Verifiable Threshold Authorization for Scalable and Secure Digital Rights Management

Zhaofeng Ma[1,2], Jianqing Huang[3], Yixian Yang[1], Xinxin Niu[1]
1. Department of Computer Science and Technology, Beijing University of Posts and Telecommunications, 100876, Beijing, China
2. Beijing National Security Science and Technology Co., Ltd, 100876, Beijing, China
3. Library of Beijing University of Posts and Telecommunications, 100876, Beijing, China
Email: mzf@bupt.edu.cn

***Abstract*—With fast development of network computing and storage technologies, it became more and more convenient to share and spread digital resources through kinds of network services, however without protection and constraint of copyright, digital content can be illegally copied, altered and distributed, which could cause revenue loss to commercial digital resource providers, to solve this problem, digital rights management(DRM) is adopted to control copyrights of digital resources in a reasonable degree. Most of current DRM systems were built up in centered authorization mode which can work efficiently in normal case, but once the DRM administrator is unauthentic or the server collapsed, it will not provide authentication and authorization service again. In this paper, a verifiable threshold authorization scheme (VETAS) based on ellipse curve cryptosystem (ECC) and Lagrange polynomial is adopted for scalable and robust digital rights management, in which authorization was based on t-out of n qualified members, less than t members cannot implement authorization, and the system can still work well once part of the members are unauthentic. The advantage of the VETAS scheme is that it works in a "mutual authentication and threshold authorization" mode, thus end-user and the authorization center can authenticate each other to enhance security of corresponding identity, another advantage of the VETAS scheme is it can provide real-time rights management with fairly good robustness and reliability in a threshold authorization mode.**

***Index Terms*—Verifiable Threshold Authorization, Mutual Authentication, Digital Rights Management (DRM)**

I. INTRODUCTION

Widespread and fast development of Internet made it easy to share and exchange digital content via network services such as FTP, WWW, P2P and BitTorrent, through which digital images, music, video, e-Books and games can be freely distributed to end-users. However, without protection and constraint of digital rights, digital content can be copied, altered and distributed. The illegal usage of commercial digital goods could cause revenue loss to digital resource providers. As one of the most important issues that International Property Organization (WIPO [1]) declared, many content providers made much effort to protect their digital products from being violated. However the effects were not so good as they expected, for customers wanted to use digital resource such as software, movies, music and games at lowest cost (even they expect free use), while content providers would like to provide digital goods in a copyrighted way for profits. To explore efficient and effective approaches to protect digital rights, in 2001 W3C built up a special group focusing on digital rights management (DRM) to discuss the illegal copying and spreading of rights-protected digital resources [2]. Meanwhile, since 2001, ACM SIGSAC has sponsored 4 times annual conferences on DRM [3,4] for the efforts of property protection of various digital products(DRM'01, DRM'02, DRM'03, DRM'04, and the DRM'05 is now being on its given schedule). While in 2004 IEEE Signal Processing called for papers on topics of DRM and the forthcoming IEEE conference on DRM will be hold in 2006 again. In fact, as a new security application field, DRM was now being studied much more, since 2001, at least 18 international conferences related to security regard digital rights management as one of most important security interests topic. In general, digital rights management allows content owners to define and enforce restrictions on how the content is used [1-3], which mainly includes publishing architecture, business models for online content distribution, digital policy management, privacy and anonymity, security including encryption, authentication and authorization, tamper resistance, and watermarking, traitor tracing, broadcast encryption, obfuscation, usability aspects of DRM systems. In a DRM system, authorization is one of most important issues should be taken into account, for the whole procedure of DRM relies on the authorization to get rights of the protected content, which includes authentication of principal, license creation, releasing, revocation and transferring, during the whole process it must ensure data security, integrity, and fairness and non-repudiation of the transaction, and it must maintain the authorization for latent update of license for rights management [1-5].

However, most of the current researches focused much more on DRM architecture and rights expression language, but lacked of attention on authorization methods and technologies (which will be detailed in section II). In fact, most of current DRM systems were

doi:10.4304/jsw.8.6.1526-1535

built up in centered authorization mode which can work efficiently in normal case, but once the DRM administrator is unauthentic or the server collapsed, it will not provide authentication and authorization service again.

To solve this problem, in this paper, a verifiable threshold authorization scheme (VETAS) is adopted for collaborative and robust authorization, where ellipse curve cryptosystem (ECC) and Lagrange polynomial was applied to construct effective threshold scheme, thus any t-out of n qualified members can cooperatively implement the authorization, and less than t members cannot do it. The advantage of the VETAS scheme is that it works in a "mutual-authentication and threshold authorization" way, thus each member and the authorization center can authenticate each other, and through the threshold mechanism it enhanced reliability and fault tolerance of the system, and even part of the qualified members was absent, but the authorization can still work well as usual. Cryptanalysis manifests the proposed VETAS scheme is secure, verifiable and reliable for digital rights management with real-time performance.

The rest of the paper is organized as follows: in section II we overview the related work in DRM authorization. In Section III, we detail the principle of threshold schemes, then in Section IV we present our verifiable threshold authorization scheme (VETAS) for digital rights management, and in section V, we analyze the security, integrity and verifiability of our proposed VETAS scheme, in which various attacks upon VETAS are discussed to reflect the security and robustness. Finally in section VI we give brief remarks and conclusion of the paper.

II. RELATED WORK

As for digital rights management, especially for the protection of multimedia resources, watermarking was the most popular and effective approach for copyright identification [5-8], in which copyright information was embedded in the objects that to be protected (so called carrier), when necessary the embedded watermarking can be recovered to prove the copyright. Watermarking is fairly suitable for identification and conformation of the original owner rights for multimedia resources. However it cannot prevent the digital resources from being illegal copied and arbitrarily distributed [8], because the primal goal of watermarking is to provide copyright identification rather than copy protection, thus resources embedded with watermarking can be played and used without any disturbing [8]. In fact, current DRM conferences paid much more attention to copy protection rather than watermarking identification for the later had been studied thoroughly and made much progress, however the copy protection is still a challenge, and till now there are some work had been done that tried to solve the problems, upon which Feng Bao proposed Fair Exchange Protocols with On-line TTP [9]. A.O. Waller studied how to delivery digital content over Internet [10], Kundur, D adopted fingerprint for digital content protection [11]. Claudine Conrado proposed Identity-based scheme based on authorization certificates for rights distribution and management [12]. Iwata, T announced a P2P DRM system for content delivery [13]. Andreaux, J.P. used broadcast for the multiple devices of end-user for multimedia rights management in home network [14]. Upon the above researches, Feng's scheme built on a third trusted part (TTP) which is fairly efficient in licensing management (for its fairness), unfortunately it couldn't provide remote persistent control in open network environment. Fingerprint is not so efficient when the media resource content is large. Authentication and Identity-based scheme by Claudine Conrado did not prove its fairness and it involved user's privacy, its disadvantage is that the license releasing mode is static, which can't support license migration among multiple devices. Recently, Messerges proposed mobile digital rights management which provided a useful rights control explore in mobile computing environment [15], however it didn't consider authentication among different domain. Byers analyzed the frangibility and security of DRM content creation and releasing [16], and Reihaneh Safavi-Naini studied the interoperation among heterogeneous DRM systems [17], Bogdan proposed DRM security architecture for home networks [18], in which a pre-authorization mechanism is adopted to reduce the communication cost, but it can't ensure forward security. In fact, the most important principle of DRM systems is a trade-off between security and accessibility [19].

As for the expression and definition of DRM, till now, several international DRM languages were developed, such as ODRL Initiative implemented Open Digital Rights Language (ODRL [20]) for rights definition. ContentGuard developed XrML [21] for rights expression, which had been adopted as draft for MPEG-2. Till today, Digital Object Identify (DOI [22]) is now being put to use for digital resource identification (i.e. IEEE paper identification).

Moreover, in commercial fields, there are several DRM systems, among which IBM Electronic Media Management System (EMMS) [23-24], Microsoft Windows Media Rights Manager (WMRM) [25], InterTrust Rights System [26], and DRM Real Systems Media Commerce Suite (RMCS) [27] are the most promising digital rights management systems.

IBM EMMS [23] was developed for the preparation and secure rights management of all forms of digital content. The EMMS supported pay-per-use, pay-per-time, and subscription, and controlled printing, and protected transfer to portable devices and portable media, but up to date EMMS only supports Windows platforms. Another solution of IBM is its Cryptolope technology [24] (cryptographic envelope) which consists of Cryptolope builder, player and clearing house, encrypt key content information into a cipher envelope to provide secure distribution, the advantage of Cryptolope is that it supports super-distribution, however the demerit of Cryptolope system is that it strictly constraint customers into a closed InfoMarket environment.

Microsoft WMRM [25] is a Client/Server DRM

system for rights management of multimedia resources, which was built up on component object model (COM) to provide application programming interface (API) for high-level operation. However it only supports WMA (Windows Media Audio) and WMV (Windows Media Video) file formats. A most important demerit of WMRM is that the algorithm in WMRM is not so efficient and secure.

InterTrust Rights System [26] offered a solution for content packaging, distribution and rights management based on a packager program and rights server. It supports pay-per-use, rentals, sales, and try-before-buy business models. Up to date, InterTrust Rights System is fairly good to provide authorization, but it is fully based on a centered Client/Server mode.

RealNetworks RMCS [27] consists of a series servers for packaging, streaming and a secure plug-in for licensing management of Real format file, which supports Windows and UNIX platform adaptively for content subscription, video on demand and other business models.

Expects for the above major solutions on multimedia resource protection, there are still many other commercial systems such as Liquid Audio (www.liquidaudio.com), Alchemedia (www.alchemedia.com), Digital World Services (www.dwsco.com), SealedMedia (www.sealedmedia.com). Another application of DRM is E-Book, upon which EBX working group established the EBX standard [28] for digital rights management of electronic books, which control digital books resource through a right-protection reader to protect digital books from being copying and spreading.

The common problems in the current DRM systems are the compatibility and interoperability, for example, WMRM only supports windows media format (wma, wmv), while RMCS can only work for Real Networks file format. Another problem of current DRMs is although they could provide dynamic authorization, however they do not support authorization transferring. As for the architecture of DRM, current DRM authorization was based on socket connected-oriented mode, which is effective only when the socket connection amount is not too large, the demerits is with the increment of connection of license requests the system will get deficient in replying the concurrent requests from large amount clients. While authorization in Browse/Server mode is efficient in concurrency, however its real-time performance is not so good. Usually the centralized systems rely much more on the server and are weak in security, stability and reliability.

Existing DRM authentication and authorization was not efficient in real-time performance which will become a bottleneck for online license management of digital multimedia resources. Current DRM systems can provide license release service, however they didn't consider the authorization mode (centered or distributed), license revocation, license storage. Upon the usage control, it is weak in reliability and persistent remote control to ensure that the content was used in a secure way and not to be cracked.

Most of current DRM systems built up based on their own authentication and authorization mechanism, during which the fairness, privacy and creditability of the transaction is unknowable to users. Another problem is heterogeneous DRM systems are weak in interoperability, scalability and availability.

In fact, according to the W3C DRM draft and requirement of ACM DRM proposal, the authorization mode in DRM can be classified into static pre-authorization and dynamic post-authorization, while in terms of whether the authorization support license transferring or not, authorization can be classified as non-transferable and transferable types. A secure and reliable DRM authorization should meet the following requirement:

(1) The authorization protocol should be secure, fair, and reliable during the whole procedure of authorization.

(2) The status of the license should be self-contained and consistent, by which the DRM authorization can be maintained correctly with consistency.

(3) Authorization and revocation should be efficient, effective and robust for real-time license management.

(4) The operation of DRM authorization should be available and scalable for dynamic license management.

The security of DRM authorization is based on the fact the DRM administrator must be trustable, however the assumption is not true all the time, once the administrator is not trustable, then there's no security, then it is necessary for the system to build up a secure and efficient mechanism to decrease the risk. To enhance the reliability and security, voting mechanism is an efficient and acceptable method to make group-oriented decision, upon which the implementation can adopt threshold cryptosystem to realize. Based on the above criterion of authorization in DRM, we proposed a verifiable threshold authorization scheme (VETAS) for digital rights management. The following sections will give detailed description of the VETAS scheme (as a basic component, the threshold scheme for secret sharing is introduced first).

III. Threshold Scheme for Secret Sharing

A. General Structure of Threshold Scheme

Threshold scheme was firstly proposed independently by Blakley and Shamir in 1979 [29-30], since then threshold cryptosystem had been studied much more. Generally, a secret sharing scheme is a method of distributing shares of a secret among a set of participants in such a way that only qualified subsets can reconstruct the secret from their shares. Such a scheme is said to be perfect if the subsets that are not qualified to reconstruct, the secret is absolutely kept on without leakage of any information.

Whether a certain subset is qualified or not is determined by a fixed, so-called, access structure [31-32], a secret sharing scheme is the family of qualified subsets. Considering a monotone access structures: If $X \in T$ and $X \subseteq X' \subseteq P$, then $X' \in T$. A minimal qualified subset $Y \in T$ is a subset of participants such that $Y' \in T$, for all $Y' \subset Y$. The basis of T, denoted by T_0, is the family of all

minimal qualified subsets. For any $T_0 \subseteq 2^P$ the closure of T_0 is $C(T_0) = \{\exists X \in T_0, X \subseteq X' \subseteq P\}$. Therefore, an access structure T is the same as the closure of its basis T_0. A secret sharing scheme is called perfect if unqualified subsets of participants obtain no information about the secret. It means that the prior probability $P(K=K_0)$ equals the conditional probability $P(K=K_0| X)$, where X is the unqualified subsets of T. From the point of view of information theoretic models we can state the requirements for a secret sharing scheme using the entropy function H as follows:

(1) Any qualified subset can reconstruct the secret

$$\forall_{X \in T} H(K \mid X) = 0 \tag{1}$$

(2) Any unqualified subset has no information about the secret

$$\forall_{X \notin T} H(K \mid X) = H(K) \tag{2}$$

Usually, the participants were authorized to an average share, when giving different weight of sub-key k_i to each participant, and then the threshold scheme is called as Weighted Threshold Scheme (WTS), which means that different participants have different weight of authorization ability. Given $w_i \in N$ as the share that the member p_i hold, to recover the master key k_0, only the following condition is satisfied:

$$w_{i1} + w_{i2} + \ldots w_{it} \geqslant t \tag{3}$$

B. Variant Construction of Threshold Scheme

As for the construction of threshold scheme, there are many approaches to build up the secret sharing system [29-32, 58-59]: such as Shamir's Lagrange polynomial and Blakley's vector space secret sharing scheme. In fact, Knapsack problem, Chinese Remainder Theory, and Group theory et al can be adopted to construct threshold scheme. And moreover, Reed-Solomon coding method was introduced by McEliece and Sawate to construct secret sharing which can prevent part of the cooperator providing false secret share.

C. Principle of Threshold Scheme for Secret Sharing

Simply to say, the principle of the threshold scheme build up an efficient way to ensure the system's reliability and security based on redundant information in a *t* out of *n* members [51-54], which can be viewed as a group-oriented decision making strategy. From the point of view of geometry, threshold scheme is equivalent to the problem that *n* vectors can be expressed by *t* kernel vectors, where *t* is the rank of the n vectors, and moreover the *t* independent vectors are the maximal linear independent group of the space. While according to matrix theory, the construction of a threshold scheme can be viewed as a *t*-rank matrix $T_{t\times t}$ expands to a *n*-order matrix $N_{n\times n}$. Now we give detailed explain of the above statement through an instance by Lagrange Polynomial Threshold Scheme.

Supposing $K \in Z_q$ (Z_q is a prime field with generator q), randomly select a t-1 order polynomial f(x) which satisfied the condition *f(0)=k*, then sending each user u_i a secret share $f(u_i)$, where u_i is the identity of user U_i. Any t members can corporately recover k through the construction of Lagrange polynomial:

$$k = \sum_{i-1}^{t} f(u_i) \prod_{j=1, j\neq i}^{t} \frac{u_j}{u_j - u_i} \tag{4}$$

Generally, from the point of view of mathematics, given *t* points $(x_1, y_1), \ldots, (x_t, y_t)$, then we can definitely decides a *t-1* order polynomial, which can be constructed as follows:

Supposing $(x_1, y_1), \ldots, (x_t, y_t)$ stands for the *t* members in the system, to recover the secret *k*, given the polynomial to be constructed is denoted by:

$$p_{t-1}(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i \tag{5}$$

Then applying the above t points to the polynomial p(x), then we have:

$$\begin{cases} y_0 = a_0 + \sum_{i=1}^{t-1} a_i (x_0)^i \\ y_1 = a_0 + \sum_{i=1}^{t-1} a_i (x_1)^i \qquad (*) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ y_{t-1} = a_0 + \sum_{i=1}^{t-1} a_i (x_{t-1})^i \end{cases} \tag{6}$$

Upon the above equation group (*), there are *t* equations with *t* unknowns and the order of each unknowns is 1, thus (*) is a definite linear equation group, whose solution can be deduced according to Vandermonde theory. In fact, the coefficients of the above equations are a Vandermonde determinant, which can be denoted by:

$$V_0 = \begin{vmatrix} 1 & x_1^1 & x_1^2 \ldots x_1^{t-1} \\ 1 & x_2^1 & x_2^2 \ldots x_2^{t-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 1 & x_t^1 & x_t^2 \ldots x_t^{t-1} \end{vmatrix} \quad V_y = \begin{vmatrix} y_0 & x_1^1 & x_1^2 \ldots x_1^{t-1} \\ y_1 & x_2^1 & x_2^2 \ldots x_2^{t-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ y_t & x_t^1 & x_t^2 \ldots x_t^{t-1} \end{vmatrix} \tag{7}$$

If there exist two values $x_i = x_j$, then $V_y = 0$, otherwise, according to Cramer theorem, the equations (*) can be resolved definitely to decide each coefficients a_0, a_1, $a_2, \ldots, a_{t-1}$, where

$$a_0 = V_0 / V_y \tag{8}$$

Thus the secret *k* can be decided definitely.

In another point of view of numeric method, *n* points in 2-demension can definitely decide an *n-1* order polynomial, by Lagrange method, the polynomial is decided as follows:

$$p_{t-1}(x) = \sum_{i=0}^{t-1} (yi \cdot \prod_{j=0, j\neq i}^{t-1} \frac{x - x_i}{x_j - x_i}) \tag{9}$$

Let x=0, then the constant can be deduced as:

$$k= p_{t-1}(0) = \sum_{i=0}^{t-1}(y_i \cdot \prod_{j=0, j\neq i}^{t-1} \frac{x_i}{x_i - x_j}) \quad (10)$$

Then if we denote $b_j = \prod_{j=0, j\neq i}^{t-1} \frac{x_i}{x_i - x_j}$, then $k=\sum_{j=0}^{t-1} b_j y_j$, thus the master key k is the linear combination of *t* sub-keys. Especially when all members union to construct the master key, i.e. in (t, n) scheme, t=n, then the threshold scheme leads to Knapsack problem.

In fact, from the point of view of algebra theory, Shamir's threshold scheme and Berkely's are isomorphic. The construction of threshold scheme based on two fundamentals, firstly, decision-making is decided by group-oriented operation, which is similar to vote mechanism. According to geometry theory, the construction of (t, n) threshold scheme can be viewed as that in a *t*-dimension space, it can be spanned by the t-dimension maximal linear independent vectors to n-vector structure whose rank is still t, for the randomicity of the *n-t* vectors, and thus it is difficult to search (guess) the *n-t* solutions in polynomial time. However we must pointed out that according to information theory, Berkely's scheme is not perfect scheme but Shamir's is perfect scheme. The strict proof of the security of perfect threshold scheme can refer to information theory.

Since Blakley and Shamir firstly independently proposed threshold cryptosystem, much progress had been done. Although the shares were created securely by the system center (called dealer), however during the cooperation stage of reconstructing the secret, some participants may provide false share, to solve the problem, Tompa and Woll proposed a (t, n) threshold scheme that can detect cheat [33], however Brickell and Lin pointed out that Tompa's scheme explored secret when detecting cheaters [34], and then proposed a scheme that can avoid the problem in cheat detection. Later Pedersen proposed a new threshold scheme without a dealer[35], later Li pointed out the scheme is not secure[36], for t or more members can compensate together to recover the secret and moreover they can deduce each member's sub-key. In fact, this type of scheme can't ensure the correctness of each share, to solve this problem, Chor proposed verifiable secret sharing (VSS) [37], later Gennaro R. and Micali S. enhanced Chor's scheme by reducibility [38]. Cramer proposed a domestics non-interactive multi-part computing scheme, however for it can't ensure the security of the sub-key from the key distribution center (KDC), thus it is not secure [39]. Marsh proposed robust threshold secret sharing scheme [40], Han proposed a verifiable secret sharing scheme based on ECC and Lagrange [41], however the signature is directly applying to the message itself rather than the message's digest, thus when the message is too large such as a multimedia file, the system will not be so efficient, another demerits of Han's scheme is its weak security for the signature does not use hash function. Chen proposed group-oriented verifiable secret sharing scheme [42], which built up the system based on the assumption that each member in the system is trustable, obviously the assumption is not reasonable all the time, thus the scheme is not secure in practice. Markus A. Stadler proposed publicly verifiable secret sharing(PVSS) scheme [43], and Mao proposed a PVSS scheme based on factoring problem [44], later Fabrice Boudot and Jacques Traore found that Stadler and Mao's scheme is deficient for its much more interaction turns, and proposed a delay secret recover scheme based on discrete logarithm and factoring problem [45]. In fact, in practice, authorization in DRM system should not only meet the command of security but be real-time and reliable for robust operation. Most of the above schemes were built up based on discrete logarithm or factoring problem, whose efficiency and real-time performance is not enough for online real-time licensing management and authorization, some of above stated schemes themselves are not secure.

Based on the above research work [41-45], in this paper, we improved and enhanced the work in [41] and a verifiable threshold authorization scheme (so called VETAS) is adopted for robust DRM authorization. The VETAS is based on [41] and uses ellipse curve cryptosystem (ECC) and Lagrange polynomial to provide robust, real-time licensing management, which works in a "mutual-authentication and threshold authorization" mode, in which authorization was based on t-out of n qualified members, less than t members cannot implement authorization, and the system can still work well once part of the members are unauthentic. To prevent membership personation, the VETAS scheme was enhanced with special authentication constrained with each member's machine space character. The advantage of the VETAS is it works in a "mutual authentication and threshold authorization" mode, thus end-user and the authorization center can authenticate each other for enhanced security of corresponding identity, and another advantage of the proposed VETAS scheme is it can provide real-time and online rights management with fairly good robustness and reliability in a threshold authorization mode. Comparing with current scheme, the VETAS scheme can only works on special machine with time and space constraint.

IV. The Proposed VETAS Scheme

The VETAS scheme improves and enhances the work in [41] was based on the elliptic curve cryptosystem (ECC) and Lagrange polynomial, in which ECC was first proposed independently by Neal Koblitz [46] from the University of Washington, and Miller[47], who was then at IBM, Yorktown Heights in 1985, the ECC has now been widely used in cryptosystems. The security of the ECC depends on the difficulty of solving the ECDLP [46-47]. The ECC is constructed using integer points over an elliptic curve in a finite field. Basic operations include addition and multiplication under the ECC, so operations based on the ECC are more efficient than other cryptosystems, including the RSA and DSA. The ECC is employed to solve the security problems of a cryptosystem, while maintaining efficiency. Up to date, the ECC cryptosystem has now become the de factor

standards of many organization and association, such as ANSI X9.42, ANSI X9.63 and IEEE P1363, FIPS 186- 2 [48-50,55-57].

A. Elliptic Curve Cryptosystems

An *elliptic curve E defined over* F_q is a set of points $P= (x_p, y_p)$ where x_p and y_p are elements of F_q that satisfy a certain equation, if $q = p$ is an odd prime and $p > 3$, then a and b shall satisfy $4a^3+27b^2 \neq 0 \pmod p$, and every point $P = (x_p, y_p)$ on E (other than the point *2*) shall satisfy the following equation in F_p : ${y_p}^2 = {x_p}^3 + ax_p + b$. For further back- ground of the case that $q = 2^m$ and other details on elliptic curves, see [46-47].

Supposing that GF(p) is a finite field with characters p≠2,3, for a, b∈ GF(P) where $4a^3+27b^2 \neq 0 \pmod p$. Elliptic Curve $E_{(a, b)}$ (GF(p)) in GF(p) is defined as the point set （x, y）∈ GF(p) × GF(p) that satisfies the equation $y^2 = x^3 + ax + b$,where the infinite point O is included in $E_{(a, b)}$ (GF(p)). All points in GF(p) is an Abelian group, where the identical element is O. Supposing P and Q are points in $E_{(a, b)}$(GF(p)), if P=O，then $-P = O$, $P + (-P) = O$; denote P=(x_1,y_1),Q(x_2,Y_2)，then -P=(x_1,y_1) ， and P+(-P)=O, if Q≠ — P, $P + Q = (x_3, y_3)$, where $P + Q = (x_3, y_3)$

$$\begin{aligned} x_3 &= u^2 - x_1 - x_2 \\ y_3 &= u(x_1 - x_3) - y_1 \end{aligned} \tag{11}$$

$$u = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases} \tag{12}$$

The Elliptic Curve Digital Signature Algorithm (ECDSA) includes 4 stages, elliptic curve domain parameter generation and their validation, key generation and validation, signature generation and signature verification.

B. Elliptic Curve Domain Parameter

Elliptic curve domain parameters over F_p consists of the following parameters:

(1) A field size $q = p$ that defines the underlying finite field F_q, where $p > 3$ should be a prime.

(2) If the elliptic curve was randomly generated, a bit string SEED with length at least 160 bits is needed (this is the Optional parameters).

(3) Two field parameters a and b in F_q which is used to define the equation of the elliptic curve E:

$$y^2 = x^3 + ax + b ; \tag{13}$$

(4) A point $G= (x_G, y_G)$ of prime order on E, where $G \neq 0$ is a must condition.

(5) The order n of the point G, should be satisfied $n > 2^{160}$ and $n > 4\sqrt{q}$;

(6) The cofactor $h = \#E(F_q)/n$ *is* a optional parameter.

For convenience, Elliptic curve domain parameters over F_p can be written as:

$$P_{ECC} = (q, FR, a, b, G, n, h) \tag{14}$$

C. VETAS: Verifiable Threshold Authorization Scheme

The VETAS scheme includes a License Authorization Center (LAC), n qualified members (U_i) to construct the system. The proposed scheme includes secret sharing stage, joint signature for license authorization stage and signature verification stage.

(1) Secret Sharing

Given K∈Z_q, LAC randomly selects a polynomial f(x) in Z_q with order t-1, where f(0)=k, then releases the secret share f(ui) to Ui, here ui is the public identify information of Ui. Any t members can reconstruct the above secret k, through the following formula:

$$k_0 = \sum_{i-1}^{t} f(u_i) \prod_{j=1, j\neq i}^{t} \frac{u_j}{u_j - u_i} \tag{15}$$

In secret sharing stage, LAC distributes the sub-keys ki(i=1,…,n) to each valid members, and each member ui can only get his(her)own sub-key rather than other that of other's.

Step1: Each user U_i sends his/her machine id, called MID_i, which can be TPM or network MAC, CPU serial.

Step2: LAC computes secretly and passed for each user U_i's session key K_{ui} according to each user's MID_i respectively.

Step3: LAC acts as Dealer and secretly creates the key k_0.

Step4: LAC then builds up the Lagrange polynomial based on the above polynomial as following:

$$f(x) = k_0 + a_1 x + a_2 x^2 + ...a_{t-1} x^{t-1} \bmod n \tag{16}$$

where $k_0 = f(0)$.

Step5: LAC computes $t_i = f(u_i)$ (i=1,…,n) for all the members, and then computes $t'_i = E_{k_{ui}}(t_i)$ and passes t'$_i$ to corresponding member.

Step6: LAC computes $F_i = a_i G$ (i=1,…,n) and broadcasts them to u_i .

Step7: After received t'$_i$ and F_i, LAC decrypt t'$_i$ to t_i , $t_i = D_{k_{ui}}(t'_i)$, then any t out of n members can cooperate to verify the validity of messages that got from LAC through the following equation:

$$t_i G = \sum_{j=0}^{t-1} u_i^j F_j \quad (17)$$

If the above equation is hold, u_i accepts the sub-key from LAC, otherwise, he (she) rejects the message from LAC.

(2) Joint Signature for License Authorization

Step1: LAC computes d_i secretly as $d_i = a_i \prod_{\substack{j=0 \\ j \neq i}}^{t-1} \frac{u_j}{u_j - u_i} \bmod n$, and denotes $d_0 = k_0$, and computes $Q_i = d_i G$ (i=0,…,t-1),here $Q=d_0G$, and then sending Q_i to each member u_i secretly.

Step2: Each u_i randomly and secretly selects k_i (i=0,…,t-1) ,and computes $X_i = k_i G$, to LAC, then Ui's MID_i is automatically gained and submitted with X_i together, then encrypt and pass the message to LAC, that is $C_{u_i} = E_{k_{ui}}(\mathrm{MID_i} || \mathrm{X_i})$.

Step3: After received C_i, LAC decrypt Ci, $M_i' = D_{k_{ui}}(C_i)$ Mi'=[MID'i|| Xi], then LAC authenticates whether the MIDi in Mi' is equal to the MID_i each U_i commits in Secret Sharing Stage , if the $MID'_i = MID_i$, LAC computes $X = \sum_{i=0}^{t-1} X_i = (x, y)$ .otherwise LAC rejects X_i.

Step4: LAC computes the digest of m by hash function: e=SHA-1(m), and computes $r = ex \bmod n$, then LAC broadcast *e* and *r* to u_i.

Step5: u_i computes $s_i = (ek_i + d_i r) \bmod n$, and sends s_i to LAC.

Step6: LAC verifies $eX_i = s_i G - rQ_i$. If this is hold, then return to Step6, otherwise denies the co-signature.

Step7: LAC computes $s = \sum_{i=0}^{t-1} s_i$, then (r, s) is the co-signature of m in VETAS scheme.

(3) Signature Verification

Step1: When verifying the signature from LAC, the verifier V computes $sG - rQ = (x_e, y_e)$, and $r' = x_e \bmod n$.

Step2: V validates whether r=r' is true or not. If it is hold, V accepts the signature, otherwise denies it.

(4) Members Management in VETAS

Once some participants in the system was later found incredible, it is important for the LAC to takes steps to prevent him/her to access the system, while when allowing new members to enlist as qualified members for threshold authorization, the system can accept the members securely and correctly. According to the criterion whether to change the master key or not, there are two strategies to manage the dynamic maintain of the membership (deletion and insertion).

(1) The first strategy is keep the master key k_0 not change, re-compute and re-distribute sub-keys k_i to each credible member. This method can be done as : in the Lagrange polynomial $f(x) = k_0 + a_1 x + a_2 x^2 + ... a_{t-1} x^{t-1}$, keep the constant k_0 as it was as its original value, and then re-computes sub-keys for each member U_i with a new different member Identity u_i', and distributes the new sub-keys to each member in the system as the secret sharing stage.

(2) The second strategy is change the master key k_0 which is not equivalent as its original value, and re-compute each new sub-keys k_i for the left credible members respectively.

For the new comer's enlistment, if enlist n_0 members in the system, then the total member will become to $n+ n_0$, thus LAC can either partially incrementally enlists n_0 members or thoroughly updates all $n+ n_0$ members in the system, obviously the complexity of the later approach is higher than the former one, whose time complexities are $O(n_0)$ and $O(n+n_0)$ respectively. However for the security and reliability when distributing sub-keys for new members it must ensure that new members have different identity from existent ones, otherwise the system will lead to failure of recover the master key.

V. Cryptoanalysis of VETAS Scheme

A. Security Assumption of the VETAS Scheme

In VETAS, a basic assumption is that only *t* out *n* members can finish co-signature for authorization, less than *t* members can't finish the work. Even there exist part incredible members, the system can still work in a secure mode. In fact, the Lagrange polynomial threshold scheme is perfect for secret sharing rather than other methods in efficiency. Another security assumption of the proposed scheme VETAS is the security of the public cryptosystem ECC, which is much more secure and efficient than any other ones, such as RSA, DSA (ElGamal).

B. Security Analysis of VETAS

In secret sharing stage, LAC controls the Lagrange polynomial f(x), LAC computes $t_i = f(u_i)$ for each members u_i, under the condition of unawareness of f(x) , u_i can't deduce other's secret share t_i.

LAC computes and broadcasts F_i to each user u_i, and each ui computes as $t_i G = \sum_{j=0}^{t-1} u_i^j F_j$ to verify whether the secret share from LAC is valid or not. The problem from F_i to deduce a_i is equivalent to the ECDLP difficulty, thus VETAS is verifiable threshold authorization scheme.

Theorem 1: In secret sharing stage, each user u_i can verify the validity of the shared secret he got from LAC by validating whether the following equation is true or not: $t_i G = \sum_{j=0}^{t-1} u_i^j F_j$.

Proof: In secret sharing stage, LAC computes $t_i = f(u_i)$ for u_i and sends it secretly to each u_i respectively. Although the identification information of each member u_i is public, however each user u_i cannot deduce t_j (j=0,…,t-1) from u_i because he(she) does not

know the Lagrange polynomial. On the other side, when u_i received t_i from LAC, to authenticate t_i from LAC, u_i computes $F_i = a_i G$ (i＝0,…,t-1) and verifies whether the formula $t_i G = \sum_{j=0}^{t-1} u_i^j F_j$ is hold or not. If the formula is hold, it manifests the secret share is valid, otherwise there must exist at least one false share. In fact, from $t_i = f(u_i)$ and $F_i = a_i G$, we can deduced:

$$\begin{aligned}\sum_{j=0}^{t-1} u_i^j F_j &= \sum_{j=0}^{t-1} u_i^j (a_j G) = \sum_{j=0}^{t-1} a_j u_i^j G = G\sum_{j=0}^{t-1} a_j u_i^j \\ &= G[k_0 + a_1(u_i) + a_2(u_i)^2 + \cdots + a_{t-1}(u_i)^{t-1}] \\ &= G[f(u_i)] \\ &= t_i G\end{aligned}$$

Thus before jointly signing by each member, each user u_i can verify the LAC's identify and keep the sub-key secretly, so the VETAS scheme is verifiable for u_i to authenticate LAC without exploring each member's own secret.

Theorem 2: After receiving the signature (r, s) of the license message m, the verifier can verify the signature by computing whether $X_e = sG - rQ = (x_e, y_e)$ and $r' = x_e \bmod n$ are hold or not to confirm the validity of the signature.

Proof: During the verification stage, according to the joint signature for license authorization stage procedure, then we have:

$$\begin{aligned}sG - rQ &= \sum_{i-0}^{t-1} s_i G - rQ = G\sum_{i-0}^{t-1} s_i - rQ = G\sum_{i-0}^{t-1} (d_i r + e k_i) \bmod n - rQ \\ &= (r\sum_{i-0}^{t-1} d_i G + e\sum_{i-0}^{t-1} k_i G) \bmod n - rQ \\ &= rG\sum_{i=0}^{t-1} a_j \prod_{\substack{j=0 \\ j\neq i}}^{t-1} \frac{u_j}{u_j - u_i} \bmod n + e\sum_{i-0}^{t-1} k_i G \bmod n - rQ \\ &= rd_0 G - rQ + e\sum_{i-0}^{t-1} k_i G \bmod n \\ &= rd_0 G - rd_0 G + e\sum_{i-0}^{t-1} X_i \\ &= X_e\end{aligned}$$

In fact, $\sum_{i=0}^{t-1} d_i = \sum_{i=1}^{t-1} a_j \prod_{\substack{j=0 \\ j\neq i}}^{t-1} \frac{u_j}{u_j - u_i} \bmod n$, where $a_j \prod_{\substack{j=0 \\ j\neq i}}^{t-1} \frac{u_j}{u_j - u_i}$ is the algebra value of Lagrange polynomial f(x), where $f(0)$=k_0.

Meanwhile, there exists $X_e = eX = e\sum_{i=0}^{t-1} X_i = (x_e, y_e)$, where x_e= ex mod n, and $(x, y) = X = \sum_{i=0}^{t-1} X_i$, so r'=r is hold, thus the signature is true.

Theorem 1 manifests VETAS scheme is verifiable, by $F_i = a_i G$ embedding the coefficient a_i of f(x) onto Elliptic Curve, therefore the secrecy of the sub-key was protected during the verification of LAC. Theorem 2 gives the security and correctness proof of VETAS scheme, in which at least *t* out of *n* qualified members can recover the shared key, less than t members can't perform the operation. During the secret sharing stage, each u_i can authenticate the share from LAC, while in the joint signature stage LAC can authenticate sub-signature from u_i, thus the proposed VETAS scheme is mutual authentication scheme. Moreover, the VETAS scheme can efficiently re-build the system once some of the members are incredible. Theorem 1, 2 prove the VETAS scheme is verifiable, efficient and secure for license authorization in digital rights management.

C. Efficiency Analysis of VETAS

The VETAS scheme is built up on Lagrange polynomial and ECC cryptosystem, which is efficient in computation and security, and can provide real time authentication and authorization service in network environment. In the same computation environment, although RSA cryptosystem can achieve fast computation speed through selecting a small public key *e* (such as e=3), however in decryption stage, for the relationship between public and private key: $ed = 1 \bmod \varphi(n)$, a smaller public key *e* lead to a larger the private key *d*, thus the computation in decryption stage will get lower than that in encryption stage. In fact, ECC is much more efficient than RSA and ElGamal algorithms. As a public performance comparison result, 160-bit ECC in security is equivalent to that of 1024-bit RSA, and as for efficiency, the computation speed of a 155-bit ECC on a 40MHZ processor can achieve 40,000 times per second which is 10 times of that for 1024-bit RSA algorithm.

D. Attacks Analysis of VETAS

(1) Membership Personation Attack

Supposing that there are t-1(or less than) participants who intend to recover the shared secret. However, the proposed VETAS scheme is based on the Lagrange Polynomial threshold approach, which is perfectly secure, that is, less than *t* qualified or unqualified members can get no information about the secret shared among the qualified participants.

Comparing with [41], in the secret sharing and joint signature stage, each user's membership is authenticated by its special space identity Midi, this condition restricts each member must work in an authentic machine and ensure he is the owner of the machine. During the message interaction stage (including secret sharing and joint signature stage) messages were transferred in cipher mode, thus membership personation attack can't work.

(2) Signature Forgery Attack

Supposing that the attacker forge a group signature, under the situation without the personal secret share t_i of u_i, the attacker may forge a random numbers t_i not related to u_i, even if he can computes $X_i = k_i G$, $s_i = (ek_i + d_i r) \bmod n$. However he will fail in the verification of $eX_i = s_i G - rQ_i$ by LAC. Otherwise, if he tries to pass the verification equation, he will encounter the difficulty of solving the elliptic curve discrete

logarithm problem. Therefore, such an attack is unworkable.

(3) Mutual-Authentication Attack

During secret sharing stage, if LAC tries to cheat some members in the system, and LAC sends false shares to the participants. When the members in the system receives the secret shares $t_i = f(u_i)$ and the broadcast messages $F_i = a_i G$

(i=1,…,n), each member can verify the validity of messages he received from LAC by the equation $t_i G = \sum_{j=0}^{t-1} u_i^j F_j$. If the messages provided by LAC are false, the above equation will not be hold.

As stated in *Membership Personation Attack*, the VETAS authenticates each member's identity via its space character to prevent personation attack in the first two stages. And thus each U_i and LAC can authenticate each other, so Mutual-Authentication is ensured to enhance the security.

As for the authorization mode, comparing Client/Server DRM, VETAS authorization provides a fairly good trial for threshold authorization which is reliable, scalable and robust, and can avoid the problem that the single-point centralized authorization server is deficient with large amount concurrent end-user for license requests or the case the server collapsed. In the (t, n) threshold authorization mode, even part of the member is absent the system can still work as usual. Once some members becomes incredible VETAS can rebuild the system efficiently which can prevent the previous members from personate as valid ones for authorization.

VI. Conclusion

Digital rights management is now becoming an important issue for international property protection, current DRM systems are centered for authorization, however they are not so reliable once the server collapsed or the systems are not authentic, to solve this problem, in this paper, a new verifiable threshold authorization scheme (VETAS) for digital rights management based on ellipse curve cryptosystem (ECC) and Lagrange polynomial is proposed and implemented for collaboration licensing management, in which authorization was decided by t-out of n authorization members, less than t members can not cooperate for license authorization, and the system can still work well when part of the members are unauthentic. The VETAS scheme works in a "mutual-authentication and threshold authorization" mode, thus each member and the license center can authenticate each other. Proof manifests the proposed VETAS scheme is secure, verifiable and reliable for digital rights management with real-time performance.

As another most important issue, secure digital content release should be taken into account, which is related to copyright mode, such as single distribution or multilevel distribution. Although this is another topic in DRM field beyond of the work in this paper, however it is important and indispensable for the whole digital rights management procedure.

Acknowledgment

The work is supported by The National Natural Science Foundation of China under Grant No. 61272519, and the National High-Tech Research and Development Plan of China under Grant No.2003AA414031, 2004AA413010.

References

[1] WIPO - World Intellectual Property Organization. [Online]. Available: http://www.wipo.int

[2] Digital Rights Management. [Online]. Available: http://www.w3.org/2000/12/drm-ws

[3] Digital Rights Management. http://www.acm.org/sigs/sigsac/ccs/CCS2003/drm.html

[4] Digital Rights Management. [Online]. Available: http://www.cse.uconn.edu/~drm2004

[5] AVS: Audio and Video Standard of China. [Online]. Available: http://www.avs.org.cn

[6] Oliveira A.L. Techniques for the creation of digital watermarks in sequential circuit designs. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2001, 20(9): 1101-1117.

[7] Kundur D., Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication. Proceedings of the IEEE Digital Rights Management. 1999, 87(7):1167-1180.

[8] Kwok S.H, Yang C.C, Tam K.Y. Watermark design pattern for intellectual property protection in electronic commerce applications. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. 2000.

[9] Feng Bao; Deng, R.H. Efficient and practical fair exchange protocols with off-line TTP.IEEE Symposium on Security and Privacy, 1998: 77-85.

[10] Waller, A.O.; Jones, G.; Whitley, T.. Securing the delivery of digital content over the Internet. Electronics & Communication Engineering Journal, 2002, 14(5): 239-248.

[11] Conrado, C.; Kamperman, F.. Privacy in an identity-based DRM system. IEEE Proceedings of 14th International Workshop on Database and Expert Systems Applications, 2003:389-395.

[12] Kundur, D.; Karthik, K.. Video Fingerprinting and Encryption Principles for Digital Rights Management, Proceedings of the IEEE, 92(6), 2004: 918–932.

[13] Iwata, T.; Abe, T.. A DRM system suitable for P2P content delivery and the study on its implementation, the 9th Asia-Pacific Conference on Communications, 2003:806-811.

[14] Andreaux, J.P., Durand, A.. Copy protection system for digital home networks. IEEE Signal Processing Magazine, 21(2), 2004: 100–108.

[15] Messerges, Thomas S. and Dabbish, Ezzat A, "Digital rights management in a 3G mobile phone and beyond". in *Proc. the 2003 ACM workshop on Digital rights management*, Washington, 2003,pp. 27-38.

[16] Bogdan C. Popescu and Bruno Crispo, "A DRM security architecture for home networks", in *Proc. the 4th ACM workshop on Digital rights management,* Washington, 2004,pp.1-10.

[17] Byers, Simon; Cranor, Lorrie; Korman, Dave; McDaniel, Patrick and Cronin, Eric, "Analysis of security vulnerabilities in the movie production and distribution process", in *Proc. the 3rd ACM workshop on Digital rights management*, Washington, 2003, pp.1-12.

[18] Reihaneh Safavi-Naini, "Import/Export in Digital Rights Management", in *Proc.* the *3rd* ACM workshop on Digital rights management, Washington, 2004, pp.99-110.
[19] Foroughi A, Albin M, Gillard S. Digital Rights Management: A Delicate Balance between Protection and Accessibility. Information Science. 2002, 28 (5): 389-395.
[20] ODRL: Open Digital Rights Language. [Online]. Available: http://www.odrl.net
[21] XrML Specifications. [Online]. Available: http://www.xrml.org/get_XrML.asp
[22] DOI: digital objcect identify, [Online]. Available: www.doi.org
[23] IBM Cryptolope (cryptographic envelope).IBM corporation [Online]. Available: http://www.ibm.com/software/security/cryptolope
[24] IBM Electronic Media Management System (EMMS). http://www.ibm.com/software/emms
[25] Microsoft Media Rights Server. Microsoft Corp [Online]. Available: http://www.microsoft.com/windows/windowsmedia/drm/default.aspx
[26] InterTrust Technologies Corp. (2002): Technology - Rights|System. http://www.intertrust.com/main/technology/index.html.
[27] RealNetworks, Inc. (2001): RealSystem Media Commerce Suite Technical White Paper. http://www.realnetworks.com
[28] EBX. [Online]. Available: http://www.pc104.com.cn/Specification/EBX.pdf
[29] Shamir, A. "How to share a secret", *in Commun. ACM*, vol.24, 1979, pp. 612–613.
[30] Blakley, G.R. "Safeguarding cryptographic keys", in *Proc. AFIPS 1979 Nat. Computer Conf*., vol. 48, 1979, pp. 313–317.
[31] A. Renvall, C. Ding, The access structure of some secret-sharing schemes, in: Information Security and Privacy, Proc. ACISP'96, Lecture Notes in Computer Science, vol. 1172, Springer, Berlin, 1996,pp. 67-78.
[32] Chunru Zhang, Kwok-Yan Lam. Sushil Jajodia. Scalable threshold closure, Theoretical Computer Science, 226 (1999) 185-206.
[33] Tompa, M., Woll, H. "How to share a secret with cheaters", *Journal of Cryptography*, Vol.30, 1994, pp. 809-810.
[34] Brickell, E.F., Stinson, D.R. "The detection of cheaters in threshold schemes", in *Proc. Advances in Cryptography-CRYPTO'88,* New York: Lecture Notes in Computer Science, 1990, pp.564-577.
[35] Pedersen T. "A threshold cryptosystem without a trusted party", in *Advances in Cryptology—EUROCRYPT'91*. UK: ROCRYPT, 1991.
[36] Li CH ,Hwang T ,Lee NY." (t, n) threshold signature schemes based on discrete logarithm", *in Advances in Cryptology—EUROCRYPT'94,* 1994.
[37] Chor, B., Goldwasser, S., Micali, S., et al. "Verifiable secret sharing and achieving simultaneity in the presence of faults", *in Proc. 26th IEEE Symposium on Foundations of Computer Science*, Washington, 1985, pp.251-160.
[38] Gennaro R, Micali S. "verifiable secret sharing as secure computation", *in Advances in Cryptology—EUROCRYPT'95,* Fance: EUROCRYPT, 1995, pp.57-63.
[39] Cramer R., Damgrd I, Nielsen J B. "Multi party computation from threshold homomorphic encryption", *in Advances in Cryptology —EUROCRYPT'01*, Australia: EUROCRYPT, 2001, pp.223- 229.
[40] Marsh M.A, Schneider F.B. "CODEX: A Robust and Secure Secret Distribution System". *IEEE Transactions on Dependable and Secure Computing*, vol.1, 2004, pp.34-47.
[41] Han Yiliang Yan Xiaoyuan Sun Jun Li Delong. "Verifiable Threshold Cryptosystems Based on Elliptic Curve". *in Proc. 2003 International Conference on Computer Networks and Mobile Computing*, 2003, pp.116-119.
[42] Chen, Tzer-Shyong. "A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem", *Computer Standards and Interfaces*, vol.27, 2004, pp.33-38.
[43] Markus A. Stadler. "Publicly Verifiable Secret Sharing", New York: Lecture Notes in Computer Science, Vol.1070, 1996, pp. 190.
[44] W. Mao, "Guaranteed Correct Sharing of Integer Factorization with Offline Shareholders", *in Proc. Public Key Cryptography,* 1998, pp.27-42.
[45] Fabrice Boudot, Jacques Traore. "Efficient Publicly Verifiable Secret Sharing Schemes with Fast or Delayed Recovery", New York: Lecture Notes in Computer Science, Vol.1726, 2004, pp.87-102.
[46] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation. 1987(48): 203– 209.
[47] Miller V.S. Use of Elliptic Curve in Cryptography [C]. Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science, Spring-Verlag, 1986, 218: 417-426.
[48] ANSI X9.62. Public Key Cryptography for the Finacial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).1999.
[49] *Digital Signature Standard.* Federal Information Processing Standards Publication 186-2. [Online]. Available: http://csrc.nist.gov
[50] I*EEE P1363. Standard Specifications for Public-Key Cryptography*. IEEE. Standard P1363, 2000.
[51] Wang Yuming, Liu Jianwei. "Security of Telenetwork: Theory and Technology (in Chinese)".Xi'an: Xidian press, 1999.
[52] Huang, Feng; Qu, Xilong. "Design of image encryption algorithm based on compound two-dimensional maps". *Journal of Software*, Vol.6, pp. 1953-1960, 2011
[53] Lu, Yang; Li, Jiguo. "Generic construction of forward-secure identity-based encryption". *Journal of Computers*, Vol.7, pp. 3068-3074, 2012
[54] Schneier B. "Applied Cryptography-Protocols, Algorithm and Source Code in C", 2nd edition, New York: John Wiley & Sons Inc., 1996.
[55] A. Menezes, P. van Oorschot, and S. Vanstone. "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.
[56] Hu, Liang; Liu, Zheli; Cheng, Xiaochun. "Efficient identity-based broadcast encryption without random oracles". *Journal of Computers*, Vol.5, pp. 331-336, 2010
[57] Wu, Qing; Wang, Wenqing. "New identity-based broadcast encryption with constant ciphertexts in the standard model". *Journal of Software*, Vol.6, pp. 1929-1936, 2011
[58] Kwok Yan Lam, Francesco Sica. "The Weight Distribution of C_5 (1, n)". *Designs, Codes and Cryptography*, Vol. 24, pp. 181-191, 2001.
[59] Lam, Kwok-Yan; Chung, Siu-Leung; Gu, Ming; Sun, Jia-Guang. "Security middleware for enhancing interoperability of Public Key Infrastructure", *Computers and Security,* Vol.22, June, pp.535-546, 2003.