# DEVELOPING DIGITAL SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM PROBLEM

**Luu Hong Dung[1], Le Dinh Son[2], Ho Nhat Quang[3], Nguyen Duc Thuy[4]**

[1] Faculty of Information Technology, Military Technical Academy - Ministry of Defense
[2] Faculty of Information Technology, Military Technical Academy - Ministry of Defense
[3] Faculty of Information Technology, Military Technical Academy - Ministry of Defense
[4] Faculty of Information Technology, Ho Chi Minh City Technical and Economic College
*luuhongdung@gmail, ledinhson@mta.edu.vn, honhatquang@gmail.com, thuyphulam2013@gmail.com*

***ABSTRACT*** *- This paper proposes methods for developing digital signature scheme based on the difficulty of the discrete logarithm problem. From the establishment of overview scheme, some digital signature schemas have been proposed for practical applications.*

***KEYWORDS*** *- Digital Signature, Digital Signature Schema, discrete logarithm problem.*

## I. PROBLEM POSING

In electronic transactions (e-government, e-commerce ...), digital signature is used to meet the authentication requirements of origin and integrity information. 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 the country.

This paper proposes methods for developing digital signature scheme based on the difficulty of the discrete logarithm problem and some digital signature schemas have been developed in this general method.

## II. CONSTRUCTING 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 $Z_P^*$ group. Then the discrete logarithm problem - DLP (Discrete Logarithm Problem) on the $Z_P$, also known as the problem $DLP_{(p,g)}$ is stated as follow:

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

$$g^x \bmod p = y \tag{1.1}$$

The algorithm for the discrete logarithm problem with the public parameters $\{p, g\}$ written as an algorithm for calculating $DLP_{(p,g)}(.)$ 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 $DLP_{(p,g)}$ 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: $y = g^x \bmod p$ (1.2)

*Note:*

(i) $DLP_{(p,g)}$ is difficult in the sense that it cannot be done in real time, but not difficult with ever $y \in Z_P^*$ at all, $DLP_{(p,g)}$, 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 $DLP_{(p,g)}(y)$ 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 [1, 2] since no polynomial time algorithm for it is found and ElGamal cryptosystem [3] 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 America Digital Signature Standard (DSS) [4] or R34.10-94 GOST of Russian Federation [5], including methods of forming parameters, methods of forming and checking signature shown below.

- Method of initialization-generating parameters and keys

Input: p, q, and x.

Output: g, y, H (.).

Steps:

1. Calculate generating elements of $Z_p^*$: $g = h^{(p-1)/q} \bmod p$, with: $1 < h < p$ (2.1)

2. Calculate public key: $y = g^{\pm x} \bmod p$ (2.2)

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

*Remarks:*

(i) p, q: 2 prime numbers satisfy: $q \mid (p - 1)$.

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

- Method of signing messages

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

Output: (e, s).

Steps:

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

$$r = g^k \bmod p \tag{2.3}$$

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

$$e = f_1(M, r) \bmod q \tag{2.4}$$

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

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

or:

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

*Remarks:*

(i) M: data messages for signing.

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

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

- Method of verifying signature

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

Output: 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*:

$$u = g^{s.f_2(M,e)} \times y^{f_2(M,e).f_3(M,e)} \bmod p \text{, if s is calculated according to (2.5)} \tag{2.7}$$

Or:

$u = g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p$, if s is calculated according to (2.6) (2.8)

2. Calculate the value *v*:

$v = f_1(M,u) \bmod q$ (2.9)

3. Check if: v = e, then: (2.10)

(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) and (2.2), digital signature is formed according to the formula from (2.3) to (2.6), while checking digital signature shall be implemented from (2.7) to (2.9), the condition indicated by (2.10) will be satisfied.

**Lemma 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*. If: $g = h^{(p-1/q} \bmod p$ then: $g^q \bmod p = 1$.

Proof:

We have:

$g^q \bmod p = (h^{(p-1)/q} \bmod p)^q \bmod p = h^{(p-1)} \bmod p$

According to Fermat theorem:

$h^{(p-1)} \bmod p = 1$

Therefore:

$g^q \bmod p = 1$

Lemma has been proved.

**Lemma 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 $g = h^{(p-1/q} \bmod p$ . If: $m \bmod q = n \bmod q$ then: $g^m \bmod p = g^n \bmod p$.

Proof:

If: $m \bmod q = n \bmod q$ then: $m = n + k.q$ or: $n = m + k.q$, where k is an integer. Without loss of generality, assume: $m = n + k.q$.

Therefore:

$g^m \bmod p = g^{n+k.q} \bmod p = g^n \times g^{k.q} \bmod p = (g^n \bmod p).(g^{k.q} \bmod p) \bmod p$

$= (g^n \bmod p).(g^q \bmod p)^k \bmod p$

According to Lemma 1.1, we have:

$g^q \bmod p = 1$

So:

$g^m \bmod p = g^n.1^k \bmod p = g^n \bmod p$

Lemma has been proved.

**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: $y = g^{-x} \bmod p$, $r = g^k \bmod p$, $e = f_1(M,r) \bmod q$, $s = [k.f_2(M,e)^{-1} + x.f_3(M,e)] \bmod q$, $u = g^{s.f_2(M,e)} \times y^{f_2(M,e).f_3(M,e)} \bmod p$, $v = u \bmod q$ or: $v = f_1(M,u) \bmod q$ then: $v = e$.

Proof:

Indeed, we have:

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

So:

$$s.f_2(M,e) \bmod q = [k + x.f_2(M,e).f_3(M,e)] \bmod q$$

By Lemma 2.2 we have:

$$g^{s.f_2(M,e)} \bmod p = g^{k+x.f_2(M,e).f_3(M,e)} \bmod p$$

Then infer:

$$g^{s.f_2(M,e)} \times g^{-x.f_2(M,e).f_3(M,e)} \bmod p = g^k \bmod p$$

Or:

$$g^{s.f_2(M,e)} \times y^{f_2(M,e).f_3(M,e)} \bmod p = g^k \bmod p \quad (2.11)$$

From (2.3) and (2.11) we have:

$$u = r$$

Therefore:

$$v = f_1(M,u) \bmod q = f_1(M,r) \bmod q \quad (2.12)$$

From (2.4) and (2.12) 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: $y = g^x \bmod p$, $r = g^k \bmod p$, $e = f_1(M,r) \bmod q$, $s = k.[f_2(M,e) + x.f_3(M,e)]^{-1} \bmod q$, $u = g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p$, $v = u \bmod q$ or: $v = f_1(M,u) \bmod q$ then: $v = e$.

Proof:

Indeed, from (2.6) we have:

$$k = s.[f_2(M,e) + x.f_3(M,e)] \bmod q \quad (2.13)$$

By Lemma 2.2 and (2.13) we infer:

$$g^{s.f_2(M,e)} \times g^{x.s.f_3(M,e)} \bmod p = g^k \bmod p$$

Or:

$$g^{s.f_2(M,e)} \times y^{s.f_3(M,e)} \bmod p = g^k \bmod p \quad (2.14)$$

From (2.3) 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 (2.4) and (2.15) we infer: $v = e$

Things are proved.

### *2.3 Some digital signature schema developed from the generalized form*

#### *2.3.1 The first scheme LD 1.01*

Scheme LD 1.01 was developed from the generalized scheme with selections: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$, $f_3(M,e) = H(M)$, 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 and Table 2 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

*a) Algorithm for signing messages*

**Table 1**

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

*Notes:*

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

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

*b) Algorithm for verifying signature*

**Table 2**

| | |
|---|---|
| Input: p, q, g, y, M - Messages need verifying, (e, s) - the signature of U on M.<br>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* }<br>else {return *false* } | |

*c) The correctness of the scheme LD 1.01*

Set: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$, $f_3(M,e) = H(M)$. 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 second scheme LD 1.02*

Scheme LD 1.02 was developed from the generalized scheme with selections: $f_1(M,r) = H(M \| r) \bmod q$, $f_2(M,e) = e$ , $f_3(M,e) = 1$, 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 and Table 4 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

*a) Algorithm for signing messages*

**Table 3**

| | |
|---|---|
| Input: p, q, g, x, M.<br>Output: *(e, s)* - the signature of U on M. | |
| [1]. select k: $1 < k < q$ | |
| [2]. $r \leftarrow g^k \bmod p$ | (3.6) |
| [3]. $e \leftarrow H(M \| r) \bmod q$ | (3.7) |
| [4]. $s \leftarrow [k.e^{-1} + x] \bmod q$ | (3.8) |
| [5]. return *(e, s)* | |

*Notes:*

"||": operator connects two bit strings.

*b) Algorithm for verifying signature*

**Table 4**

| | |
|---|---|
| Input: p, q, g, y, M - Messages need verifying, (e, s) - the signature of U on M.<br>Output: *(e, s) = true / false* . | |
| [1]. $u \leftarrow g^{s.e} \times y^{e} \bmod p$ | (3.9) |
| [2]. $v \leftarrow H(M \,\|\| u) \bmod q$ | (3.10) |
| [3]. if ( $v = e$ ) then {return *true* }<br>else {return *false* } | |

*c) The correctness of the scheme LD 1.02*

Set: $f_1(M,r) = H(M \,\|\| r) \bmod q = e$, $f_2(M,e) = e$ and: $f_3(M,e) = 1$. By (3.6), (3.7), (3.8), (3.9), (3.10) and Proposition 1.1, we have: $v = e$. Things are proved.

*2.3.3 The third scheme LD 2.01*

Scheme LD 2.01 was developed from the generalized scheme with 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 5 and Table 6 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

*a) Algorithm for signing messages*

**Table 5**

| | |
|---|---|
| Input: p, q, g, x, M.<br>Output: *(e, s)* - the signature of U on M. | |
| [1]. select k: $1 < k < q$ | |
| [2]. $r \leftarrow g^{k} \bmod p$ | (3.11) |
| [3]. $e \leftarrow r \bmod q$ | (3.12) |
| [4]. $s \leftarrow k.[e + x.H(M)]^{-1} \bmod q$ | (3.13) |
| [5]. return *(e, s)* | |

*b) Algorithm for verifying signature*

**Table 6**

| | |
|---|---|
| Input: p, q, g, y, M - Messages need verifying, (e, s) - the signature of U on M.<br>Output: *(e, s) = true / false* . | |
| [1]. $u \leftarrow g^{s.e} \times y^{s.H(M)} \bmod p$ | (3.14) |
| [2]. $v \leftarrow u \bmod q$ | (3.15) |
| [3]. if ( $v = e$ ) Then {return *true* }<br>else {return *false* } | |

*c) The correctness of the scheme LD 2.01*

Set: $f_1(M,r) = r \bmod q$, $f_2(M,e) = e$, $f_3(M,e) = H(M)$ . By (3.11), (3.12), (3.13), (3.14), (3.15) and Proposition 1.2, we have: $v = e$. Things are proved.

*2.3.4 The fourth scheme LD 2.02*

Scheme LD 2.02 was developed from the generalized scheme with selections: $f_1(M,r) = H(M \,\|\| r) \bmod q$ , $f_2(M,e) = 1$, $f_3(M,e) = e$, 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 7 and Table 8 below. The algorithm initialization-generating parameters and keys similar to Generalized scheme.

*a) Algorithm for signing messages*

**Table 7**

| Input: p, q, g, x, M.<br>Output: *(e, s)* - the signature of U on M. | |
|---|---|
| [1]. select k: $1 < k < q$ | |
| [2]. $r \leftarrow g^k \bmod p$ | (3.16) |
| [3]. $e \leftarrow H(M \,\|\| \, r) \bmod q$ | (3.17) |
| [4]. $s \leftarrow k.[1 + x.e]^{-1} \bmod q$ | (3.18) |
| [5]. return *(e, s)* | |

*b) Algorithm for verifying signature*

**Table 8**

| Input: p, q, g, y, M - Messages need verifying, (e, s) - the signature of U on M.<br>Output: *(e, s) = true / false* . | |
|---|---|
| [1]. $u \leftarrow g^s \times y^{s.e} \bmod p$ | (3.19) |
| [2]. $v \leftarrow H(M \,\|\| \, u) \bmod q$ | (3.20) |
| [3]. if ( $v = e$ ) Then {return *true* }<br>else {return *false* } | |

*c) The correctness of the scheme LD 2.02*

Set: $f_1(M,r) = H(M \,\|\| \, r) \bmod q$, $f_2(M,e) = 1$, $f_3(M,e) = e$ . By (3.16), (3.17), (3.18) (3.19), (3.20) and Proposition 1.2, we have: $v = e$. Things are proved.

### *2.4 The safety level of the proposed new schema*

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.

*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 9 as follows:

**Table 9**

| Scheme | Conditions for (e,s) to be the valid signature for the message M |
|---|---|
| LD 1.01 | $e = (g^{s.e} \times y^{e.H(M)} \bmod p) \bmod q$ |
| LD 1.02 | $e = H([g^{s.e} \times y^{e} \bmod p] \,\|\| \, M) \bmod q$ |
| LD 2.01 | $e = (g^{s.e} \times y^{s.H(M)} \bmod p) \bmod q$ |
| LD 2.02 | $e = H([g^{s} \times y^{s.e} \bmod p] \,\|\| \, M) \bmod q$ |

The nature of finding the (e,s) satisfying the conditions shown in Table 9 is solving the discrete logarithm problem. From the research results published, it can be seen that this is a difficult problem if the selected systematic parameters are large enough to method of attack as "brute force" is infeasible in practical applications.

## III. CONCLUSION

This paper proposes the method of developing digital signature scheme based on the discrete logarithm problem by developing a generalized schema, thereby developing some schema 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, it is

important to realize that, the schema should be carefully evaluated in terms of the safety level as well as effective implementation to be applied in practice.

## IV. BIBLIOGRAPHY

[1] Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[2] Hans Delfs, Helmut Knebl (2007), “Introduction to Cryptography: Principle and Applications”, Second Edition, Springer.

[3] T. ElGamal (1985), "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.

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

[5] 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).