Đã có những nghiên cứu xem xét vấn đề lựa chọn các tham số này sao cho thuật toán có độ bảo mật cao nhất có thể [12,13,14,15].

4) Việc tính khoá công khai $y = x^t \bmod n$ được thực hiện bằng thuật toán bình phương và nhân trong phép modulo n [24]. Ta cũng có thể tính khoá công khai bằng công thức gần giống như trong thuật toán RSA

$$y = x^{-t} \bmod n.$$

2.2. Thuật toán hình thành chữ ký

Để thực hiện thuật toán ký, tức là, tạo ra chữ ký số lên văn bản. Chữ ký số lên văn bản thực chất là một số nguyên lớn được tạo ra bằng thuật toán ký từ giá trị hàm băm của văn bản cần ký M mà người ký muốn chuyển cho người nhận và khoá bí mật của người ký. Giả thiết rằng, lược đồ chữ ký Ở đây chúng ta tạo ra một cặp chữ ký 2 thành phần là (r, s) và mỗi chữ ký đều gắn chặt với giá trị băm m tương ứng với văn bản M. Để tạo ra các chữ ký chúng tôi xây dựng ba hàm số khác nhau là f_1, f_2, f_3. Đây là ba hàm hai biến số và chúng đều là những hàm có giá trị nguyên, tức là, đó là các hàm xác định trên miền các cặp số nguyên và miền giá trị của chúng cũng là các số nguyên. Có thể nghiên cứu thêm về tính chất các hàm để thu được một lược đồ hiệu quả cao. Ở đây ta chưa đề cập đến các vấn đề này. Chúng tôi sẽ có thêm những nghiên cứu tiếp theo bằng cách đề xuất các hàm cụ thể để xây dựng các lược đồ có thể ứng dụng vào thực tế. Chẳng hạn như $f_1 = k, f_2 = 1$, $f_3 = H(M).r$, trong đó, $H(M)$ là giá trị hàm băm của văn bản M. Khi chọn một bộ 3 hàm cụ thể thì hình thức xác thực có thay đổi nhưng bản chất vẫn không thay đổi là trong mọi trường hợp ta đều chứng minh được $m = m'$. Yêu cầu chủ yếu của chữ kí điện tử là sử dụng nó thì ta có thể khẳng định được tính toàn vẹn của văn bản gửi đi và nguồn gốc của văn bản đó. Ta cần nhấn mạnh rằng, khác với chữ ký RSA, ở đây và các lược đồ chữ ký số lên văn bản nói chung chỉ xác thực tính toàn vẹn và nguồn gốc văn bản chứ không đảm bảo được tính toàn vẹn của văn bản. Chính yêu cầu bắt buộc này đối với các loại chữ ký điện tử cho phép người dùng tuỳ biến cách sinh ra chúng, miễn làm sao đảm bảo được tính xác thực. Ta chọn hàm thứ nhất $f_1(k, m)$ là hàm hai biến, trong đó, biến thứ nhất là số nguyên k trong khoảng từ 1 đến $\phi(n)$ và nguyên tố cùng $\phi(n)$, biến thứ hai là giá trị băm m của văn bản M. Hàm này được dùng để sinh ra thành phần thứ nhất của chữ ký số hay chữ ký số thứ nhất r. Thành phần r này lại là một biến của các hàm $f_2(r, m), f_3(r, m)$, còn biến thứ hai của các hàm này đều là giá trị băm m của văn bản M. Trong từng trường hợp cụ thể có thể chọn được các dạng thích hợp cho từng hàm số. Trong phần chứng minh tính đúng đắn của lược đồ ta sẽ đề xuất một số tính chất quyết định của các hàm số này trong việc xác thực văn bản.

Sau khi chọn được các hàm số f_1, f_2, f_3 người gửi sử dụng các tham số đã được hình thành trong thuật toán hình thành các tham số và khoá tiến hành xây dựng các thành phần chữ ký số. Thuật toán gồm các bước như sau:

1^0. Băm văn bản M

$$m = H(M)$$

2^0. Chọn một số nguyên k thoả mãn điều kiện

$$1 < k < \phi(n);\ \gcd(k, \phi(n)) = 1.$$

3^0. Tính giá trị hàm số $f_1 = f_1(k,m)$.

4^0. Tạo thành phân thứ nhất của chữ ký hay chữ ký số thứ nhất:

$$r = y^{f_1} \bmod n, \qquad (2)$$

trong đó, y là khoá công khai (1) được tạo trong thuật toán sinh các khoá.

5^0. Tính các giá trị $f_2 = f_2(r,m),\ f_3 = f_3(r,m)$.

6^0. Tạo thành phần thứ hai của chữ ký

$$s = x^{f_1 \cdot f_2 - f_3} \bmod n, \qquad (3)$$

trong đó, x là khoá bí mật được chọn trong thuật toán sinh các khoá.

Chú ý:

1) Hàm băm văn bản $H(M)$ là hàm một chiều, tức là, từ giá trị băm m không thể khôi phục được văn bản M. Do đó, người gửi bắt buộc phải gửi cả văn bản gốc cho người nhận. Các hàm băm hiện đại có một tính chất đặc biệt quan quan trọng là chưa tìm thấy hai văn bản khác nhau có cùng giá trị băm. Chính tính chất này cho ta khả năng xác thực tính toàn vẹn của văn bản. Tức là, nếu người nhận có được giá trị băm m của văn bản gốc (văn bản cần nhận) và nhận được một văn bản M' thì sau khi băm văn bản M' được m' và nếu $m = m'$ thì kết luận chắc chắn văn bản nhận được toàn vẹn không bị thay đổi nội dung, còn nếu $m' \neq m$ thì chắc chắn nội dung văn bản đã bị thay đổi.

2) Giá trị k cũng được chọn giống như t trong thuật toán sinh các khoá và không loại trừ khả năng chúng bằng nhau. Điều này luôn xảy ra với

cùng $\phi(n)$ vì phương pháp chung chọn các số này là như nhau và đều kiểm tra từ số bế nhất, do đó các số chọn được là như nhau.

3) Văn bản M và chữ ký r, s được gửi cho B. Trước khi gửi đi, có thể M được mã hoá bằng một thuật toán mã hoá thoả thuận trước với B.

4) Việc tính các giá trị r, s cũng giống như tính y cùng một thuật toán bình phương và nhân.

2.3. Thuật toán kiểm tra chữ ký

Ý nghĩa chính của chữ ký số điện tử được thể hiện chính trong thuật toán kiểm tra chữ ký, tức là, sau khi nhận được chữ ký số (cặp các số r, s) và văn bản M', người nhận tiến hành băm lại văn bản nhận được và thu được một số m' nào đó, và nếu nhận đúng văn bản gốc thì ta phải có $m' = m$, trong đó, m là giá trị băm của văn bản gốc M. Do vậy, nếu hai giá trị băm bằng nhau thì nội dung văn bản không bị thay đổi. Nhưng người nhận không biết m mà chỉ nhận được chữ ký liên hệ chặt chẽ với m và không thể tính được m từ chữ ký. Do đó, lược đồ tổng quát đề xuất ở đây cho phép ta thông qua chữ ký (tất nhiên là với giả thiết nhận đúng chữ ký!) và bằng các phép biến đổi (chủ yếu là phép nâng lên luỹ thừa trong modulo n) mà có thể suy ra được các giá trị m và m' có bằng nhau hay không. Và chỉ khi kết luận được hai giá trị này bằng nhau thì có thể kết luận người nhận nhận đúng văn bản và đúng người gửi, tức là, tính toàn vẹn và tính xác thực của văn bản được đảm bảo. Sự liên quan đến m là sự liên quan ẩn dưới các chữ ký, bởi vì các chữ ký hình thành từ m và các hàm bổ trợ. Người nhận dùng khoá công khai y để giải mã, tức là, để kiểm tra. Thuật toán kiểm tra bao gồm các bước sau đây:

1^0. Tính $m' = H(M')$.

2^0. Tính các giá trị

$$u = r^{f_2(r,m')} \bmod n;$$
$$v = \left(s^t . y^{f_3(r,m')}\right) \bmod n.$$

3^0. Kiểm tra $u = v$?

- Nếu đẳng thức đúng thì kết luận nhận được văn bản đúng và đúng người gửi.

- Nếu đẳng thức sai thì không xác thực được văn bản nhận được: văn bản nhận được sai hoặc nhận được không phải từ người gửi chính thức, tức là, nhận được chữ ký giả mạo.

Chú ý:

1) Người nhận tính được các giá trị u, v nhờ biết các khoá y, t, các giá trị r, s, các hàm f_2, f_3 cũng như giá trị băm m' của văn bản M' nhận được tính theo cùng một hàm băm thoả thuận trước với người gửi.

2) Các giá trị u, v được tính theo thuật toán bình phương và nhân áp dụng cho phép mũ modulo n.

3. Tính đúng đắn của lược đồ

Tính đúng đắn của lược đồ được chứng minh bằng khẳng định $u = v$ khi bản tin cần thẩm tra không bị thay đổi nội dung và chữ ký tương ứng không bị giả mạo. Ngược lại, nếu 1 trong 2 điều kiện đó hoặc cả 2 không thoả mãn, nghĩa là bản tin bị sửa đổi nội dung, hoặc chữ ký bị giả mạo hay cả 2 cùng xảy ra thì $u \neq v$. Trong đó u, v được tính trong thuật toán kiểm tra chữ ký. Ta cần phải nhấn mạnh rằng, tính đúng đắn của thuật toán chỉ xảy ra khi người nhận nhận đúng văn bản M và đúng chữ ký lên văn bản này. Như vậy, nếu nhận sai chữ ký hay nhận sai văn bản hay cả hai thì tính đúng đắn không xảy ra hay không xác thực được tính toàn vẹn của văn bản cũng như nguồn gốc của văn bản đó.

Giả sử m là giá trị văn bản gửi đi, m' là giá trị văn bản nhận được và

$$u = r^{f_2(r,m')} \bmod n;$$
$$v = \left(s^t . y^{f_3(r,m')}\right) \bmod n, \quad (4)$$

trong đó, r, s là các chữ ký nhận được và được tính theo các công thức (2)-(3), t, y là các khoá công khai, f_2, f_3 là các hàm đã biết như trong thuật toán hình thành chữ kí. Ta phải chứng minh rằng: nếu $u = v$ thì $m = m'$ và ngược lại, nếu $u \neq v$ thì $m \neq m'$.

Chứng minh. Giả sử $u = v$. Vậy ta có

$$r^{f_2(r,m')} \bmod n = \left(s^t . y^{f_3(r,m')}\right) \bmod n. \quad (5)$$

Từ các công thức (1)-(3) ta được

$$s^t = x^{(f_1.f_2-f_3).t} \bmod n = y^{f_1.f_2-f_3} \bmod n.$$
$$v = y^{f_1f_2-f_3} . y^{f_3(r,m')} \bmod n = y^{f_1f_2} . y^{f_3(r,m')-f_3} \bmod n.$$
$$u = r^{f_2(r,m')} \bmod n = y^{f_1.f_2(r,m')} \bmod n.$$

Do đó, nếu $u = v$ thì ta phải có

$$y^{f_1f_2} . y^{f_3(r,m')-f_3} \equiv y^{f_1.f_2(r,m')} \bmod n,$$

hay

$$y^{f_1f_2} . y^{f_3(r,m')-f_3} \equiv y^{f_1.f_2(r,m')} \bmod n,$$
$$1 \equiv y^{f_1(f_2(r,m')-f_2)} . y^{f_3-f_3(r,m')} \bmod n.$$

Đẳng thức cuối cùng trên đây có thể xảy ra không phải với mọi hàm f_2, f_3. Tuy nhiên, nếu các phương trình

$$f_2(r,m) = h_2, r = \text{const}, h_2 = \text{const};$$
$$f_3(r,m) = h_3, r = \text{const}, h_3 = \text{const}$$

có nghiệm duy nhất m thì từ đẳng thức trên suy ra $m = m'$.

Vậy, nếu các hàm f_2, f_3 là các đơn ánh theo m thì từ điều kiện $u = v$ suy ra $m = m'$. Ngược lại, nếu $u \neq v$ và các hàm f_2, f_3 vẫn là các đơn ánh thì suy luận tương tự ta được $m \neq m'$.

Từ đây ta thấy, nếu các hàm f_2, f_3 là đơn ánh thì để kiểm tra tính xác thực của văn bản nhận được ta chỉ việc tính các giá trị $f_2(r,m'), f_3(r,m')$

và so sánh chúng tương ứng với các giá trị đã có $f_2(r,m), f_3(r,m)$ và nếu

$$f_2(r,m) = f_2(r,m'); \quad f_3(r,m) = f_3(r,m') \tag{6}$$

thì kết luận tính xác thực được đảm bảo. Do đó, thay vì phải tính các giá trị *u, v* theo các công thức (4) ta chỉ cần tính các giá trị $f_2(r,m'), f_3(r,m')$ đơn giản hơn nhiều và nếu thoả mãn các đẳng thức (6) thì kết luận $m = m'$, tức là, tính xác thực được đảm bảo, nội dung văn bản nhận được không bị thay đổi.

4. Bàn về tính an toàn của lược đồ chữ ký số

Tính an toàn của lược đồ thể hiện ở chỗ người nhận xác thực được nội dung và nguồn gốc của văn bản nhận được đồng thời khả năng không xác thực được là ít xảy ra. Chỉ có như vậy thì một lược đồ chữ ký số mới có ý nghĩa và mới áp dụng được cho việc truyền thông tin trên mạng.

Ta có 4 tình huống sau đây:

- Nhận đúng văn bản và đúng chữ ký.
- Nhận đúng chữ ký nhưng sai văn bản.
- Nhận sai chữ ký nhưng đúng văn bản.
- Sai cả hai.

Xét tình huống thứ nhất: nhận đúng văn bản và đúng chữ ký. Rõ ràng khi đó hàm kiểm tra văn bản cho ta giá trị TRUE, tức là, văn bản đúng và đúng người gửi. Ở đây có sự tương ứng như sau: người gửi chữ ký và người gửi văn bản là một. Tuy nhiên có một câu hỏi như sau: Làm sao biết đúng người gửi và đúng văn bản cần nhận? Tức là người nhận có nhận đúng văn bản cần nhận và tới từ người gửi văn bản đó không? Có nhiều người gửi đến người nhận và có thể cùng một văn bản? Làm sao phân biệt được ai gửi? Chẳng hạn, một người khác khi chặn được văn bản và chữ ký có thể sử dụng các khoá công khai để ký lên một văn bản khác và gửi đi. Khi đó, rõ ràng người nhận hoàn toàn không thể biết được ai gửi bởi vì kiểm tra vẫn cho TRUE. Như vậy, tính an toàn trong trường hợp này phụ thuộc vào mức độ an ninh mạng người dùng.

Tình huống thứ hai: nhận đúng chữ ký nhưng nhận văn bản sai. Trong trường hợp này rõ ràng là các giá trị *u, v* khác nhau, tức hàm xác thực False. Tuy nhiên người nhận bối rối vì không thể biết được văn bản sai hay chữ ký sai hay cả hai. Trong trường hợp này kẻ tấn công không làm thay đổi chữ ký nhưng làm sai văn bản với mục đích phá sự tính toàn vẹn của văn bản giao dịch. Do đó, trong trường hợp này tính an toàn của lược đồ không bị đe doạ.

Tình huống thứ ba: nhận sai chữ ký nhưng đúng văn bản. Tình huống này có thể coi là tình huống tấn công chữ ký hay giả mạo chữ ký. Kẻ tấn công như vậy chỉ làm sai lệch nguồn gốc xuất xứ văn bản, tức người ký văn bản. Tuy nhiên có một điều thực tế là chặn được chữ ký, chặn được văn bản mà chỉ thay đổi chữ ký và không thay đổi văn bản thì kẻ giả mạo chỉ là kẻ phá bĩnh mà thôi. Ta cũng nên nhấn mạnh rằng, kể cả trong tình huống này, vai trò tính an toàn của lược đồ không được thể hiện.

Tình huống cuối cùng: nhận sai cả hai nội dung. Đây mới là tính huống đáng kể. Kẻ tấn công với mục đích giả mạo chữ ký để gửi đi một văn bản theo ý mình (có lợi cho mình) y như người gửi thật. Thật vậy, nếu kẻ tấn công chặn được cả hai thứ: chữ ký và văn bản thì chúng hoàn toàn chủ động như người ký chính thức, lấy một văn bản khác và thực hiện các bước như trên và gửi lại người gửi. Cái đáng nói là người nhận vẫn xác thực đúng nhưng không biết mọi thứ đã bị đánh tráo. Như vậy, trong trường hợp này, vai trò tính an toàn của lược đồ vẫn không được thể hiện.

Ta trao đổi thêm về chữ ký số RSA khi gửi văn bản (không phải thuật toán RSA). Giả sử cần trao đổi một văn bản *M* giữa *A* và *B*. Ta xét hai trường hợp:

- Trường hợp 1. *B* tạo các khoá, giữ lại khoá bí mật. *A* tạo chữ ký từ các khoá công khai và giá trị băm *m* của văn bản *M* rồi gửi chữ ký và văn bản cho *B*. *B* băm văn bản nhận được thành một số *m'* rồi dùng khoá bí mật tính được giá trị *m* để kiểm tra. Nếu *m = m'* thì tính xác thực đúng đắn: đúng văn bản đúng chữ ký. Trong trường hợp này vẫn xảy ra bốn tình huống như trình bày trên đây và trong từng trường hợp thuật toán không đảm bảo được tính bảo mật, chỉ đảm bảo được tính xác thực, tức là, nếu nhận đúng cả hai văn bản và chữ ký thì xác thực đúng, còn không phải như thế thì xác thực sai.

- Trường hợp thứ 2. Người gửi *A* tạo các khoá, dùng khoá bí mật tạo chữ ký và gởi văn bản cùng chữ ký cho người nhận *B*. Người nhận *B* dùng các khoá công khai mở chữ ký để tính *m*. Sau đó băm văn bản nhận được theo hàm băm thoả thuận trước *m'*. Nếu *m = m'* thì tính xác thực đúng, tức là xác thực được. Ngược lại không xác thực được, văn bản không đến từ người gửi. Như vậy, thuật toán chỉ đảm bảo tính xác thực, còn tính bảo mật thì không.

Từ đây ta thấy, vai trò khoá bí mật rất hạn chế. Ở trường hợp 1 chỉ khoá bí mật mới tính được *m* nhưng tính được chỉ để xác thực mà thôi. Ở trường hợp thứ 2, khoá mật không dùng để mở khoá và như vậy nó không có vai trò trong bảo mật cũng như xác thực.

Trong thuật toán RSA gốc sử dụng khi văn bản nhỏ thì khoá bí mật là vô cùng quan trọng: không có khoá bí mật không giải mã được thông điệp. Đây chính là lý do quyết định đến tính mật của hệ thống: không thể lộ khoá bí mật. Do đó, kẻ

tấn công phải tìm cách phá khoá bằng cách tìm cho được khoá bí mật sau khi chặn được thông điệp (hay chữ ký). Nhưng bài toán tìm khoá bí mật là bài toán khai căn RSA hay bài toán tìm hai số nguyên tố *p, q* từ *n* rất lớn đều là những bài toán không giải được trong thời gian thực tế. Thuật toán RSA nếu áp dụng cho văn bản lớn như ta trình bày trên thì không có tính bảo mật như thuật toán RSA gốc.

Lời cảm ơn

Nghiên cứu này được tài trợ bởi Trung tâm Nghiên cứu Ứng dụng Khoa học và Công nghệ, trường Đại học Sư phạm Kỹ thuật Hưng yên, đề tài mã số UTEHY.T002.1718.03. Tác giả chân thành cảm ơn Trung tâm, các bạn đồng nghiệp trong khoa Khoa học Cơ bản và Tạp chí Khoa học và Công nghệ của trường Đại học Sư phạm kỹ thuật Hưng Yên.

Tài liệu tham khảo

[1]. R. L. Rivest, A. Shamir, and L. M. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Commun. of the ACM*, **Vol. 21**, No. 2, 1978, pp. 120-126.

[2]. Hoàng Thị Mai, Lưu Hồng Dũng, Nguyễn Hữu Mộng, "Một dạng lược đồ chữ ký xây dựng trên bài toán phân tích số". *Kỷ yếu Hội nghị khoa học quốc gia lần thứ VIII-Nghiên cứu cơ bản và ứng dụng CNTT (FAIR 2015)*, tháng 8/2015, pp. 376-386

[3]. Hoàng Thị Mai, Lưu Hồng Dũng, Nguyễn Hữu Mộng, "Một dạng lược đồ chữ ký xây dựng trên bài toán phân tích số". *Tạp chí Nghiên cứu KHKT&CNQS*, ISSN 1859-1043, **No. 39**, 2015, pp. 75-81.

[4]. Hoàng Thị Mai, Lưu Hồng Dũng, "Một dạng lược đồ chữ ký xây dựng trên bài toán phân tích số và bài toán khai căn". *Tạp chí Khoa học và Kỹ thuật, Học viện KTQS*, ISSN 1859-0209, **No. 172**, 2015, pp. 32-41

[5]. Lưu Hồng Dũng, Nguyễn Hiếu Minh, A flexible Multisignature Scheme Using GOST R34.10-94. *Tạp chí Khoa học và Kỹ thuật (Học viện KTQS)*, 2010, **số 134 (06-2010)**, tr. 45 – 53.

[6]. Luu Hong Dung, Nguyen Hieu Minh, New Digital Multisignature Scheme with Distinguished Signing Responsibilities. *IJCSNS International Journal of Computer Science and Network Security*, January 30, 2010, **Vol.10, No.1**, pp. 51-57.

[7]. Lưu Hồng Dũng, Trần Trung Dũng, Xây dựng lược đồ đa chữ ký số tuần tự. *Tạp chí Khoa học và Kỹ thuật (Học viện KTQS)*, 2011, **số 141 (06-2011)**, tr. 5-13.

[8]. Lưu Hồng Dũng, Phát triển lược đồ đa chữ ký số trên cơ sở bài toán logarit rời rạc. *Chuyên san Các công trình nghiên cứu, phát triển và ứng dụng CNTT và TT*, tập V-1, 2011, **số 5(25) (06-2011)**, tr. 60 – 66.

[9]. Lưu Hồng Dũng, Một thiết kế mới cho các lược đồ chữ ký số. *Tạp chí Khoa học và Kỹ thuật (Học viện KTQS)*, 2011, **số 142 (08-2011)**, tr. 29-38.

[10]. Lưu Hồng Dũng, Nguyễn Thị Thu Thủy, Nghiên cứu xây dựng mô hình tổng quát cho các lược đồ CKS phân biệt trách nhiệm. *Tạp chí Khoa học và Kỹ thuật (Học viện KTQS)*, 2012, **số 146 (02-2012)**, tr. 124 – 136.

[11]. Bùi Việt Hồng, Xây dựng thuật toán xác thực bản tin bằng chữ kí số theo hệ ký RSA -PSS. *Tạp chí Nghiên cứu KHKT&CNQ,* **số 19, 6-2007**.

[12]. Lều Đức Tân, Hoàng Văn Thức, Một thuật toán sinh cặp số nguyên tố RSA mạnh p, q thoả mãn điều kiện IP-QI có ước nguyên tố lớn. *Tạp chí Nghiên cứu KHKT&CNQ,* 2007, s**ố 20, 9-2007**.

[13]. Nguyễn Ngọc Cương, Phạm Văn Tuấn, Trần Duy Hưng, Một cách chọn tham số e, d cho hệ mật RSA. *Tạp chí NC KHKT&CNQ*, 2010, **số 8, 08-2010**.

[14]. Hoàng Văn Thức, Thuật toán sinh tham số RSA an toàn. *Tạp chí NC KHKT&CNQ*, 2010, **số 5, 02-2010**.

[15]. Vũ Huy Hoàng, Hồ Thuần, Một phương pháp đơn giản xây dựng hệ RSA an toàn với số mũ giải mã lớn. *Tạp chí NC KHKT&CNQ*, 2011, **số 11, 02- 2011**.

[16]. Phạm Văn Tuấn, Các tấn công thám mã lên hệ mật RSA. *Tạp chí NC KHKT&CNQ*, 2013, **Số Đặc san ATTT 13, 05-2013**.

[17]. Hoàng Văn Thức, Bạch Nhật Hồng, Một tiêu chuẩn mới cho số mũ công khai của hệ các tiêu chuẩn tham số mới. *Tạp chí NC KHKT&CNQ*, 2009, **số 4, 08-2009**.

[18]. R. Kenneth, Elementary Number Theory and its Applications. *AT & T Bell Laboratories, 4th Edition*, ISBN:0-201-87073-8, 2000.

ISSN 2354-0575

A GENERAL DIGITAL SIGNATURE SCHEME

Abstract:

This paper presented a general scheme of digital signature. The generality of scheme is customization features of several integer functions. From the general scheme by customization features of several integer functions we can gain different practical diagrams. We also emphasize the mathematical aspects of the proposed algorithms. The correctness of the scheme is the authenticity of the received text as well as its integrity.

Keywords: *Scheme, digital signature, RSA, large prime numbers, Euler function, public key, secret key.*