A Design Method of Digital Signature Scheme Based on Discrete Logarithm Problem

Thuy Nguyen Đuc †, Giang Nguyen Tien ††, Son Le Dinh†††, Dung Luu Hong †††

† Ho Chi Minh City Technical and Economic College, Vietnam
†† Information Technology Department, Department of Defense
††† Military Technical Academy, Vietnam

Abstract
This paper proposes a design method of digital signature scheme based on the difficulty of the discrete logarithm problem. With the proposed method, we can develop a lot of other digital signature schemes to choose suitable for practical applications.

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

1. Problem Posing

In 1985, T. ElGamal [l] proposed the digital signature scheme based on the discrete logarithm problem. Then, in 1989, C.P. Schnorr [2] proposed an efficient signature scheme to shorten the length of the signature and to speed up the signature generation/verification process, and in 1991, the NIST (National Institute of Standards and Technology) proposed the Digital Signature Algorithm (DSA) [3] for the digital signature standard based on ElGamal and Schnorr signature schemes. Currently, the digital signature has been widely applied in e-government, e-commerce ... in the world and initially deployed in Vietnam. Therefore, it is required to be set out the digital signature scheme research - development to design - manufacture new products, safe equipment and information security in countries such as Vietnam. This paper proposes a construction method of digital signature scheme based on the difficulty of the discrete logarithm problem by generalizing ElGamal and Schnorr's method, and some digital signature schemes have been developed based on this method.

2. Construction of digital signature scheme based on discrete logarithm problem.

2.1 Discrete logarithm problem

Let p be a prime number and g is a generating element of $\mathbb{Z}p^*$ group. Then the discrete logarithm problem – DLP (Discrete Logarithm Problem) on the $\mathbb{Z}p^*$, also known as the problem DLP(g,p) is stated as follow:

DLP(g,p): For each positive integer $y \in \mathbb{Z}p^*$, find x satisfying the following equation:

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

The algorithm for the discrete logarithm problem with the public parameters {p,g} written as an algorithm for calculating DLP(g,p)(.) with the input variable y and the value function is the root x of equation (1.1):

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

In an electronic trading system, digital authentication application to authenticate the origin and integrity of information for the data message, the problem DLP(g,p) is difficult in the sense that it cannot be done in real time. There, each member U of the system selects secret key x at will satisfying: 1< x < (p-1), calculate and disclose parameters:

$$y = g^x \bmod p \qquad (1.2)$$

Note:

(i) $DLP_{(g,p)}$ is difficult in the sense that it cannot be done in real time, but not difficult with ever $y \in \mathbb{Z}_p^*$ at all, $DLP_{(g,p)}$, for example, the $y = g^x \bmod p$ with x is not large enough, by browsing gradually x = 1, 2, ... until finding root of (1.2) we will find the secret key x, so the value of the secret key x must be selected so that the calculation $DLP_{(g,p)}(y)$ is difficult.

(ii) Such choice of x means that no one other than U knows the value of x, so knowing x is enough to verify that it is U.

Currently, the problem is still considered to be difficult since no polynomial time algorithm for it is found and ElGamal cryptosystem [1] is an actual proof for the difficult solution of the problem.

2.2 Construct generalized scheme

Generalized scheme is used to develop digital signature scheme for practical applications. Generalized scheme proposed here is constructed basing on difficult solution of discrete logarithm problem and is designed as a signature generation scheme with 2 components similar to DSA in

Manuscript received February 5, 2017
Manuscript revised February 20, 2017

America Digital Signature Standard (DSS) [3] or R34.10-94 GOST of Russian Federation [4], including methods of forming parameters, methods of forming and checking signature shown below.

Method of initialization-generating parameters and keys

Input data: p, q, and x.

Results: g, y, H (.).

Steps:

1. Calculate generating elements of $\mathbb{Z}_p^*$:
$g = h^{(p-1)/q} \bmod p$, with: $1 < h < p$

2. Calculate public key: $y = g^{\pm x} \bmod p$ (2.1)

3. Select hash function H: $\{0,1\}^* \to Z_q$, with:
$q < p$.

Remarks:

(i) p, q: 2 prime numbers satisfy q | (p-1).

(ii) x: secret key of signing object satisfy: $1 < x < q$.

Method of signing messages

Input data: p, q, g, x, M.

Results: (e, s).

Steps:

1. Select value k satisfying: $1 < k < q$. Calculate value *r* by the formula:

$$r = g^k \bmod p \quad (2.2)$$

2. The first component *e* of digital signature is selected in one of two forms:

$$e = f_1(M, r) \bmod q \quad (2.3)$$

3. The second component *s* of digital signature is formed by one of following forms:

$$s = [k.f_2(M,e)^{-1} + x.f_3(M,e)] \bmod q \quad (2.4)$$

or: $s = k.[f_2(M,e) + x.f_3(M,e)]^{-1} \bmod q$ (2.5)

or: $s = x^{-1}.[k.f_2(M,e) + f_3(M,e)] \bmod q$ (2.6)

Remarks:

(i) M: data messages for signing.

(ii) (e, s): signature on M of the object holding {*x*, *y*}.

(iii) $f_1(M,e), f_2(M,e), f_3(M,e)$: as a function of M and e.

Method of verifying signature

Input data: p, q, g, y, M, (e, s).

Results: Assert (e, s) is the valid signature ((e,s) = true) or (e,s) is false and/or M is no longer intact ((e, s) = false).

Steps:

1. Calculate the value *u*:

$$u = g^{s.f_2(M,e)} \times y^{f_2(M,e).f_3(M,e)} \bmod p$$, if s is calculated according to (2.4) (2.7)

or:

$$u = g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p$$, if s is calculated according to (2.5) (2.8)

or:

$$u = y^{s.f_2(M,e)^{-1}} \times g^{f_2(M,e)^{-1}.f_3(M,e)} \bmod p$$, if s is calculated according to (2.6) (2.9)

2. Calculate the value *v*:

$$v = f_1(M,u) \bmod q \quad (2.10)$$

3. Check if: v = e, then: (2.11)

(e,s) = true, otherwise: (e,s) = false.

The correctness of the generalized scheme

That need proving here is: if parameters and key are formed under (2.1), digital signature is formed according to the formula from (2.2) to (2.6), while checking digital signature shall be implemented from (2.7) to (2.10), the condition indicated by (2.11) will be satisfied.

Proposition 1.1:

Let *p* and *q* be two prime numbers with *q* is a divisor of (p-1), *h* is a positive integer less than *p* and $g = h^{(p-1)/q} \bmod p$, $1 < x, k < q$. If: $y = g^{-x} \bmod p$, $r = g^k \bmod p$, $e = f_1(M,r) \bmod q$, $s = [k.f_2(M,e)^{-1} + x.f_3(M,e)] \bmod q$, $u = g^{s.f_2(M,e)} \times y^{f_2(M,e).f_3(M,e)} \bmod p$, $v = f_1(M,u) \bmod q$ then: $v = e$.

Proof:

Indeed, we have:

$$\begin{aligned} u &= g^{s.f_2(M,e)} \times y^{f_2(M,e).f_2(M,e)} \bmod p \\ &= g^{f_2(M,e)\left(k.f_2(M,e)^{-1} + x.f_3(M,e)\right)} \times g^{-x.f_2(M,e).f_2(M,e)} \bmod p \\ &= g^{k + x.f_2(M,e).f_2(M,e) - x.f_2(M,e).f_2(M,e)} \bmod p \\ &= g^k \bmod p \end{aligned} \quad (2.12)$$

From (2.2) and (2.12) we have: u = r.

Therefore:

$$v = f_1(M,u) \bmod q = f_1(M,r) \bmod q \quad (2.13)$$

From (2.3) and (2.13) we infer: v = e.

Things are proved.

Proposition 1.2:

Let p and q be two prime numbers with q is a divisor of $(p-1)$, h is a positive integer less than p and $g = h^{(p-1)/q} \bmod p$, $1 < x,k < q$. If: $y = g^x \bmod p$, $r = g^k \bmod p$, $e = f_1(M,r) \bmod q$, $s = k.[f_2(M,e) + x.f_3(M,e)]^{-1} \bmod q$, $u = g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p$, $v = f_1(M,u) \bmod q$ then: $v = e$.

Proof:

Indeed, we have:

$$\begin{aligned} u &= g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p \\ &= g^{f_2(M,e).k.(f_2(M,e)+x.f_3(M,e))^{-1}} \times g^{x.f_3(M,e).k.(f_2(M,e)+x.f_3(M,e))^{-1}} \bmod p \\ &= g^{k.(f_2(M,e)+x.f_3(M,e)).(f_2(M,e)+x.f_3(M,e))^{-1}} \bmod p \\ &= g^k \bmod p \end{aligned} \quad (2.14)$$

From (2.2) and (2.14) we have: u = r.

Therefore:

$$v = f_1(M,u) \bmod q = f_1(M,r) \bmod q \quad (2.15)$$

From (2.3) and (2.15) we infer: v = e.

Things are proved.

Proposition 1.3:

Let p and q be two prime numbers with q is a divisor of (p-1), h is a positive integer less than p and $g = h^{(p-1)/q} \bmod p$, $1 < x,k < q$. If: $y = g^x \bmod p$, $r = g^k \bmod p$, $e = f_1(M,r) \bmod q$, $s = x^{-1}.[k.f_2(M,e) + f_3(M,e)] \bmod q$, $u = y^{s.f_2(M,e)^{-1}} \times g^{-f_2(M,e)^{-1}.f_3(M,e)} \bmod p$, $v = f_1(M,u) \bmod q$ then: $v=e$.

Proof:

Indeed, we have:

$$\begin{aligned} u &= y^{s.f_2(M,e)^{-1}} \times g^{-f_2(M,e)^{-1}.f_3(M,e)} \bmod p \\ &= g^{x.f_2(M,e)^{-1}.x^{-1}.(k.f_2(M,e)+f_3(M,e))} \times g^{-(f_2(M,e)^{-1}.f_3(M,e))} \bmod p \\ &= g^{k+(f_2(M,e)^{-1}.f_3(M,e))-(f_2(M,e)^{-1}.f_3(M,e))} \bmod p \\ &= g^k \bmod p \end{aligned} \quad (2.16)$$

From (2.2) and (2.16) we have: u = r.

Therefore:

$$v = f_1(M,u) \bmod q = f_1(M,r) \bmod q \quad (2.17)$$

From (2.3) and (2.17) we infer: v = e.

Things are proved.

2.3 Some digital signature schemes developed from the generalized form

2.3.1 The scheme LD 16.12 – 01

Scheme LD 16.12 – 01 was developed from the generalized scheme with (2.4) and (2.7), selections: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$ and $f_3(M,e) = H(M)$, where H (.) is a hash function and H (M) is the representative value of the signed message M. The public key is calculated by using the formula: $y = g^{-x} \bmod p$. The proposed new signature scheme consists of two algorithms: (a) signing messages, and (b) verifying signature - are described in Table 1.1 and Table 1.2 below. The algorithm initialization – generating parameters and keys similar to Generalized scheme.

a) Algorithm for signing messages

Table 1.1. Algorithm for signing messages

Input: p, q, g, x, M. Output: (e, s).	
[1]. select k: $1 < k < q$	
[2]. $r \leftarrow g^k \bmod p$	(3.1)
[3]. $e \leftarrow r \bmod q$	(3.2)
[4]. $s \leftarrow [k \times e^{-1} + x \times H(M)] \bmod q$	(3.3)
[5]. return (e, s)	

Notes:

(i) U: signing object possesses the secret key x.

(ii) M: Message signed by the object U.

(iii) (e, s): the signature of U on M.

b) Algorithm for verifying signature

Table 1.2. Algorithm for verifying signature

Input: p, q, g, y, M, (e, s). Output: *(e, s) = true / false* .	
[1]. $u \leftarrow g^{s.e} \times y^{e.H(M)} \bmod p$	(3.4)

[2].	$v \leftarrow u \bmod q$	(3.5)
[3].	if ($v = e$) then {return *true* } else {return *false* }	

c) The correctness of the scheme LD 16.12 – 01

Set: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$ and $f_3(M,e) = H(M)$. By (3.1), (3.2), (3.3), (3.4), (3.5) and Proposition 1.1, it is easy to get things proved here: $v = e$.

2.3.2 The scheme LD 16.12 – 02

Scheme LD 16.12 – 02 was developed from the generalized scheme with (2.5) and (2.8), selections: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$, $f_3(M,e) = H(M)$, the public key is calculated by using the formula: $y = g^x \bmod p$. The algorithms: (a) signing messages, and (b) verifying signature are described in Table 2.1 and Table 2.2 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

a) Algorithm for signing messages

Table 2.1. Algorithm for signing messages

Input: p, q, g, x, M. Output: *(e, s)* - the signature of U on M.		
[1].	select k: $1 < k < q$	
[2].	$r \leftarrow g^k \bmod p$	(5.1)
[3].	$e \leftarrow r \bmod q$	(5.2)
[4].	$s \leftarrow k \times [e + x \times H(M)]^{-1} \bmod q$	(5.3)
[5].	return *(e, s)*	

b) Algorithm for verifying signature

Table 2.2. Algorithm for verifying signature

Input: p, q, g, y, M, (e, s) Output: *(e, s) = true / false* .		
[1].	$u \leftarrow y^{s.H(M)} \times g^{s.e} \bmod p$	(5.4)
[2].	$v \leftarrow u \bmod q$	(5.5)
[3].	if ($v = e$) Then {return *true* } else {return *false* }	

c) The correctness of the scheme LD 16.12 – 02

Set: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$, $f_3(M,e) = H(M)$. By (5.1), (5.2), (5.3), (5.4), (5.5) and Proposition 1.2, we have: *v=e*. Things are proved.

2.3.4 The scheme LD 16.12 – 03

Scheme LD 16.12 – 03 was developed from the generalized scheme with (2.6) and (2.9), selections: $f_1(M,r) = H(M \| r) \bmod q$, $f_2(M,e) = 1$ and $f_3(M,e) = e$, the public key is calculated by using the formula: $y = g^x \bmod p$. The algorithms: (a) signing messages, and (b) verifying signature are described in Table 3.1 and Table 3.2 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

a) Algorithm for signing messages

Table 3.1. Algorithm for signing messages

Input: p, q, g, x, M. Output: (e, s).		
[1].	select k: $1 < k < q$	
[2].	$r \leftarrow g^k \bmod p$	(6.1)
[3].	$e \leftarrow H(M \| r) \bmod q$	(6.2)
[4].	$s \leftarrow x^{-1} \times (k + e) \bmod q$	(6.3)
[5].	return *(e, s)*	

b) Algorithm for verifying signature

Table 3.2. Algorithm for verifying signature

Input: p, q, g, y, M, (e, s). Output: *(e, s) = true / false* .		
[1].	$u \leftarrow g^{-e} \times y^s \bmod p$	(6.4)
[2].	$v \leftarrow H(M \| u) \bmod q$	(6.5)
[3].	if ($v = e$) Then {return *true* } else {return *false* }	

c) The correctness of the scheme LD 2.02

Set: $f_1(M,r) = H(M \| r) \bmod q$, $f_2(M,e) = 1$ and $f_3(M,e) = e$. By (6.1), (6.2), (6.3) (6.4), (6.5) and Proposition 1.3, we have: *v=e*. Things are proved.

2.4 The safety level of the proposed schemes

The safety level of digital signature scheme is generally assessed through following capabilities:

a) Prevent attacks which reveal the secret key

In the proposed new schema, the public key of signer is formed from the secret key corresponding to: $y = g^{\pm x} \bmod p$. Thus, the ability of attack prevention of this scheme depends on the difficulty solution of the discrete logarithm problem $DLP_{(p,q)}$.

b) Anti – phishing signature

Verifying algorithm of the proposed new schema show that a fake pair (e,s) will be recognized as valid digital signature for a message M if it satisfies conditions shown in Table 5 as follows:

Table 5.

Scheme	Conditions for (e,s) to be the valid signature for the message M
LD 16.12 – 01	$e = \left(g^{s.e} \times y^{e.H(M)} \bmod p\right) \bmod q$
LD 16.12 – 02	$u = \left(y^{s.H(M)} \times g^{s.e} \bmod p\right) \bmod q$
LD 16.12 – 03	$e = H\left(M \| \left(y^s \times g^{-e} \bmod p\right)\right) \bmod q$

The nature of finding the (e,s) satisfying the conditions shown in Table 5 is solving the discrete logarithm problem $DLP_{(p,q)}$.

3. Conclusion

This paper proposes the design method of digital signature scheme based on the discrete logarithm problem by developing a generalized schema, thereby developing some schemes that can be applied in practice. The safety level of the new proposed schema is evaluated by the difficulty level of the discrete logarithm problem. However, the schemes should be carefully evaluated in terms of the safety level as well as effective implementation to be applied in practice.

References

[1] 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, 1985.

[2] Schnorr, C.P., "Efficient identification and signatures for smart cards". Advances in cryptology - CRYFTO '89, August 2&24, 1989, Santa Barbara, pp. 239-252, (Springer-Verlag)

[3] National Institute of Standards and Technology, NIST FIPS PUB 186-3. Digital Signature Standard, US Department of Commerce, 1994.

[4] GOST R 34.10-94. Standard Russian Federation. 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, 1994 (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 Military Technical Academy.

Son L.D is a lecture at the Military Technical Academy (Ha Noi, Viet Nam). He received the Information Technology engineer degree (2001) from Military Technical Academy and Ph.D (2007) from Saint Petersburg Electrotechnical University "LETI", St. Petersburg, Russia.

Giang N.T graduated from Military Technical Academy. He works at Information Technology Department, Department of Defense. His research is information security.