A New Construction Method of Digital Signature Algorithms

Thuy Nguyen Đuc[†] and Dung Luu Hong[††]

[†] Faculty of Information Technology, Ho Chi Minh City Technical and Economic College
[††] Faculty of Information Technology, Military Technical Academy

Summary
The article presents a new construction method of digital signature algorithms based on difficulty of the discrete logarithm problem. From the proposed method, the different signature schemes can be deployed to choose suitably for applications in practice.

Key words:
Digital signature; Digital signature algorithm; Discrete logarithm problem.

1. Problem

Currently, the digital signature has been widely applied to the fields of e-Government, e-Commerce, ... in the world and has been initially deployed applications in Vietnam to meet the authentication requirements for the origin and the integrity of information in electronic transactions. However, the initiative research - development of new digital signature schemes to meet the requirements for product, safety equipment design - manufacture and information security in the country has always been essential problem arising. In the country, a number of research results in this field have been published [1], [2], [3], [4] and implemented in practical applications.

In this article, the authors propose a new construction method of signature schemes based on difficulty of the discrete logarithm problem in the field of finite elements. As well as methods that have been proposed in [1], [2], [3], [4], an advantages of the newly proposed method here is that it can be used for the purpose of developing different digital signature schemes to choose suitably to the requirements of applications in practice.

2. Construction of digital signature algorithm

2.1 Construction method

This newly proposed sheme is built up based on difficulty of the Discrete Logarithm Problem [5]. Discrete logarithm problem – DLP(g,p) can be stated as follows: Let p be prime number, r is the birth particle of the group $\mathbb{Z}p^*$. For each positive integer $y \in \mathbb{Z}p^*$, find x satisfying the equation:

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

Here, the discrete logarithm problem is used as a one-way function in formation of the key of entities in the same system with the common parameter set {p,g}. It is easy to see that, if x is a secret parameter, calculation of the public parameter y from x and systematic parameters {p,g} is absolutely easy. However, the opposite is very difficult to implement, ie from y and {p,g}, the calculation of the secret parameter x is unfeasible in practical applications. It should be noted that, according to [6] and [7] in order for discrete logarithm problem to be difficult, p selected must be large enough with: $|p| \geq 512$ bit.

Algorithm for the problem DLP(g,p) can be written as a function calculating algorithm DLP(g,p)(.) with the input variable y and function value is the root x of the equation:

$$x = DLP_{(g,p)}(y)$$

This signature scheme built up based on the newly proposed method allows entities signing in the same system to share the parameter set {g,p}, where each member U of the system chooses oneself the secret key x satisfying: $1 < x < (p-1)$, calculate and disclosure the parameter:

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

It also should be noted that the secret parameter x must be chosen so that the calculation of DLP(g,p) (y) is difficult. With the above stated choice, only the signer U knows the value of x, so the person who knows x is enough to authenticate is U.

Assuming that the secret key of the signer x is randomized in the range (1,p) and the corresponding public key y is formed from x in accordance with:

$$y = g^x \bmod p \qquad (1.1)$$

Here, p is the chosen prime number so that solution of the problem DLP(g,p) (y) is difficult, g is the birth particle of the group $\mathbb{Z}p^*$ has the degree of q, with q|(p-1).

Assume that (r,s) is the signature on the message M, u is one value in the range (1,q) and r is calculated from u by the formula:

$$r = g^u \bmod p \qquad (1.2)$$

And s calculated from v by the formula:

$$s = g^v \bmod p \qquad (1.3)$$

Here: v is also one value in the range (1,q).

Also assume that the verifying equation of the scheme is formed:

Manuscript received December 5, 2016
Manuscript revised December 20, 2016

$$s^{f_1(M,f(r,s))} \equiv r^{f_2(M,f(r,s))} \times y^{f_3(M,f(r,s))} \bmod p$$

With $f(r,s)$ is the function of r and s. Consider the case:

$$f(r,s) = r \times s \bmod p = g^k \bmod p \quad (1.4)$$

Where k is a randomly chosen value in the range (1,q). Set:

$$g^k \bmod p = Z \quad (1.5)$$

Then, the verifying equation can be taken to the form:

$$s^{f_1(M,Z)} \equiv r^{f_2(M,Z)} \times y^{f_3(M,Z)} \bmod p \quad (1.6)$$

From (1.1), (1.2), (1.3) and (1.6) we have:

$$g^{v.f_1(M,Z)} \equiv g^{u.f_2(M,Z)} \times g^{x.f_3(M,Z)} \bmod p \quad (1.7)$$

From (1.7) infer:

$$v \times f_1(M,Z) \equiv [u \times f_2(M,Z) + x \times f_3(M,Z)] \bmod q \quad (1.8)$$

So:

$$v = (u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z) \bmod q \quad (1.9)$$

On the other hand, from (1.2), (1.3) and (1.4) we have:

$$(v+u) \bmod q = k \quad (1.10)$$

From (1.9) and (1.10) we have:

$$[u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z) + u] \bmod q = k$$

Or:

$$[u \times (f_1(M,Z)^{-1} \times f_2(M,Z) + 1) + x \times f_1(M,Z)^{-1} \times f_3(M,Z)] \bmod q = k \quad (1.11)$$

From (1.11), infer:

$$u = [(f_1(M,Z)^{-1} \times f_2(M,Z) + 1)^{-1} \times (k - x \times f_1(M,Z)^{-1} \times f_3(M,Z)] \bmod q \quad (1.12)$$

From (1.12), the first component of signature is calculated by (1.2):

$$r = g^u \bmod p$$

and the second component is calculated by (1.3):

$$s = g^v \bmod p$$

with v calculated by (1.9):

$$v = [u \times f_1(M,Z)^{-1} \times f_2(M,Z) + x \times f_1(M,Z)^{-1} \times f_3(M,Z)] \bmod q$$

From here, a form of signature scheme corresponding to the case: $f(r,s) = r \times s \bmod p = g^k \bmod p$ is shown as Table 1, Table 2 and Table 3 below.

Table 1. Algorithm for formation parameter and key

Input: p, q, x. Output: g, y.
[1]. select h: 1<h<p
[2]. $g \leftarrow h^{(p-1)/q} \bmod p$
[3]. if (g = 1) then go to [1]
[4]. $y \leftarrow g^x \bmod p$
[5]. return {g,y}

Remarks:

(i) p,q: primes satisfying conditions: $p = N \times q + 1$, N=1,2,3,….

(ii) x,y: secret, public keys of signing object U.

Table 2. Algorithm for formation of signature

Input: p, q, g, x, M. Output: (r,s).
[1]. select k: *1<k<q*
[2]. $Z \leftarrow g^k \bmod p$
[3]. $w_1 \leftarrow f_1(M,Z)$
[4]. $w_2 \leftarrow f_2(M,Z)$
[5]. $w_3 \leftarrow f_3(M,Z)$
[6]. $w_4 \leftarrow (w_1)^{-1} \times w_2 \bmod q$
[7]. $w_5 \leftarrow (w_1)^{-1} \times w_3 \bmod q$
[8]. $u \leftarrow (w_4+1)^{-1} \times (k - x \times w_5) \bmod q$
[9]. $r \leftarrow g^u \bmod p$
[10]. $v \leftarrow (u \times w_4 + x \times w_5) \bmod q$
[11]. $s \leftarrow g^v \bmod p$
[12]. return (r,s)

Remarks:

(i) M: the message to be signed, with: $M \in \{0,1\}^\infty$.

(ii) (r,s): signature of U on M.

Table 3. Algorithm for verifying signature

Input: p, q, g, y, {M,(r,s)}. Output: *true* / *false*.
[1]. $Z \leftarrow f(r,s)$
[2]. $w_1 \leftarrow f_1(M,Z)$
[3]. $w_2 \leftarrow f_2(M,Z)$
[4]. $w_3 \leftarrow f_3(M,Z)$
[5]. $A \leftarrow s^{w_1} \bmod p$
[6]. $B \leftarrow r^{w_2} \times y^{w_3} \bmod p$
[7]. if (*A=B*) then {return *true*} else {return *false*}

Remarks:

(i) M, (r,s): the messages, signature need verifying.

(ii) If the return is true, the integrity and origin of M are confirmed. Conversely, if the return is false, M is denied the origin and integrity.

It should be noted that the signature created here is not necessarily the pair of (r,s). From the Table 2 shows that the value v can be selected as the second component of the signature instead of s, thus reduce one calculation step in the procedure for formation of signature. Indeed, if the hypothesis of the verifying equation of the scheme is formed:

$$g^{v.f_1(M,f(r,v))} \equiv r^{f_2(M,f(r,v))} \times y^{f_3(M,f(r,v))} \bmod p \qquad (1.13)$$

and:

$$f(r,v) = r \times g^v \bmod p = g^k \bmod p \qquad (1.14)$$

Set:

$$g^k \bmod p = Z$$

Then, from (1.1), (1.2) and (1.13) we also have:

$$g^{v.f_1(M,f(r,v))} \equiv g^{u.f_2(M,f(r,v))} \times g^{x.f_3(M,f(r,v))} \bmod p$$

From here, algorithms for formation and verifying signature of the form of the scheme corresponding to new assumptions given in Table 4 and Table 5 as follows:

Table 4. Algorithm for formation of signature

Input: p, q, g, x, M. Output: (r,v).
[1]. select k: $1<k<q$
[2]. $Z \leftarrow g^k \bmod p$
[3]. $w_1 \leftarrow f_1(M,Z)$
[4]. $w_2 \leftarrow f_2(M,Z)$
[5]. $w_3 \leftarrow f_3(M,Z)$
[6]. $w_4 \leftarrow (w_1)^{-1} \times w_2 \bmod q$
[7]. $w_5 \leftarrow (w_1)^{-1} \times w_3 \bmod q$
[8]. $u \leftarrow (w_4+1)^{-1} \times (k - x \times w_5) \bmod q$
[9]. $r \leftarrow g^u \bmod p$
[10]. $v \leftarrow (u \times w_4 + x \times w_5) \bmod q$
[11]. return (r,v)

Table 5. Algorithm for verifying signature

Input: p, q, g, y, {M,(r,v)}. Output: *true* / *false*.
[1]. $Z \leftarrow f(r,v)$
[2]. $w_1 \leftarrow f_1(M,Z)$
[3]. $w_2 \leftarrow f_2(M,Z)$
[4]. $w_3 \leftarrow f_3(M,Z)$
[5]. $A \leftarrow g^{v.w_1} \bmod p$
[6]. $B \leftarrow r^{w_2} \times y^{w_3} \bmod p$
[7]. if ($A = B$) then {return *true* } else {return *false* }

2.2 Several algorithms for signature built up under the proposed method

2.2.1 The first scheme

a) *Structure and operation*

The first signature scheme proposed here - symbols LD 16.9–01, is built up under Table 1, 2 and 3 in section A with selections: $f_1(M,Z) = H(M)$, $f_2(M,Z) = Z$, $f_3(M,Z) = H(M)$. Algorithms for formation of parameter and key, algorithm for signature and verifying signature of the scheme are described in the Table 6, Table 7 and Table 8 below.

Table 6. Algorithm for formation of parameter and key

Input: p, q, x. Output: g, y, H(.).	
[1]. select h: $1<h<p$	
[2]. $g \leftarrow h^{(p-1)/q} \bmod p$	
[3]. if (g = 1) then goto [1]	
[4] $y \leftarrow g^x \bmod p$.	(2.1)
[5]. select $H: \{0,1\}^* \mapsto Z_n$, $q < n < p$	
[6]. return {g,y,H(.)}	

Remarks:

- H(.): Hash function (SHA, MD5, ...).

Table 7. Algorithm for signing messages

Input: p, q, g, H(.), x, M . Output: (r,s).	
[1]. $E = H(M)$	
[2]. select k: $1<k<q$	
[3] $Z \leftarrow g^k \bmod p$	(2.2)
[4]. $u \leftarrow (E^{-1} \times Z + 1)^{-1} \times (k - x) \bmod q$	
[5]. $r \leftarrow g^u \bmod p$	(2.3)
[6]. $v \leftarrow (u \times E^{-1} \times Z + x) \bmod q$	(2.4)
[7]. $s \leftarrow g^v \bmod p$	(2.5)
[8]. return (r,s)	

Table 8. Algorithm for verifying signature

Input: p, q, g, H(.), y, M, (r,s). Output: *true* / *false*.	
[1]. $E = H(M)$	
[2]. $A \leftarrow s^E \bmod p$	(2.6)
[3]. $w \leftarrow r \times s \bmod p$	(2.7)
[4]. $B \leftarrow r^w \times y^E \bmod p$	(2.8)
[5]. if ($A = B$) then {return *true* } else {return *false* }	

b) *Correctness of the scheme LD 16.9-01*

The thing to be proved is: Let p, q are 2 primes with q|(p-1), $H: \{0,1\}^* \mapsto Z_n$, $q < n < p$, $1 < k, x < q$,

$y = g^x \bmod p$, $E = H(M)$, $Z = g^k \bmod p$, $u = (E^{-1} \times Z + 1)^{-1} \times (k - x) \bmod q$, $r = g^u \bmod p$, $s = (u \times E^{-1} \times Z + x) \bmod q$. If: $w = r \times s \bmod p$, $A = s^E \bmod p$, $B = r^w \times y^E \bmod p$ then: $A = B$.

Correctness of the newly proposed scheme is proved as follows:

From (2.4), (2.5) and (2.6) we have:

$$\begin{aligned} A &= s^E \bmod p \\ &= g^{v.E} \bmod p \\ &= g^{(u.E^{-1}.Z+x).E} \bmod p \\ &= g^{u.Z+x.E} \bmod p \end{aligned} \quad (2.9)$$

From (2.1), (2.3), (2.7) and (2.8) we also have:

$$\begin{aligned} B &= r^w \times y^E \bmod p \\ &= g^{u.(r.s \bmod p)} \times g^{x.E} \bmod p \\ &= g^{u.Z} \times g^{x.E} \bmod p \\ &= g^{u.Z+x.E} \end{aligned} \quad (2.10)$$

From (2.9) and (2.10) infer the thing to be proved: $A = B$

Safety level of the scheme LD 16.9-01

In form of the newly proposed scheme, the public key is formed from the secret key based on difficulty of the discrete logarithm problem DLP(g,p). Therefore, if the parameters {p,q,g} is selected for the problem DLP(g,p) to be difficult, the safety level of the newly proposed scheme in terms of resistance to attacks disclosing secret key will be assessed by the level of difficulty of the problem DLP(g,p). It should be noted that, in order for DLP(g,p) to be difficult, the parameters {p,q,g,n} can be selected similarly to DSA [6] or GOST R34.10-94 [7], with: $|p| \geq 512bit$, $|q| \geq 160bit$, $|n| \geq 160bit$.

The Algorithm for verifying signature (Table 8) of the scheme LD 16.9-01 shows, any pair of (r,s) will be recognized as a valid signature of U on a message M if it meets the condition:

$$s^E \equiv r^{(s.r \bmod p)} \times y^E \bmod p \quad (2.11)$$

Here: U is signing object owning a public key y and $E = H(M)$ are representative value of the message M to be verified.

To find (r,s) from (2.11), the first way is to select a value for r in advance, then calculate s. Then (2.11) will be formed:

$$a^s \equiv s^b \bmod p \quad (2.12)$$

Or in the second way is select s in advance then calculate r. Then (2.11) will be formed:

$$r^r \bmod p = b \quad (2.13)$$

In both two cases, a and b constants. It is easy to see that solutions of (2.12) and (2.13) to find s and r is more difficult than solution of the discrete logarithm problem DLP(g,p).

2.2.1 The second scheme

a) *Structure and operation*

The second signature scheme - symbols LD 16.9–02, is built up under the method stated in Table 4 and 5 in section A with selections: f1(M,Z) = Z, f2(M,Z) = H(M), f3(M,Z) = H(M). The algorithm for formation of parameter and key is similar to that in the scheme LD 16.9–01 (Table 6), algorithms for signature and verifying signature of the scheme are described in Table 8 and Table 10 below.

Table 9. Algorithm for signing messages

Input: p, q, g, H(.), x, M . Output: (r,v).	
[1]. select k: $1<k<q$	
[2]. $Z \leftarrow g^k \bmod p$	(3.1)
[3]. $E = H(M)$	(3.2)
[4]. $w_1 = Z^{-1} \times E \bmod q$	(3.3)
[5]. $u \leftarrow (w_1 + 1)^{-1} \times (k - x \times w_1) \bmod q$	(3.4)
[6]. $r \leftarrow g^u \bmod p$	(3.5)
[7]. $v \leftarrow w_1 \times (u + x) \bmod q$	(3.6)
[8]. return (r,v)	

Table 10. Algorithm for verifying signature

Input: p, q, g, H(.), y, M, (r,v). Output: *true* / *false*.	
[1]. E = H(M)	
[2]. $w_2 \leftarrow r \times g^v \bmod p$	(3.7)
[2]. $A \leftarrow g^{v.w_2} \bmod p$	(3.8)
[3]. $B \leftarrow (r \times y)^E \bmod p$	(3.9)
[4]. if ($A = B$) then {return *true* } else {return *false* }	

b) Correctness of the scheme LD 16.9-02

The thing to be proved is: Let p, q are 2 primes with q|(p-1), $H: \{0,1\}^* \mapsto Z_n$, $q < n < p$, $1 < k, x < q$, $y = g^x \bmod p$, $Z = g^k \bmod p$, $E = H(M)$, $w_1 = Z^{-1} \times E \bmod q$, $u = (w_1 + 1)^{-1} \times (k - x \times w_1) \bmod q$, $r = g^u \bmod p$, $v = w_1 \times (u + x) \bmod q$. If: $w_2 = r \times g^v \bmod p$ $A \leftarrow g^{v.w_2} \bmod p$, $B = (r \times y)^E \bmod p$ then: $A = B$.

Correctness of the newly proposed scheme is proved as follows:

From (3.7) and (3.8) we have:

$$\begin{aligned} A &= g^{v.w_2} \bmod p \\ &= g^{v.(r.g^v \bmod p)} \bmod p \\ &= g^{v.Z} \bmod p \\ &= g^{Z^{-1}.E.(u+x).Z} \bmod p \\ &= g^{(u+x).E} \bmod p \end{aligned} \quad (3.10)$$

From (2.1), (3.5) and (3.9) we also have:

$$B = (r \times y)^E \bmod p$$
$$= g^{(u+x).E} \bmod p \quad (3.11)$$

From (3.10) and (3.11) infer the thing to be proved: $A = B$.

c) Safety level of the scheme LD 16.9-02

From the Algorithm for verifying signature (Table 10) of the scheme LD 16.9–02 shows that, any pair of (r,v) will be recognized as a valid signature if the scheme generated from a message M if it meets the condition:

$$g^{v.(r.g^v \bmod p)} \equiv (r \times y)^E \bmod p \quad (3.12)$$

Similarly, (2.11), to find *r* and *v* from solution of (3.12) is more difficult than solution of the problem $DLP_{(g,p)}$.

3. Conclusion

The article proposes a method of digital signature scheme design based on difficulty discrete logarithm problem. An advantages of the newly proposed method is that it can be used for developing different digital signature schemes to choose suitably for applications in practice. Signature schemes of LD 16.9–01 and LD 16.9–02 presented here has somewhat showed the feasibility of the newly proposed method.

References

[1] Luu Hong Dung, Le Dinh Son, Ho Nhat Quang, Nguyen Duc Thuy,"DEVELOPING DIGITAL SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM PROBLEM", the Eighth National Scientific Meeting of Basic Research and Information Technology Applications (FAIR 2015), ISBN: 978-604-913-397-8.

[2] Luu Hong Dung, Hoang Thi Mai, Nguyen Huu Mong "A form of signature scheme built up based on the digital analysis problem", the Eighth National Scientific Meeting of Basic Research and Information Technology Applications (FAIR 2015), ISBN: 978-604-913-397-8.

[3] Luu Hong Dung, Ho Ngoc Duy, Nguyen Tien Giang, Nguyen Thi Thu Thuy, "Development of a new form of digital signature scheme", the Proceedings of the Sixteenth National Seminar: Some Selected Issues of Information Technology and Communication - Da Nang.

[4] Hoang Thi Mai, Luu Hong Dung, "A form of signature scheme built up based on the digital analysis problem and the square root problem", Journal of Science and Engineering - Military Technical Academy No. 172 (Journal of IT and Communication, No.7 - 10/2015), page: 32 – 41. ISSN: 1859 – 0209.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. IT-31, No. 4. pp.469–472.

[6] National Institute of Standards and Technology. NIST FIPS PUB 186-3(2013). Digital Signature Standard, U.S. Department of Commerce.

[7] GOST R 34.10-94. Russian Federation Standard. Information Technology. Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm. Government Committee of the Russia for Standards (in Russian).

Thuy N.D received the B.S from HUFLIT University in 2005 and M.S degree from Faculty of Information Technology, Military Technical Academy in 2013. My research interests include cryptography, communication and network security.

Dung L.H is a lecture at the Military Technical Academy (Ha Noi, Viet Nam). He received the Electronics Engineer degree (1989) and Ph.D (2013) from the Military Technical Academy.