A Novel Practical Certificate-Less Digital Signing System Based on Super-Elliptic Bilinear Map Parings

Wenxue Tan , Xiping Wang
Institute of Network Technology, Hunan University of Arts and Science, Changde , P.R.China
College of Economy and Management, Hunan University of Arts and Science, Changde , P.R.China
Email: {twxpaper,xpwang}@163.com

***Abstract*— In this paper, we propose a novel practical *C*ertificate-*L*ess digital signing system based on bilinear map pairings defined on super elliptic curve, which is proved more efficiency than some similar systems pioneered heretofore as viewed from information security application widely applied in mobile-thin computation environment often with a narrow communication bandwidth concomitant. For a long span, the complex managing public key certificate job involved in crypto-system based on identity has been keeping from a more efficient digital signing and disturbing engineers engaging in designing secure mobile *E-C*ommerce. By this scheme, signing subroutine can be in no need of pairs-computation, and verifying can be performed only at cost of 3 times pairs-computation while not introducing special hash function, a necessity in some similar schemes initiated in some references. With respect to security, the system manifests a satisfying immunity from *R*eplacing *P*ublic *K*ey *A*ttack, *F*orging *S*ignature *A*ttack and some other typical attack methods from angle of computability of NP-problem and of provable security. By comparison and analysis in detail and in depth, it is made clear that the signing system can provide a favorable macro-availability and performance, and be fit to be promoted into the application of mobile *E-C*ommerce and some similar requirements.**

***Index Terms*— Bilinear Map; Certificate-Less Signing; Super-Elliptic; Public Key Replacement Attack; Forging Signature.**

I. INTRODUCTION

For the purpose of putting off the burden of digital certificate management, a crypto-system based on the identity was pioneered [1]. However, the inherent problem arises as an accompanist in the encryption system based on the identity, i.e. the task of key-trust, which should be performed by a separated authority named **P**rivate **K**ey **G**enerator, abbreviated by **PKG** which is enabled to absolutely control private key information of all participants. Thus, to some **PKG**s which have evil intentions, there are some possibilities that they forge some participants' signature and in whose name to grasp at some interest and right, while cheating them [2]. In recent years, researching on novel signature schemes or innovated cryptosystems has been a focus of attention in the area of information security.

A. Previous work

An idea of **C**ertificate-**L**ess Public **K**ey **C**rypto **S**ystem, which abbreviated by **CL-PKCS**, was initiated in [2]. **CL-PKCS** doesn't involve the job of key-trust, a necessity in the crypto-system based on the identity, so, it is in no need of her or his public key certificated and approved by the certificate authority. By comparison, to a certain extent, it spares a lot of cost and enables itself fitter for security application designed for the mobile computation environment with low wattage-output and narrow communication bandwidth. Since then, **CL-PKCS** catches crypto professionals' eyes, and many scenarios of **CL-PKCS** are devised [3]–[5].

B. Our contributions

In the course of survey and experiment, a novel practical algorithm of certificate-less digital signing is proposed, for which foundation is laid by the bilinear map parings defined on super-elliptic curve, and in contrast which saves some times of pairing computation in the phrase of signing and of verifying. In addition, the scheme doesn't needs extra function which maps from message to point and especial hash function from stem to stern.

Compared with some homologous schemes pioneered heretofore, its macro-performance has more attraction to those security applications to be deployed in thin-client platforms.

II. SOME CONCERNED FUNDAMENTALS

A. Basic Notations

Some basic notations used throughout the paper are specified in Table I, and the left ones are explained where referred.

B. Bilinear Map Pairings and Characteristics

Definition 1. Let $\mathbf{G}_1$ be a cyclic additive group with a prime order p, P is a generator of $\mathbf{G}_1$ for which $P \in \mathbf{G}_1$, and let $\mathbf{G}_2$ be a cyclic multiplicative group with prime

Submitted date. 2010-10-8.Revised date. 2011-03-08.
This work is partially supported by the Provincial Natural Science Foundation Project of Hunan, Mainland of P.R.China, under Grant No. 09JJ6086.
Correspondence to: Western part of Dong-ting Road, No. 170,415000, Changde, Hunan, Mainland of P.R.China.

doi:10.4304/jsw.6.8.1403-1408

order p . Define a map as (1), and its characteristics are as follows [4].

$$\hat{e} : \mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2 \tag{1}$$

1).Bi-linear. $P_1 \in \boldsymbol{G}_1$,$P_2 \in \boldsymbol{G}_1$,$a_1 \in \boldsymbol{G}_2$,$a_2 \in \boldsymbol{G}_2$ for which (2) is always satisfied.

$$\hat{e}(a_1, P_1, a_2, P_2) = \hat{e}(P_1, P_2)^{a_1 a_2} \tag{2}$$

2). Non-degenerative. For any nonzero-element P_1 and some S for which $P_1 \in \mathbf{G}_1, S \in \mathbf{G}_1$ and equation (3) is satisfied only on condition of $S = O$, in other words be zero-element of $\mathbf{G}_1$.

$$\hat{e}(P_1, S) = 1 \tag{3}$$

3).Computable. For any $P_1, P_2 \in \mathbf{G}_1$ there is found a practical algorithm to compute (4).

$$\hat{e}(\boldsymbol{P}_1, \boldsymbol{P}_2) \tag{4}$$

Such a map as above is defined bilinear map.

The theory of elliptic curve function reveals that bilinear map can be constructed by Weil-Pairing or Tate-Paring on super singularity elliptic curve. As to such bilinear map defined over super elliptic curve on limited field, P is treated as a certain point on elliptic curve; and $\mathbf{G}_1$ as a group with a defined add-operation named point-adding and with a set of all points on super-elliptic curve and the infinity point; and $\mathbf{G}_2$ as a group with a defined multiplication-operation named modular-p-multiplication and with a set of modular-p-residual integers, and O denotes the infinity point.

TABLE I.
BASIC NOTATIONS

Notations	Implication
$\{0,1\}^*$	Bit strings of any bits in length.
$\{0,1\}^n$	Bit strings of *n* bits in length.
$\mathbf{G}_1$	A cyclic additive group with a prime order *p*.
$\mathbf{G}_2$	A cyclic multiplicative group with a prime order *p*.
P	A point generator on ecliptic curve, often denoted by a capital.
x, a, c	Some integer scalars which often denoted by lowercases.

C. Hardness Hypothesis

Definition 2.**E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem. Given 2 groups $\mathbf{G}_1, \mathbf{G}_2$, and 2 distinctive points $P \in \mathbf{G}_1$, $Q \in \mathbf{G}_1$, extract some integer $x \in \mathbf{G}_2$ subject to (5).This problem is defined the **E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem, abbreviated by **ECDLP** [6]. There hasn't been devised a polynomial time algorithm to it. In computational complexity theory, **NP** is one of the most fundamental complexity classes. The abbreviation **NP** refers to "**N**ondeterministic **P**olynomial time". Intuitively, **NP** is the set of all decision problems for which the root can't be verifiable or recognized in polynomial-running-time by a deterministic Turing machine. Obviously, **ECDLP** is an element in **NP**.

$$Q = xP \tag{5}$$

Definition 3. q -**S**trong-**D**iffle-**H**ellman-**P**roblem. Given 2 groups $\mathbf{G}_1, \mathbf{G}_2$, a certain prime q , another integer $a \in \mathbf{G}_2$,any point $P \in \mathbf{G}_1$ and a $q+1$ tuple $(P, aP, a^2P, ..., a^qP)$, and given a random integer $c \in \mathbf{G}_2$,the problem of how to compute (6) is defined q -**S**trong-**D**iffle-**H**ellman-**P**roblem, abbreviated by q-**SDHP** [7]. The principles of Number Theory reveal that q-**SDHP** is a known problem as a member of **NP** .

$$\frac{P}{(c+a)} \tag{6}$$

Definition 4. **N**egligible **Q**uantum. Let $p(\cdot)$ be a positive polynomial of n for which there always exists a certain integer N, subject to $n > N$ and (7), $\varepsilon(n)$ be another positive polynomial, then we say that the function $\varepsilon(n)$ is negligible, and name it **N**egligible **Q**uantum. In Theory of Probability,if probability of some matter is a **N**egligible **Q**uantum, that is to say that such matter occurs impossibly at all.

$$\varepsilon(n) < \frac{1}{p(n)} \tag{7}$$

Definition 5. **P**robability **A**lgorithm for q-**SDHP**. Let A be a certain algorithm, by which the probability to correctly answer q-**SDHP**, denoted by ε , i.e. can be expressed by (8).

$$\begin{aligned} &Pr[A(P, aP, a^2P, ..., a^qP | a \in G_1, P \in G_2) \\ &= (c, P\frac{1}{c+a})] \geq \varepsilon \end{aligned} \tag{8}$$

Then to say A is an algorithm with oddment of ε to solve q-**SDHP** over in favor. In cryptography, most of methods of attack against crypto-system are some probability algorithm. If probability of which are some negligible quantum, they are threats beyond security.

Hypothesis 1. **Security Hypothesis** for q-**SDHP**. If there exists an algorithm by which it spends time t at most to solve q-**SDHP** over $(\mathbf{G}_1, \mathbf{G}_2)$ with oddment of ε, then we say that q-**SDHP** over $(\mathbf{G}_1, \mathbf{G}_2)$ is problem with difficulty parameters (t, ε).

D. Model of Random Oracle Machine

Hash function plays an important part in security proof of crypto-scheme. During the course of proving security, an algorithm denoted by A is always devised as a challenger to attack the crypto-system in question. **R**andom **O**racle **M**achine is proposed as a challenge attack model which abstracted from prototype of hash function [8].

Definition 6.**R**andom **O**racle **M**achine.Hash function as (9),which can be characterized by 3 items as follows.

$$H : \{0,1\}^* \rightarrow \{0,1\}^n \tag{9}$$

Uniformity: output of H is distributed in the scale of $\{0,1\}_n$ uniformly.

Determinability: if inputs of H are alike, outputs of H are equal determinedly.

Availability: given an input bit-string x , output $H(x)$ can have been extracted in time of polynomial expression of length of x, in other words, which can be depicted by a **P**-class problem [9].

Hash function as (8) subject to mentioned be defined as a **R**andom **O**racle **M**achine.

Definition 7. Model of **R**andom **O**racle **M**achine. In the course of proving security of crypto-system, if a certain **R**andom **O**racle **M**achine is introduced, such proof architecture is defined as Model of **R**andom **O**racle **M**achine, abbreviated by **ROM**.

III. A Novel Digital Signature System

The digital signature scheme based on bilinear pairing proposed consists of 7 sub-algorithms include: construction of system, extraction of partial private key, extraction of secret parameters, setting private key, setting public key, generation of signature, and verifying signature. There are 3 entities involved as follows: **K**ey **G**enerating **C**enter which abbreviated by **KGC**, signer and verifier.

A. Algorithm to Construct system

At the beginning, **KGC** performs some tasks as follows.

1.Chose groups $\mathbf{G}_1, \mathbf{G}_2$ and construct a bilinear map $\hat{e}$ over $\mathbf{G}_1, \mathbf{G}_2$.

2.Select a generator $P \in \mathbf{G}_1$ randomly, and compute (10) subject to g be a generator $g \in \mathbf{G}_2$.

$$g = \hat{e}(P, P) \tag{10}$$

3. Chose $s \in \mathbf{G}_2$ randomly as a master key, and set P_{pub} by (11) ,which treated as the public key of system.

$$P_{pub} = sP \tag{11}$$

4. Define two hash functions as (12) and (13). After steps as above, a system parameter set is gotten as (14), denoted by $para$,where master key should be kept secret.

$$H_1 : \{0,1\}^* \rightarrow \mathbf{G}_2 \tag{12}$$

$$H_2 : \{0,1\}^* \times \mathbf{G}_2 \rightarrow \mathbf{G}_2 \tag{13}$$

$$\{\mathbf{G}_1, \mathbf{G}_2, \hat{e}, P, P_{pub}, g, H_1, H_2\} \tag{14}$$

B. Algorithm to Extract Partial Private Key

The fore 2 steps of the job of Extracting partial private key is requested to be executed by **KGC**, and last step is performed by signer denoted as j . On the whole, it is an interactive accordance process between **KGC** and signer.

Firstly, Compute (15) to extract identity information and authenticate identity of signer denoted as j.

$$q_j = H_1(ID_j). \tag{15}$$

Secondly, by computing (16) to extract P_{pri} as a part of input which determines the private key of signer , and send it to signer j over a secure channel.

$$P_{pri} = P\frac{1}{q_j + s} \tag{16}$$

At last, signer j verifies correctness and originality of by checking equality of equation (17). If incorrect parameters are used by **KGC** or mistake instructions away from the protocol are executed by **KGC** , its equality can't be satisfied.

$$\hat{e}(P_{pri}, q_j P + P_{pub}) = g \tag{17}$$

C. Algorithm to Extract Secret Parameter

After getting data-structure of $para$, signer j picks out $x_j \in \mathbf{G}_2$ randomly as a second part of his own private key, and which should be kept secret.

D. Algorithm to Setup Private Key

On condition that 3 variables are known such as system parameter $para$, the partial private key generated by **KGC**, and $x_j \in \mathbf{G}_2$ randomly picked out by signer j as a second part of private key, by computing (18) signer j integrates them and setups his private key denoted by K_{j-pri} , which should be kept carefully in confidence as his signing secret private key.

$$K_{j-pri} = x_j P_{prj} = \frac{x_j}{q_j + s} P \tag{18}$$

E. Algorithm to Setup Public Key

On the basis of $para$ and $x_j \in \mathbf{G}_2$, by computing (19) signer j extracts his public key denoted by $K_{j-pub} = (X_j, Y_j)$, which paired with his private key K_{j-pri} by sharing x_j .

$$X_j = \frac{P}{x_j}, Y_j = \frac{P_{pub}}{x_j} \tag{19}$$

F. Algorithm to Generate Signature

Signer j makes use of signing secret private key to sign message m as following steps.

1.Chose $r \in \mathbf{G}_2$ randomly, and compute (20).

$$rr = g^r, r \in \mathbf{G}_2 \tag{20}$$

2.By (21) compute message digest value of m ,denoted by h , which mixed with a random **I**nitial **V**ector rr ,which revealing the volatile-random and one-off identity information of signer j .

$$h = H_2(m, rr), h \in \mathbf{G}_2 \tag{21}$$

3.Sign h and r according to (22) and get the signature item denoted by S.Mix message digest value h, one-off identity information of signer r with the steady-going

identity information of signer j K_{j-pri} and get signature item.

$$S = (r + h)K_{j-pri}, S \in \boldsymbol{G}_1 \tag{22}$$

Then, (h, S) is a valid signature of m from signer j .

G. Algorithm to Verify Signature

When verifier denoted by v receives message m attached with signature (h, S) signed by signer j who declares he can be identified by ID_j , and his public key be K_{j-pub} . Verifier v can authenticate signature (h, S) ,message m ,K_{j-pub} and **KGC** by executing instructions as follows.

1.Check equality of (23). If result is false, then break off verifying and reject signature, else go to next step. Falseness reveals that the dependency between signer j and **KGC** is in question.

$$\hat{e}(X_j, P_{pub}) = \hat{e}(Y_j, P) \tag{23}$$

2.Retrieve identity information of signer j ID_j from **KGC** and get q_j by (15) then compute rr' by (24). This step confirms authenticity of signer firstly, and intend to restore the volatile-random and one-off ID-information of signer j denoted by rr' through inherent mathematical dependence between signature ,ID-information and public key of signer which in turn can authenticate signature.

$$rr' = \hat{e}(S', q_j X_j + Y_j)g^{-h} \tag{24}$$

3.Check equality of (25). If false is returned, then output rejecting, else output acceptance. By step 2, the volatile-random and one-off identity information of signer j denoted by rr' can be restored, which is used as an initial vector in hash operation. If rr' be correct and m be untouched, the message digest value of rehashing rr' and m can't but equal to h .

$$h = H_2(m, rr') \tag{25}$$

IV. Correctness Proof And Performance Analysis Of System

A. Correctness Proof of Signature System

If (h, S) is a valid signature of message m signed by private key which is paired with public key K_{j-pub} ,then some mathematical relation should be satisfied ,which can prove correctness of signature system,and its proof as follows.

Proof. 1. Check validity of public key of **KGC** and public key of signer j.Bilinear Map value of (26) is denoted by w .

$$w = \hat{e}(X_j, P_{pub}) \tag{26}$$

$$w = \hat{e}(\frac{P}{x_j}, sP) = \hat{e}(P, P)^{{x_j}^{-1}s} \tag{27}$$

By (19) and (11), (26) is transformed into (27). According to bilinear characteristic of map $\hat{e}$, w is rewritten by (28) according to (10).

$$w = \hat{e}(P, P)^{\frac{s}{x_j}} = g^{\frac{s}{x_j}} \tag{28}$$

Bilinear Map value of (29) is denoted by w' .

$$w' = \hat{e}(Y_j, P) \tag{29}$$

By (19) and (11), (29) is transformed into (30). According to bilinear characteristic of map $\hat{e}$, w' is rewritten by (31) according to (10).

$$w' = \hat{e}(\frac{s}{x_j}P, P) \tag{30}$$

$$w' = \hat{e}(P, P)^{\frac{s}{x_j}} = g^{\frac{s}{x_j}} \tag{31}$$

Obviously,w equals to w' , which can be seen from (28) and (31).The equality proves that key pair containing K_{j-pub} as the public key is generated through the cooperation involving **KGC** for real.

2. Check pairing validity of public key and signing secret key of signer j.Get identity information of signer j q_j by (15), and try to extract (32), result denoted by rr' determined by S ,h , K_{j-pub}.

$$rr' = \hat{e}(S, q_j X_j + Y_j)g^{-h} \tag{32}$$

By (20) and (17), (32) is changed into (33).

$$rr' = \hat{e}((r + h)P_{j-pri}, \frac{q_j}{x_j}P + \frac{s}{x_j}P)g^{-h} \tag{33}$$

By (16), (33) is rewritten by (34).

$$rr' = \hat{e}((r + h)\frac{x_j P}{q_j + s}, (\frac{q_j}{x_j} + \frac{s}{x_j})P)g^{-h} \tag{34}$$

According to bilinear characteristic of map $\hat{e}$, rr' is rewritten by (35) according to (10).

$$rr' = \hat{e}(P, P)^{(r+h)\frac{x_j}{q_j+s} \times \frac{q_j+s}{x_j}} g^{-h} \tag{35}$$

Cancel (35) and By (10), rr' can be expressed as (36).

$$rr' = g^r = rr \tag{36}$$

Considering (36) and (20), if all security variables and signature keep untouched during the period from signing to verifying, rr' can't but equal to rr . In other words rr which represents the volatile-random and one-off identity information of signer j can be restored by bilinear map operation.

3.Check signing validity of signature (h, S), Detach m ,h from the signed message, and rehash m with **I**nitiate **V**ector rr' extracted in the fore step, the result denoted by h' ,as (37)

$$h' = H_2(m, rr') \tag{37}$$

Check the equality between h' and h ,which should be satisfied if message m isn't be tampered with and rr is correctly restored. On the contrary, any of conditions is unsatisfying ,there equality relationship doesn't exist.

Summarily ,the signing system be correct.

B. Comparison and analysis of Performance

In many references, a lot of research and exploration which is located on complexity of computation bilinear pairing and on how to speed up computing bilinear pairing is taken into action, and most of corresponding achievement floats on water.

TABLE II.
COMPARISON OF COMPUTATION COST

Scheme	Pair	Mul-G_1	Add-G_1	Exp-G_1	Mul-G_2	MtoP
[5]	5	5	0	2	0	unused
[6]	2	6	0	1	0	used
[2]	3	4	1	1	1	used
$this$	3	1	1	1	0	unused

However, computation bilinear pairing is still a high time-consuming job. The direct result is that the signing program based on computation bilinear pairing still running at slower than required speed which hinged on bilinear pairing computing speed and times of atomic paring computation involved in signing system itself. So, reducing and optimizing configuration of atomic computation of system is constructive to speed up running of system.

TABLE III.
OPERATION SPECIFICATION

Operation	Implication
Pair	bilinear Pairng computation.
Mul-G_1	Scalar Multiplication Over G_1.
Add-G_1	Addition Over G_1.
Exp-G_1	Exponential Computation Over G_1.
Add-G_2	Addition Over G_2.
MtoP	**M**ap variable to **P**oint function.

We compare this signature scheme with those proposed in references [2,5,6] as viewed from configuration of atomic computation such as times of pairing computation, point-multiplication on $\mathbf{G}_1$ and application of special function. It is presupposed that all schemes are based on the same environment of parameters $(\mathbf{G}_1, \mathbf{G}_2, \hat{e})$.

In our scheme, there is no costing pairing computation in signing step because pre-computation (9) is published as a system parameter, while there are 3 times of bilinear pairing computation in use in the step of verifying. On the other hand,it only introduces 2 regular cryptographic secure hash functions,and doesn't need **M**ap-to-**P**oint hash function which is a necessity in other similar schemes and which is low-efficient computationally. The configuration of atomic computation of other schemes are listed in detail in Table II,and some abbreviated operations are specified in Table III.By comparison it is revealed that this scheme demonstrates a more optimal macro atomic-computation-configuration.

V. SECURITY PROOF OF SCHEME

A. Provable Security

Some early crypto-systems or crypto-protocols were developed on the basis of some difficult problems. However, theirs security haven't been proved strictly. Security provable method is a highlight of research in the field of crypto-system in recent years, which is similar with proof method named reduction to absurdity often used in math [10]. Reduction steps are as follows.

1. Introduce some hypothesis of hard problem. The hypothesis indicates that the success probability of solving a hard math problem is a **N**egligible **Q**uantum.

2. Define security model. Security model is a key of the proof method. **RO** model and standard model are in common use. In the architecture of provable security, security model sometimes should be depicted from both aspects of attack action and attack goal. E.g. **R**eplacing **P**ublic **K**ey **A**ttack and **F**orging **S**ignature **A**ttack [11].

3. Reduce and conclude based on security model. In **ROM** model, it is supposed that adversary can break security of scheme at a non-negligible probability, and then manage to solve some primary mathematic hard problem. Whereas, in standard model, the purpose is to demonstrate the formal security so-called which often roots in the complexity of supposition problem well known. For example, 1024-bits **I**nteger **F**actoring **P**roblem.

B. Public Key Replacement Attack

In the circle of certificate-less signature, **R**eplacing **P**ublic **K**ey **A**ttack must be paid enough attention because of signer's public key which doesn't experience compulsive certification. That is to say it isn't a public key certificate [3], [4]. However, it can be proved that **R**eplacing **P**ublic **K**ey **A**ttack has no chance of succeeding against this scheme.

Proof. As to **R**eplacing **P**ublic **K**ey **A**ttack, it is a premise for any adversary that he needs to succeed in replacing public key of signer j $K_{j-pub} = (X_j, Y_j)$ with a forged public key $K'_{j'-pub} = (X'_j, Y'_j)$. Because of (13) being public and K_{j-pub} which extracted from x_j, an adversary attempt to select x'_j and to publish a K'_{j-pub} disguising himself as signer j.

The signing private key K_{j-pri} in (16) is paired with K_{j-pub}, the verifying public key of signer j and which is generated from 2 secret values x_j and s . In addition that adversary can extract q_j because ID_j and H_1 are known and public. However, secret value x_j is the knowledge known only and uniquely by signer j , and secret value is the information known only and uniquely by **KGC**. Both conditions of the mentioned make it be a negligible quantum the probability of success in informing x_j and s by guessing randomly.

So, the forged public key $K'_{j'-pub} = (X'_j, Y'_j)$ doesn't pair with K_{j-pri}, while the public key K_{j-pub} paired with K_{j-pri} is non-forged. **R**eplacing **P**ublic **K**ey **A**ttack has no access of success.

C. Forging Signature Attack

By this scheme, signing is done on the basis of identity information which is public completely and owned by signer j. In addition, **KGC** controls partial information of signing private key of signer j . That is to say if chances of succeeding in forging signature for **KGC** full of hostility are more than other adversary? The answer is "No".

Proof: According to the process of the scheme, it is well known that **KGC** has access to control such information as system master key s , system public key P_{pub} and part of signer's private key P_{pri}. In order to forge signature of signer j , **KGC** manages to forge the signing key of signer j as (16). P_{pri} is generated in step-B and controlled by **KGC**, and only x_j is unknown which is picked out randomly by signer j.

Where does **KGC** look for signs of x_j? Obviously, the public key K_{j-pub} is extracted from x_j by equation (17). If **KGC** can find out x_j on condition of a known pair (X_j, P) or (Y_j, P_{pub}) , then it succeeds in solving an instance of **ECDLP**, which contradicts security hypothesis that at present there doesn't exist a practical algorithm to solve **ECDLP** at a cost of polynomial time [11], [12].

So, there is no path to **F**orging **S**ignature **A**ttack.

In addition, in essence this scheme is a descendant of crypto-system based on identity proposed in reference [1]. It is proved that breaking it is equivalent to solving q-**SDHP** in the model of random oracle machine,as to both chosen-message-attack, and identity-attack, forging signature,and contradicts security **Hypothesis 1**. Thus, it is secure in the circle of **R**andom **O**racle **M**achine.

VI. Conclusions

Certificate-**L**ess signing system is a novel scenario of digital signature in recent years, which reduces public key crypto-system, while not being entangled with key-trust and providing favorable operating rate and computation efficiency built in signing scheme based on identity .

In this paper, we propose a novel practical certificate-less digital signing system based on bilinear map pairings defined on super-elliptic curve. It is proved to be more efficiency than some similar systems pioneered heretofore.

By this scheme, signing subroutine is in no need of pairs-computation, and verifying is performed only at cost of 3 times of pairs-computation while not introducing special hash function, a necessity in some similar schemes initiated in some references. With respect to security, the system manifests a satisfying immunity from **R**eplacing **P**ublic **K**ey **A**ttack, **F**orging **S**ignature **A**ttack and some other typical attack methods from angle of computability of **NP**-problems and provable security.

By comparison and analysis in detail and in depth, it is made clear that the signing system can provide a favorable macro-availability and performance, and be fit for security application in the environment of mobile computation with low watt.

References

[1] H. X. Lai Xin and H. Dake, "An ID-Based Efficient Signcryption Key Encapsulation Scheme," *Journal of Computer Research and Development*, vol. 46, no. 1, May 2009.

[2] M. W. Liu Jingwei, Sun Rong, "Efficient ID-based certificateless signature scheme," *Journal on Communications*, vol. 29, no. 2, Feb. 2008.

[3] S. N. R. W. Baek J, "Certificateless pubic key encryption without pairing," in *Proceedings of the 8th International Conference of .Information Security*, Mar. 2005.

[4] W. Q. Du Hongzhen, "Effieient and Provable-secure certificateless short signature scheme from bilinear Pairings," *Computer Standards and Interfaces*, vol. 31, no. 2, Feb. 2009.

[5] D. H. Qiaoyan, "Efficient certificateless designated verifier signature and Proxy signatures," *Chinese Journal of Electronics*, vol. 18, no. 1, Jan. 2009.

[6] W. Q. Du Hongzhen, "Efficient traceable identity-based signature scheme," *Journal on Communications*, vol. 30, no. 8, Aug. 2009.

[7] Y. Y. Zhou Liang, Yang Wenzhong, "Proxy signature scheme with restricted signing capability," *Journal of Beijing University of Posts and Telecommunications*, vol. 31, no. 3, Mar. 2008.

[8] L. J. Wang and R. C. Jonathan Jen, "Novel Digital Multisignature Scheme," *ICICExpress Letters*, vol. 4, no. 4, 2010.

[9] R. L. Yuan Zhou, Zhenfu Cao, "Provably secure Proxy-Protected signature schemes based on factoring," *Applied Mathematics and Computation*, vol. 164, no. 1, Jan. 2005.

[10] M. J. Zhang J, "A novel ID-based designated verifier signature scheme," *Information Science*, vol. 17, no. 3, Mar. 2008.

[11] X. C. R. H. Jia Yu, Fanyu Kong, "A Forward Secure Threshold Signature Scheme Based on the Structure of Binary Tree," *Journal of Software*, vol. 4, no. 1, Apr. 2009.

[12] Y. L. ChinChen Chang and J. Yang, "An Efficient Authenticated Encryption SchemeBased on Elliptic Curve Cryptosystem for Broadcast Environments," *ICIC Express Letters*, vol. 4, no. 1, Jan. 2010.

Wenxue Tan (1973-). He graduated with Master's of Science in Information Technology and Earth Exploring from East China Institute of Technology, Jiangxi, China,2003.In 2004, he joined Hunan University of Arts and Science and he is an Associate Professor engaging in teaching in Computer Science.

His current research interests include Network and Information Security.

Xiping Wang (1980-). She graduated with Bachelor's of Marketing from East China Institute of Technology, Jiangxi, China, 2004. She is an Instructor of Hunan University of Arts and Science. Her current research interests include Electronic Commerce and Information Security.