Về một giải pháp nâng cao độ an toàn cho lược đồ chữ ký số trong vành hữu hạn Z_n

Nguyễn Đào Trường, Lê Văn Tuấn

***Tóm tắt*— Chữ ký số ngày càng được sử dụng rộng rãi và là yêu cầu bắt buộc đối với rất nhiều nền tảng an toàn. Bài báo đề xuất một giải pháp nâng cao độ an toàn cho lược đồ chữ ký số dựa trên bài toán logarit rời rạc trên vành hữu hạn Z_n.**

***Abstract*— The digital signature is increasingly widely used, and it is the mandatory requirement for many security platforms. The paper proposes a solution to improve the security of digital signature scheme based on the problem of discrete logarithm on finite ring Z_n.**

***Từ khóa:* chữ ký số; vành hữu hạn; logarit rời rạc.**

***Keywords*: Digital signature; finited rings; discrete logarithm.**

I. GIỚI THIỆU

Lược đồ ElGamal ([4-5]) và các biến thể của nó ([6-7]) trên trường hữu hạn Z_p không an toàn trong những tình huống lộ khóa phiên hoặc trùng khóa phiên và nguyên nhân dẫn đến mất an toàn cho các lược đồ này là công khai bậc của phần tử sinh, điều này được chỉ ra trong các kết quả nghiên cứu liên quan [8-12]. Để khắc phục những điểm tồn tại này, các nhà khoa học trong nước ([1-3], [13]) và trên thế giới đã nghiên cứu ([14-15]) và phát triển các lược đồ chữ ký số trên vành hữu hạn Z_n. Một số lý do được đưa ra như sau: *Thứ nhất,* trên vành cho phép che giấu bậc của phần tử sinh [3]; *Thứ hai,* giải bài toán logarit rời rạc trên vành Z_n ($n = p.q$, trong đó p, q là các số nguyên tố phân biệt) được cho là khó hơn giải bài toàn logarít rời rạc trên trường Z_p [3]; *Thứ ba,* cho đến nay, ngoài thuật toán Baby step - giant step của Danied Shank có thể ứng dụng để giải bài toán logarit rời rạc trên vành Z_n [16] thì các thuật toán Rho của Pollard hay thuật toán Pohlig-Hellman, chỉ có thể áp dụng để giải bài toán logarit rời rạc trên trường hữu hạn Z_p.

Bài báo có bố cục như sau: Mục II nhắc lại một số ký hiệu và định nghĩa sẽ được sử dụng trong bài. Tiếp đến Mục III sẽ đưa ra giải pháp đề xuất. Mục IV sẽ là các kết quả thực nghiệm và cuối cùng là Mục Kết luận.

Bài báo được nhận ngày 12/11/2018. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 05/12/2018 và được chấp nhận đăng vào ngày 16/12/2018. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 06/12/2018 và được chấp nhận đăng vào ngày 20/12/2018.

II. MỘT SỐ KÝ HIỆU VÀ ĐỊNH NGHĨA

A. Định nghĩa 1

Hàm H: $\{0,1\}^{\infty} \rightarrow: \{0,1\}^{512}$ chuyển một xâu có độ dài hữu hạn bất kỳ thành xâu có độ dài 512 bit (hàm H là hàm SHA512).

B. Định nghĩa 2

Hàm $Num()$ đổi một xâu nhị phân thành số nguyên không quá T bit, ký hiệu là Num: $\{0,1\}^{\infty} \rightarrow Z$. Tương ứng cặp $(T, b_0 b_1 \dots b_{H-1})$ thành số a tính theo công thức: $a = b_0 + 2^1 b_1 + \dots + 2^{min(T,H)-1} b_{min(T,H)-1}$).

C. Định nghĩa 3

Hàm $Str()$ có chức năng đổi số nguyên không âm a thành xâu nhị phân. Ký hiệu là $Str: \mathbb{Z} \geq 0 \rightarrow: \{0,1\}^{\infty}$. Giả sử ứng với số nguyên không âm a, $a = b_0 + 2.b_1 + \dots + 2^{T-1}$ thì $Str(a) = b_0 b_1 \dots b_{T-1}$.

D. Định nghĩa 4

Hàm $Random(X)$: Hàm lấy ngẫu nhiên một phần tử thuộc tập X, giả sử phần tử đó là k, ta ký hiệu $k \in_R X$.

III. GIẢI PHÁP ĐỀ XUẤT

A. Ý tưởng

Ý tưởng cơ bản của giải pháp là đề xuất một lược đồ tổng quát có độ an toàn dựa trên tính khó giải của bài toán logarit rời rạc trên vành Z_n, đồng thời phát triển một lược đồ chữ ký số cụ thể trên lược đồ cơ sở này và che giấu được bậc của phần tử sinh. Dựa trên phương pháp xây dựng ngưỡng an toàn của Arjen K. Lenstra, Eric R. Verheul [17], xây dựng công thức tính

ngưỡng an toàn và xây dựng được hệ tiêu chuẩn tham số an toàn cho lược đồ đề xuất trong lĩnh vực kinh tế - xã hội và quốc phòng, an ninh tại Việt Nam trong thời gian tới.

B. Đề xuất lược đồ chữ ký số cơ sở

Trong lược đồ cơ sở sử dụng ký hiệu $k \in_R (1,t)$ để biểu thị cho phép lấy ngẫu nhiên số nguyên k trong khoảng $(1,t)$; sử dụng hàm $Len(t)$ trả về cỡ của t tính theo bit; hai hàm số $f_1(T,r)$ và $f_2(T,r)$ với hai tham số đầu vào là thông báo cần ký, ký hiệu là T và thành phần thứ nhất của chữ ký là r.

B1. Bài toán cơ sở

Lược đồ chữ ký số cơ sở có độ an toàn dựa trên tính khó giải của bài toán logarit rời rạc trên vành hữu hạn Z_n, trong đó n là tích của hai số nguyên tố lớn, phân biệt.

B2. Miền tham số

Miền tham số của lược đồ chữ ký số trên vành Z_n, gồm có số modul n là cỡ của vành Z_n, phần tử sinh g có cấp là một hợp số, ký hiệu là t. Dựa trên một số cơ sở toán học giới thiệu trong [3], miền tham số cho lược đồ chữ ký số tổng quát được xây dựng như sau:

+ Số modul $n = p.q$ với p, q là số nguyên tố lớn. Giá trị $t = p_1.q_1$ với p_1, q_1 là các nguyên tố thỏa mãn điều kiện sau: $p_1|(p-1), q_1|(q-1), p_1 \nmid (q-1), q_1 \nmid (p-1)$.

+ Giá trị N là cỡ của t, ký hiệu $N = Len(t)$.

+ g là phần tử sinh của nhóm $< g >$ có cấp t trong modul n.

+ Giá trị x là khóa riêng phải được giữ bí mật; x được chọn ngẫu nhiên trong đoạn $(1, t-1]$ sao cho tồn tại x^{-1} trong Z_t.

+ Giá trị y là khóa công khai, với $y = g^x \bmod n$.

+ Bộ giá trị (n, g, x, t) là khóa bí mật và (n, g, y, N) là khóa công khai.

B3. Thuật toán sinh chữ ký số

Input: tham số khóa bí mật (n, g, x, t) và thông báo cần ký T.

Output: (r, s).

1. $k \in_R (1, t)$.
2. $r \leftarrow g^k \bmod n$.
3. Tạo s: $s \leftarrow x^{-1}[kf_1(T,r) - f_2(T,r)] \bmod t$
4. return (r, s).

B4. Thuật toán xác nhận chữ ký số

Input: $T, (r, s), (n, g, y, N)$

Output: "*accept*" hoặc "*reject*".

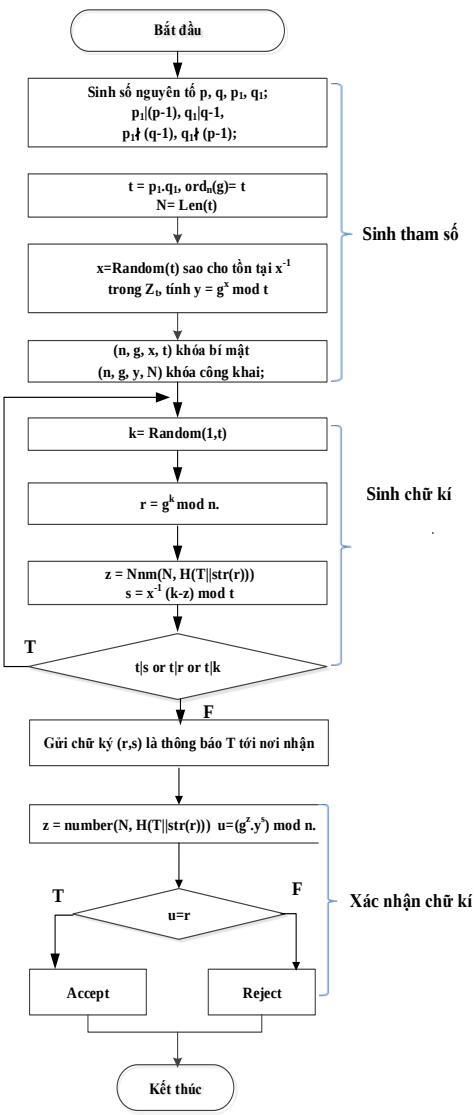
1. $u \leftarrow (g^{f_2(T,r)}.y^s) \bmod n$
2. if $(u = r^{f_1(T,r)})$ return "*accept*" else return "*reject*".

B5. Tính đúng đắn của lược đồ:

Dễ thấy: $u = (g^{f_2(T,r)}.y^s) \bmod n = g^{f_2(T,r)}.g^{x.x^{-1}.k.(f_1(T,r)-f_2(T,r))} \bmod n$

$= g^{k.f_1(T,r)} \bmod n = r^{f_1(T,r)}$

C. Đề xuất lược đồ chữ ký số mới trên vành Z_n



Hình 1. Lưu đồ thuật toán lược đồ chữ ký

Dựa trên lược đồ chữ ký số cơ sở, chọn hàm $f_1(T,r) = 1;\quad f_2(T,r) = Num(H(T,Str(r)))$, khi đó thuật toán ký và xác nhận chữ ký của lược đồ chữ ký đề xuất như Hình 1.

C1. Thuật toán sinh chữ ký

Input: (*n, t, g, x*), x^{-1}, $T \in \{0,1\}^*$.

Output: *(r,s).*

1. $k \in_R (1,t)$.
2. $r \leftarrow g^k \bmod n$.
3. $z \leftarrow Num(N, H(T||Str(r)))$
4. $s \leftarrow x^{-1}(k-z) \bmod t$.
5. if $((s=0)\ or\ (t|r))$ then goto 1.
6. return *(r, s).*

C2. Thuật toán xác nhận chữ ký

Input: Thông báo *T* và chữ ký (*r, s*), khóa công khai (*n, N, g, y*).

Output: "*accept*" hoặc "*reject*".

1. $z \leftarrow Num(N, H(T||Str(r)))$.
2. $u \leftarrow g^z . y^s \bmod n$
3. if $(r = u)$ return "*accept*" else return "*reject*".

C3. Tính đúng đắn của thuật toán

Ta có

$$u = g^z . y^s \bmod n$$
$$= g^z . g^{x(x^{-1}k - x^{-1}z) \bmod t} \bmod n$$
$$= g^z . g^{k-z} \bmod n = g^k \bmod n = r.$$

C4. Mức độ an toàn của lược đồ đề xuất

Tấn công khóa bí mật (total break):

Tấn công khóa bí mật là kiểu tấn công có mục tiêu cao nhất nhằm giành lấy cặp khóa bí mật là cặp tham số (*t, x*), khi đó kẻ tấn công có vai trò như người ký hợp lệ. Với khả năng của kẻ tấn công chỉ có khóa công khai trong tay (only key attack), để tính được khóa bí mật x, kẻ tấn công phải giải được bài toán logarit rời rạc trên vành Z_n, để tính được t (t là bậc của phần tử sinh), kẻ tấn công phải giải bài toán tìm bậc của phần tử sinh trong vành Z_n. Bài toán DLP_n và bài toán tìm bậc của phần tử sinh trong Z_n là hai bài toán khó nếu tham số của bài toán được chọn theo một hệ tiêu chuẩn an toàn. Khi tham số t được giữ bí mật, nếu tình huống trùng khóa phiên hoặc lộ khóa phiên xảy ra thì kẻ tấn công cũng khó có thể tính được khóa bí mật. Dưới đây xét hai trường hợp trùng khóa phiên và lộ khóa phiên.

+ Trường hợp thứ nhất: Khóa phiên bị lộ, khi đó khóa bí mật x sẽ được xác định bởi công thức sau đây:

$$s \leftarrow x^{-1}.(k - z) \bmod t.$$
$$\rightarrow x^{-1} \leftarrow (k-z)^{-1} \bmod t.$$

Do t được giữ bí mật nên kẻ tấn công khó có thể xác định được x^{-1} và khóa bí mật x.

+ Trường hợp thứ hai: Khóa phiên bị dùng trùng lặp, giả sử thông báo *T* và *T'* dùng cùng một khóa phiên, khi đó khóa bí mật x sẽ được xác định bởi công thức sau:

$$z \leftarrow Num(N, H(T||str(r)))$$
$$z' \leftarrow Num\ (N, H(T'||str(r)))$$
$$s \leftarrow x^{-1}.(k-z) \bmod t$$
$$s' \leftarrow x^{-1}.(k-z') \bmod t$$
$$x^{-1} = (s-s').(z'-z)^{-1} \bmod t$$

Do t được giữ bí mật nên không thể xác định được x^{-1} trong Z_t

Tấn công giả mạo chữ ký

Mục đích của kẻ tấn công giả mạo là tạo ra chữ ký hợp lệ (r,s) cho lớp thông báo T chưa từng được ký bởi người ký hợp lệ, hoặc tạo ra chữ ký thứ hai (r,s) cho một thông báo T đã được ký bởi người ký hợp lệ trước đó mà trong tay không có công cụ để ký (khóa bí mật)… Khi đó kẻ tấn công phải tìm được cặp (r,s) thỏa mãn phương trình sau:

$$r = g^{\mathrm{Num(N,H(T||Str}(g^k \bmod n)))} . y^s \bmod n$$

Do mỗi chữ ký (r,s) của một thông báo T nào đó được sinh ra trên một bộ tham số riêng, được kiểm soát giá trị (Bước 5 của thuật toán sinh chữ ký trong phần C1 không cho phép vi phạm tính chất $t|s, t|r, t|k$) và khóa phiên k có tính ngẫu nhiên nên các chữ ký đều có tính độc lập nhau. Vậy, lược đồ đề xuất an toàn với các kiểu tấn công giả mạo *Selective forgery* và *Existential forgery* kể cả khi kẻ tấn công có khả năng thực hiện các kiểu tấn công *known-message attack*, *chosen-message attack* và khả năng cao nhất là *adaptive chosen-message attack*.

Nói tóm lại, lược đồ đề xuất là an toàn với mô hình tấn công *existentially unforgeable under adaptively chosen-message attacks*, tức là với khả năng cao nhất mà kẻ tấn

công có *adaptive chosen-message attack* cũng không thực hiện được hành vi giả mạo với mục đích yếu nhất *Existential forgery*.

C5. Tính hiệu quả

Để thuận tiện cho đánh giá độ phức tạp tính toán, trong bài báo sẽ sử dụng M_L là độ phức tạp tính toán của phép nhân hai số trong modul n có $len(n) = L$ và ký hiệu M_N là độ phức tạp tính toán của phép nhân hai số trong modulo t, $len(t) = N$ bit.

Không gian lưu trữ:

Đối với các lược đồ chữ ký số đề xuất, mỗi thành viên thực hiện một phiên ký bắt buộc phải sử dụng một số modul riêng (tránh tấn công sử dụng modul chung), nên tham số hệ thống của các lược đồ chữ ký số này yêu cầu không gian lưu trữ gấp k (số người dùng trong hệ thống) lần so với yêu cầu về không gian lữu trữ trong các lược đồ chữ ký Elgamal, DSA và GOST. Hơn nữa, trong lược đồ chữ ký số DSA và GOST, thành phần r trong mỗi chữ ký là $N = len(q)$ (bit) trong khi đó thành phần r trong lược đồ đề xuất là $L = len(n)$ (bit), vậy là giá trị r của lược đồ đề xuất lớn hơn $\frac{L}{N}$ lần thành phần r trong lược đồ DSA và GOST.

Độ phức tạp tính toán:

Trong thuật toán ở phần C1, độ phức tạp thuật toán tập trung ở phép lũy thừa $r \leftarrow g^k \bmod n$, do $n = p.q$. Phép tính nghịch đảo $x^{-1} \bmod t$ được tính trước, nên ta có ước lượng thuật toán C1 như sau:

$$C_G \approx N.M_L + 2.M_N$$

Trong thuật toán ở phần C2, độ phức tạp thuật toán tập trung ở phép lũy thừa $t \leftarrow g^z.y^s \bmod n$; nên độ phức tạp của nó được ước lượng như sau:

$$C_V \approx N.M_L + M_N$$

Tóm lại: Lược đồ chữ ký số do chúng tôi đề xuất trong bài báo này sẽ yêu cầu không gian lưu trữ lớn hơn nhiều so với lược đồ chữ ký số Elgamal cùng các biến thể do mỗi thành viên trong hệ thống phải sử dụng số modul n riêng.

IV. THỬ NGHIỆM

Do khuôn khổ bài báo giới hạn nên khi thực nghiệm hệ thống phải sử dụng số modul n riêng, không gian lưu trữ lớn hơn nhiều so với lược đồ chữ ký số Elgamal cùng các biến n modul chung, nên chúng ta chỉ thực nghiệm xem thời gian chi phí sinh chữ ký so với một số lược đồ như DSA, Elgamal, RSA có đạt được hiệu quả hơn hay không. Chương trình thử nghiệm được viết bằng ngôn ngữ lập trình C++, được biên dịch bởi trình QT Creater và chạy trên hệ điều hành Window 7, bộ vi xử lý Core2 Duo 2.2 GHz, bộ nhớ 2G. Thử nghiệm sử dụng hàm băm SHA-512, giá trị băm của thông báo T là $M = H(T)$, giá trị M như sau:

M=59435B969EDE967538BADAF898EBB
A0B250D8D38C470831258EFC998C0AAB66
369BD84E1267F73DA44F54050F8E52039DC
3A0751550F0EC64458B094759D62AD

Tham số lược đồ chữ ký 01 sử dụng cho thử nghiệm như sau:

p=61172327492847069472032393719205726809135813743440799050195397570919697796091958321786863938157971792315844506873509046544459008355036150650333616890210625686064472971480622053108940024094506365700177916771190231358376137402779126675885239873863251419404875209354656290800835004059168637746666774988258648861433470364994278050623023052217454165708 3 (1152 bit)

q=42820629244992948630422675603444008766395069620408559335136778299643788457264370825250804756710580260672400007913220887956202404789698632325276676609948920239411118062419554619666051666393046202958794101132407478728356803474002085173829809743690066848239545149077325694394768007216975371594389303204322985544672631665200086624759308888712641189831 (1152 bit)

p_1=15905342063447565410024733613622675177827513271326161374945890013417660256638878157031 7 (287 bit)

q_1=41069112802488437218699642801105043081818400392119678577960763040677317218001047784921426885345550680529038529141 (375 bit)

n=$p.q$=26194375556244934026575998414768257214581501764693031085430809106003433781353981158275471151007503104338635765529637648387595679957492521915655530093656040558194802999942099286018101457875717847699989586646996169457006 4

866175517867708514536336533621838566002407821447981342971092156016188050836634833745551784760910605275367624994988473559263161471237752302430273327416831171293670916407366537944941448734232947605764487479903531748721880414425677330866678184127197408381031095038406655734682046017843032621509997606598832522747842422157721670076921026427294679915384762628705618775216583803054814986819652608719884471791934456223571574294935048434003686179154837109997575283084966470350872297 (2304 bit)

$t=p_1$. q_1=653218287365892265876515932799420561468453284243676831154063202757450614868044399278487245777380303065770717319419597871641829909476928486730869542446400108001210859733238775539835397148363394510769 7 (661 bit)

g=252028254026346034600227052024388120486039468456693874563365740722521693493144328527354271576469002992976325568864348734730446056510241575193634327059730915513327865613043291489880997495483188980647261222611365157535264216700421532347759924401547022719794905527951935312139105422441423401994341121540871525213550911048480306685908974988780974831681795165059387253550113667121278144395636273120601458487226672742417070458791625262570782059378416011046777258852823686463049657224087926953125682433633683948395123478891856189038173722472466114632420610687597594686642496693697439071578599392132177762571552323974590326354048445001531546552066590932696281768605290486274909088760689163691467097204 (2304 bit)

Khóa bí mật x:

x=287388522792493159516358366964518687889410202247967216946698630443721560262889742384506051310803400049525197506289991005813142317625328753591750679944730273021630863781189381944105410334 03 (623 bit)

Khóa công khai y:

y=178611317356058133513470494721377543693353406457329622723310029589601293799230425135704851989053538609095571280887770182955466579932865987917791569565155400131309052649050435648953508804659479712944584102052825834941115544882017394661700966437918163392639362048127006161889414675309427240847472351441063280022613274175541721402354072020111694548556239002590973553350136796555354618556833237788316343893133402137613985074073776150429853715353756592258518087522732995618055797161719942669476038673560328008717643816560448187310619097324279879770976332811839424818852006167800325869251779527254579421887694369995547000408242133633111059289607714048431287880853486113316396438391013858859060810120 29 (2303 bit)

- Sinh chữ ký

+ Giá trị khóa phiên k như sau:

k =377871905155383211952717155097304331035357277840432511992974164694989571531164619310742644776903562177008037362105418985075795250840981311046771 (477 bit).

+ Kết quả sinh chữ ký cho thông báo T như sau:

r=181164173128114944600538674408880220254066915925288666650616443371356073778217956148006360942725997218158833508181070235508025102947589094228743127351792065304742162819243990086959108149672379682741662442816925076624119720258745636844135765229318843515726410799895003148184692198628335634419641557271424141713008132855579908247339107255976943885327666260413232587231609782866838261558764528550987031952370852574444365637757284374295066451055600049176031006587327815792516241018809601654486671038908233819076793550278713061881964539679786878335130991036127344340959672276409589718048803766955713880539331969748796578080193063372776048753970558808238630337968388027053693321188037261468764051187 0 (2303 bit)

$r\ mod\ t$ =312815172992117955392683286908933952349855102207890851099862681908998364401798235871231067215604691825141679300465391071584757555465905539231247 8≠0

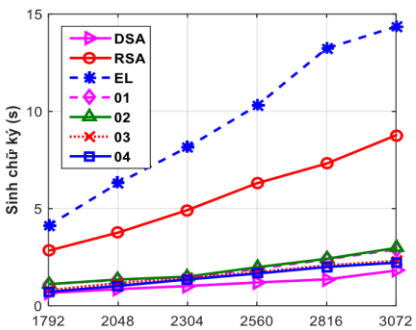
s=3024215778480216932713971159831054881097257949435493832353709720148481052109237609270575091395332233870615686390463487811279493656778139168236429232144808680722104760626689575384665769712871192574824 (660 bit).

BẢNG 1. THỜI GIAN SINH CHỮ KÝ

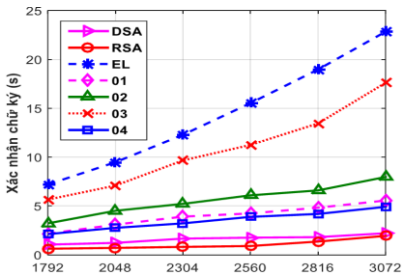
Kích thước Modulus (bit)	Thời gian sinh chữ ký						
	DSA	RSA	EL	01	02	03	04
1792	0.656	2.830	4.123	1.1060	1.108	0.800	0.712
2048	0.856	3.760	6.300	1.3325	1.348	1.162	1.016
2304	1.013	4.918	8.151	1.4590	1.495	1.425	1.352
2560	1.196	6.300	10.29	1.8980	1.980	1.725	1.657
2816	1.356	7.309	13.23	2.3870	2.414	2.076	1.992
3072	1.810	8.762	14.35	2.8960	2.971	2.302	2.216

BẢNG 2. THỜI GIAN XÁC NHẬN CHỮ KÝ

Kích thước Modulus (bit)	Thời gian xác nhận chữ ký						
	DSA	RSA	EL	01	02	03	04
1792	1.057	**0.636**	**7.213**	**2.179**	**3.234**	**5.666**	**2.130**
2048	1.234	0.723	9.490	3.102	4.523	7.102	2.776
2304	1.672	0.826	12.30	3.923	5.23	9.676	3.234
2560	1.768	0.914	15.54	4.251	6.102	11.263	3.899
2816	1.823	1.370	18.98	4.837	6.607	13.46	4.198
3072	2.223	1.950	22.85	5.572	7.978	17.62	4.923



Hình 2. So sánh thời gian sinh chữ ký



Hình 3. So sánh thời gian xác nhận chữ ký

V. KẾT LUẬN

Bài báo đã đề xuất giải pháp nâng cao độ an toàn cho lược đồ chữ ký số trên vành hữu hạn Z_n, trong đó đề xuất một lược đồ chữ ký số cơ sở trên vành hữu hạn $Z_n$và đã phát triển một lược đồ chữ ký số cụ thể trên lược đồ cơ sở này. Lược đồ đề xuất khắc phục được một số nhược điểm của lược đồ chữ ký số Elgamal và biến thể của nó, đặc biệt là khắc phục được sự mất an toàn trong tình huống lộ khóa phiên hoặc trùng khóa phiên. Hơn nữa, bài báo đã chỉ ra một số điểm tồn tại trên các lược đồ chữ ký số trong vành Z_n của một số nhà khoa học [1-3], [13-15] chưa xây dựng được cơ sở toán học cho các tham số trong lược đồ của mình; chưa xây dựng được công thức tính ngưỡng an toàn và hệ tiêu chuẩn cho các tham số an toàn....

TÀI LIỆU THAM KHẢO

[1]. Phạm Văn Hiệp, Nguyễn Hữu Mộng, Lưu Hồng Dũng, "Một thuật toán chữ ký xây dựng trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc", Tạp chí KH và CN, Đại học Đà nẵng, 2018.

[2]. Lê Văn Tuấn, Bùi Thế Truyền, Lều Đức Tân, "Phát triển lược đồ chữ ký số mới có độ an toàn dựa trên bài toán logarit rời rạc trên vành Z_n", Tạp chí KHCN Thông tin và Truyền thông, Học viện CNBCVT, 10- 2018.

[3]. Vũ Long Vân, Hồ Ngọc Duy, Nguyễn Kim Tuấn, Nguyễn Thị Thu Thủy, "Giải pháp nâng cao độ an toàn cho lược đồ chữ ký số", SOIS Tp HCM, 12 - 2017.

[4]. T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", IEEE Transaction on Information Theory, IT-31(4); pp.469-472, 1985.

[5]. W. C. Kuo, "On ElGamal Signature Scheme, Future Generation Communication and Networking" (FGCN 2007), Jeju, pp. 151-153.

[6]. C. P. Schnorr, "Efficient signaturegeneration for smartcards", Journal of Cryptology Vol. 4, pp. 161-174, 1991.

[7]. B. Yang, "A DSA-Based and Efficient Scheme for Preventing IP Prefix Hijacking", International Conference on Management of e-Commerce and e-Government, Shanghai, pp. 87-92, 2014.

[8]. J.m.Liu, X.g.Cheng, and X.m.Wang, "Methods to forge elgamal signatures and determine secret key", in Advanced Information Networking and

Applications, AINA 2006 20th International Conferenceon, vol.1.IEEE, pp. 859–862, 2006.

[9]. L. Xiao-fei, S. Xuan-jing and C. Hai-peng, "An Improved ElGamal Digital Signature Algorithm Based on Adding a Random Number, Second International Conference on Networks Security, Wireless Communications and Trusted Computing", Wuhan, Hubei, pp. 236-240, 2010.

[10].C. Y. Lu, W. C. Yang and C. S. Laih, "Efficient Modular Exponentiation Resistant to Simple Power Analysis in DSA-Like Systems, International Conference on Broadband, Wireless Computing, communication and Applications", Fukuoka, pp. 401-406, 2010.

[11].H. Zhang, R. Li, L. Li and Y. Dong, "Improved speed Digital Signature Algorithm based on modular inverse,Proceedings of 2013 2nd International Conference on Measurement, Information and Control", Harbin, pp. 706-710, 2013.

[12].Z. Ping, W. Tao and C. Hao, "Research on L3 Cache Timing Attack against DSA Adopting Square-and-Multiply Algorithm", Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, pp. 1390-1393, 2015.

[13].Lê Văn Tuấn, Bùi Thế Truyền, Lều Đức Tân, "Contructing the digital signature besed on the discrete logaríthmic problem", The research journal of military science and technology, No 51ª, ISSN 1859 – 1043, pp 44-56,11- 2017.

[14].S. K. Tripathi and B. Gupta, "An efficient digital signature scheme by using integer factorization and discrete logaríthm problem", International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, pp. 1261-1266, 2017.

[15].Chik How Tan, Xun Yi and Chee Kheong Siew, "Signature scheme based on composite discrete logarithm", Fourth International Conference on Information, Communications and Signal Processing, pp. 1702-1706, 2003.

[16].Lê Văn Tuấn, Bùi Thế Truyền, "Phát triển thuật toán của SHANK giải bài toán logarít rời rạc trên vành Z_n",Tạp chí Nghiên cứu KH & CNQS số 48, 4- 2017.

[17].Arjen K. Lenstra, Eric R. Verheul, Selecting Cryptographic Key Sizes, Springer-Verlag Berlin Heidelberger, pp. 446-465, 2000.

SƠ LƯỢC VỀ TÁC GIẢ

TS. Nguyễn Đào Trường

Đơn vị công tác: Học viện KTMM, Ban Cơ yếu Chính phủ.

Email: truongnguyendao@gmail.com

Quá trình đào tạo: Nhận bằng Kỹ sư Kỹ thuật mật mã và Kỹ sư tin học năm 2001, nhận bằng Thạc sĩ Công nghệ thông tin năm 2010, nhận học vị Tiến sĩ Cơ sở toán học cho tin học năm 2018.

Hướng nghiên cứu hiện nay: An toàn và bảo mật mạng máy tính, An toàn mạng IoT.

ThS. Lê Văn Tuấn

Đơn vị công tác: Học viện Khoa học quân sự, Bộ quốc phòng. Email: levantuan71@yahoo.com

Quá trình đào tạo: Nhận bằng cử nhân toán năm 1992, và Công nghệ thông tin năm 2000, nhận bằng thạc sĩ công nghệ thông tin năm 2007.

Hướng nghiên cứu hiện nay: mật mã khóa công khai, chữ ký số, định danh và xác thực.