Threshold Signatures: Current Status and Key Issues

Min-Shiang Hwang[1] and Ting-Yi Chang[2]
(Corresponding author: Min-Shiang Hwang)

Department of Management Information Systems, National Chung Hsing University[1],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C. (Email: mshwang@nchu.edu.tw)
Department of Computer and Information Science, National Chiao Tung University[2],
1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.

(Invited Paper)

Abstract

In this paper, we survey all related threshold signature schemes and classify them with different properties. In order to compare them with different properties, we image there is an ideal threshold signature scheme which satisfies all requirements of threshold signature schemes. Based on this ideal threshold signature, readers can easily to understand what the next generation of threshold signature schemes is and attempt to propose it.

Keywords: Authenticated encryption scheme, cryptography, factoring and discrete logarithm, message recovery, security

1 Introduction

Paper work is rapidly being replaced as e-mail, electronic commerce, electronic money, etc. become more and more widespread. In many of these new forms of communication, a digital signature is essential. Digital signatures have become more and more important in modern electronic society because they can offer such properties as integrity and authentication. Integrity guarantees that a message being transferred never gets corrupted, and authentication guarantees that the signer cannot be impersonated. Traditional digital signatures, such as RSA [2, 5, 27, 52] and DSA [25, 26, 46], only allow a single signer to sign a message, and anyone can verify the signature at any time. However, there are growing and growing numbers of times when a message needs to be signed by a set of signers and for distributing the power of a single authority. Multisignature schemes [19, 47, 48] and threshold signature schemes have thus been designed to solve such problems.

There are two major differences between threshold signature schemes and multisignature schemes. Firstly, in multisignature schemes, it is not necessary to restrict the number of signers to generate a valid signature, while in threshold signature schemes, it is necessary to predetermine the threshold value t so that at least t participants in the group can collaborate to generate a valid signature on behalf of the group, but only $t-1$ or fewer participants will not be enough. Secondly, a threshold signature represents a signature is signed by the group, while a multisignature represents a set of individuals who sign the message.

Until now, the threshold signature schemes have been developed about twelve years. Many kinds of threshold signature scheme to reach different requirements are studied. However, some papers are published at the same time but they did not refer to each other. In Figure 1, We first classify them according to *ElGamal-type* (*discrete logarithm problem*), *RSA-type* (*factorization problem*), and *Elliptic curve ElGamal-type* (*elliptic curve discrete logarithm problem*). According to different requirements, we classify them by *With undeniable*, *With traceability/untraceability*, *With* (k, l) *shared verification*, and *With distinguished signing authorities*.

(t, n) Threshold Signature
In 1987, Desmedt [13] first presented the concept of group-oriented cryptosystem for secure communications among groups. The concept of group-oriented cryptosystem [14] can be applied to threshold signature schemes. In 1991, Desmedt and Frankel [15] first proposed a group-oriented (t, n) threshold digital signature scheme based on RSA system and secret sharing scheme [53], which brings the basic requirement as follows:

- At least t participants in the group can collaborate to generate a valid signature on behalf of the group signature.
- Any one who plays the role of a verifier can use the group's public key to verify the group signature without identifying the identities of the signers.

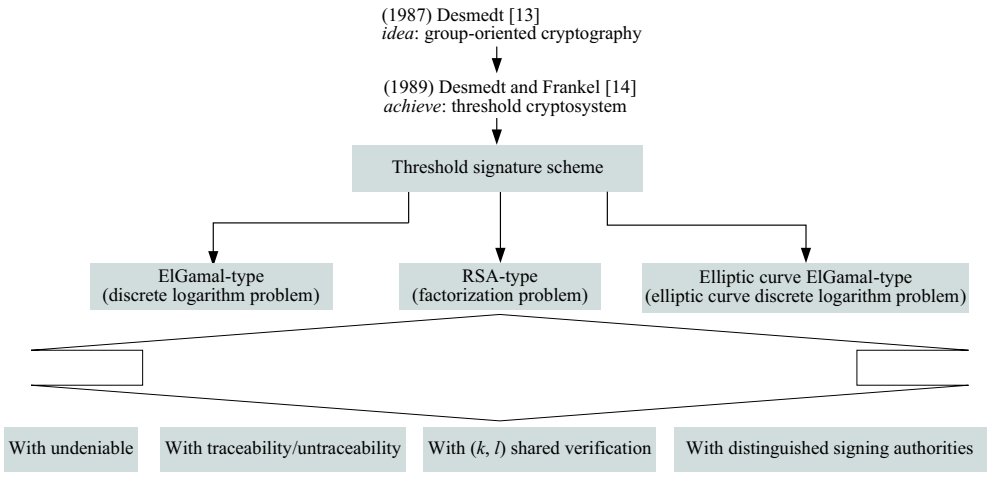

Figure 1: The classification of threshold signature schemes

Later, Li et al. [35] have pointed out that t or more malicious participants can mount the conspiracy attack to reveal the system secret and then forge the signature without taking any responsibility. And then many papers tried to use different cryptographic techniques to propose a threshold signature. Those schemes showed in Figure 1 only satisfies the basic requirement.

Based on ElGamal-type (discrete logarithm problem) in Figure 2, in 1994, Harn [20] combined Shamir's perfect secret sharing scheme and the modified ElGamal signature [1] to accomplish a (t, n) threshold signature scheme. By the property of Lagrange polynomials, the group's secret key is distributed into n different shares (shadows) to each participant. Any t or more participants can use their shares to generate their individual signatures. Then any participant may be randomly selected as a designated clerk who is responsible for the verification and computation of the group signature by using the Lagrange interpolating polynomial. The security of both the individual signature and group signature is based on the discrete logarithm problem (DLP). Later, Horster et al. [22], Lee and Chang [33], and Michels and Horster [43] pointed out that the forgery attack is successfully to break Harn's scheme, respectively. On the other hand, Park and Kurosawa [49] proposed the threshold signature scheme for a variant of ElGamal signature and Miyazaki and Sakurai [45] proposed threshold Nyberg-Rueppel type signature and signature sharing. The signature sharing is another group-oriented signature technique in which only one signer issues the signature and then he/she distribute it among n signature holders. In 2003, Wu and Hsu [64] proposed a threshold signature scheme using self-certified public keys. Unlike the previous proposed schemes, they belongs to certificate-based public key systems. Certificate-based public key systems do not require the extra communication costs for transmitting public key certificates, computational efforts for verifying public key, and space storage for storing certificates as those needed in certificate-based systems. In 2005, Shao [54] proposed an improvement on the Wu-Hsu scheme, which signature computation and verification are more efficient than that of the Wu-Hsu scheme.

Based on RSA-type (factorization problem) in Figure 2, in 2003, Liu et al. [40] proposed a threshold GQ [18] signature scheme, which is also based on the assumption that computing e-th root modulo a composite is infeasible without knowing the factor.

Based on Elliptic curve ElGamal-type (elliptic curve discrete logarithm problem) [28] in Figure 2, in 2001, Miyazaki and Takaragi [44] proposed a threshold signature scheme. Due to the advantages of elliptic curve cryptography, their scheme can easily be implemented for a smart card. In 2003, Wu et al. [66] pointed out that the Miyzazki-Takaragi scheme cannot withstand the forgery attack and proposed an improved version of their scheme. Recently, Chen et al. [9] also propose a threshold signature based on ECDLP. However, his scheme doesn't refer other threshold signature schemes and does less well than before. For example, any t or more malicious participants can mount the conspiracy attack to reveal the system secret key and then forge the signature without taking any responsibility. Recently, Cheng et al. [12] and Su et al. [55] agreed by mere coincidence to proposed an ID-based threshold signature scheme based on ECDLP. The user's public key in ID-based public key systems is simple such as name, address, etc., which can be used to uniquely identify him and is undeniably associated with him. Similar to self-certified public key systems, ID-based systems outperform certificated-based system in term of communication costs, computation efforts, and space storage. Compared with ID-based public key, self-certified public key can provide more security confidence.

(t, n) Threshold Signature with Undeniable

Undeniable signature [7] is a special kind of digital signature in the sense that the validity of an alleged signature cannot be verified without the cooperation of the signer. Since in such schemes the verifiability of signatures is only

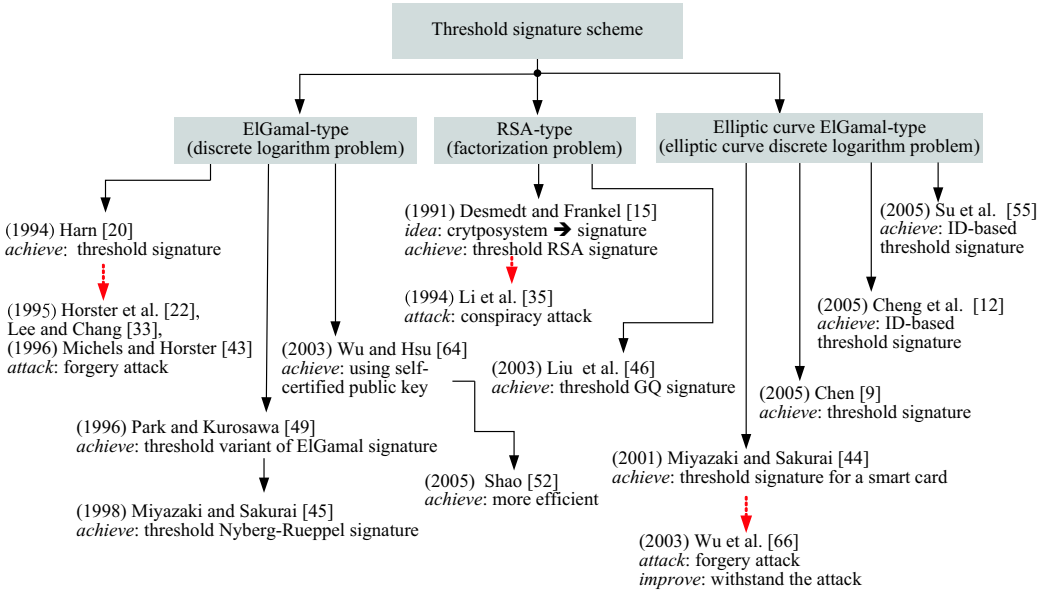

Figure 2: Classify with various signature schemes

limited to designated verifiers, undeniable signatures have been suggested to construct electronic commerce schemes, and fair exchange protocols etc. If the signature is indeed signed by signer, the signer cannot deny it.

Based on the undeniable signature, a (t, n) threshold undeniable signature scheme has the following requirement:

- At least t participants in the group can collaborate to generate a valid signature on behalf of the group signature.
- But without the cooperation of t members, a verifier cannot verify the validity of an alleged signature even if he knows group public key.

Based on ElGamal-type (discrete logarithm problem) in Figure 3, in 1992, Harn and Yang [21] designed two threshold undeniable signature schemes: $(1, n)$ scheme and (n, n) scheme. However, Langford [30] pointed out any two adjacent members can generate a valid threshold signature on any message in their (n, n) scheme. Later, Lin et al. [39] presented a general (t, n) threshold undeniable signature scheme, but it is also subjected to Langford's attack. To overcome Langford's attack, Lee and Hwang [31] constructed two threshold undeniable signature schemes with a trusted center by naturally generalizing Chaum's zero-knowledge undeniable signature [6] to group-oriented environment. In 2004, Wang [62] showed that the Lee-Hwang scheme suffers from the insider forgery attack, in which one dishonest member (maybe colluding with a verifier or the designated combiner) can get a valid signature on any chosen massage, and another attack allows a dishonest member to prevent honest members from generating valid signatures.

Based on RSA-type (factorization problem) in Figure 3, Wang et al. [61] and Lu et al. [41] proposed a threshold signature scheme based on Gennaro et al.'s undeniable RSA signature scheme [17] in 2005.

(t, n) Threshold Signature with Traceability/Untraceability

In 1994, Li et al. [36] considered a situation for a (t, n) threshold signature scheme. If t or more participants in the group act in collude, then they can impersonate any other set of participants to forge signatures. The malicious set of signers does not have to take any responsibility for the forged signatures and thus encourages collusion. Based on ElGamal-type (discrete logarithm problem) in Figure 4, in order to trace back to find the signers, they combine the idea of multisignature schemes with the (t, n) threshold signature to propose a (t, n) threshold-multisignature scheme. Here, In order to explain the property of traceability, the (t, n) threshold-multisignature is called as (t, n) threshold signature with traceability in our paper, which has the following requirement:

- At least t participants in the group can collaborate to generate a valid signature on behalf of the group signature.
- The individual signatures generated by the participants can be verified by a designated combiner (or a clerk) before they combined into a group signature.
- Any one who plays the role of a verifier can use the group's public key to verify the group signature without identifying the identities of the signers.

Obviously, their scheme is dependent on the designated combiner to know that who collectively generate the group signature by verifying the individual signatures. However, Michels and Horster [43] pointed out that the

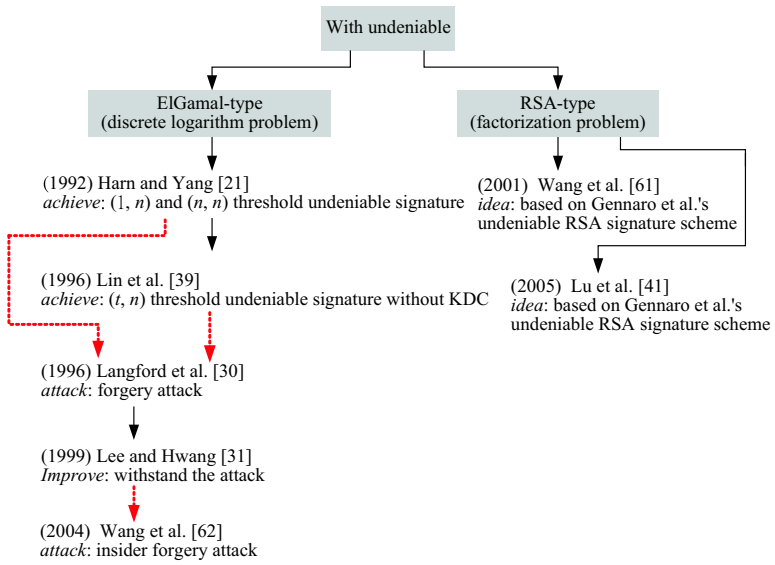

Figure 3: Classify with undeniable

signer cannot make sure who his co-signers. This weakness violates the property of traceability. In 2000, Li et al. [34] further proposed a (t, n) threshold-multisignature scheme, but Wang [59] showed that the same weakness as in [36].

We have mentioned that Harn's [20] suffer the conspiracy attacks by revealing the group secret key [36]. In order to withstand those attacks, Wang et al. [60] proposed two (t, n) threshold signature schemes with and without the SDC. Later, Tseng and Jan [57] mounted the forgery attack on their schemes, which is any attacker can generate a valid group signature for any message without knowing any secret keys of members in a group. Furthermore, Li et al.'s attack [37] is more fundamental than Tseng-Jan's attack in the sense that it cannot be recognized or blocked at the designated clerk level of the signature schemes.

On the other hand, in 2001, Li et al. [38] also proposed two (t, n) threshold signature schemes with and without the SDC. But, Wu and Hsu [65] showed that their scheme suffers from the forgery attack and cannot achieve the property of traceability if a clerk is malicious.

Based on RSA-type (factorization problem) in Figure 4, in 2000, Lee et al. [32] proposed a (t, n) threshold signature scheme with untraceability and can be augmented to give the original signers the ability to prove that they are the true signer. In 2004, Chang et al. [4] combined their scheme by using the extend Euclidean algorithm to achieve the (k, l) shared verification (we will introduce later) and provided both traceability mode and untraceability mode for participants to choose from.

In our viewpoint, the designated combiner (clerk) should be honest and he/she not only has the responsibility for verifying the individual signatures by each participant's public key (or identity) but also has the responsibility for informing who cooperatively generate the group signature. For example, the clerk can create a public notice board which is used for storing who signs the message. Anyone who wants to know that signer's identity, he/she can access those information on the board. The contents on the board can only be modified or updated by the clerk.

(t, n) Threshold Signature with (k, l) Shared Verification

Consider a situation, where the documents between business entities need to be signed and verified. That is, the documents will not be exposed to any outsider. For example, when two companies have to communicate with each other, some specified signers may have to sign certain documents according to their positions in the company, and some special verifiers may be assigned to check on these signatures. In addition, there are usually confidential data that need to be encrypted or decrypted by some specified participants. A threshold signature with (k, l) shared verification has the following requirement:

- The (t, n) threshold signature on behalf of the signing group should be able to be verified by (k, l) threshold-shared verification on behalf of the verifying group.
- At least k participants in the group can collaborate to verify a valid signature on behalf of the verifying group, but only $k - 1$ or fewer participants will not be enough.

Based on ElGamal-type (discrete logarithm problem) in Figure 5, in 2000, Wang et al. [59] have proposed two schemes: the (t, n) threshold signature with (k, l) threshold-shared verification and the (t, n) threshold-authenticated encryption with (k, l) threshold-shared verification. In their schemes [59], the share distribution center (SDC) is responsible for dividing the signing group's and verifying group's secret keys into n and l different shadows and the associating the groups' and participants'

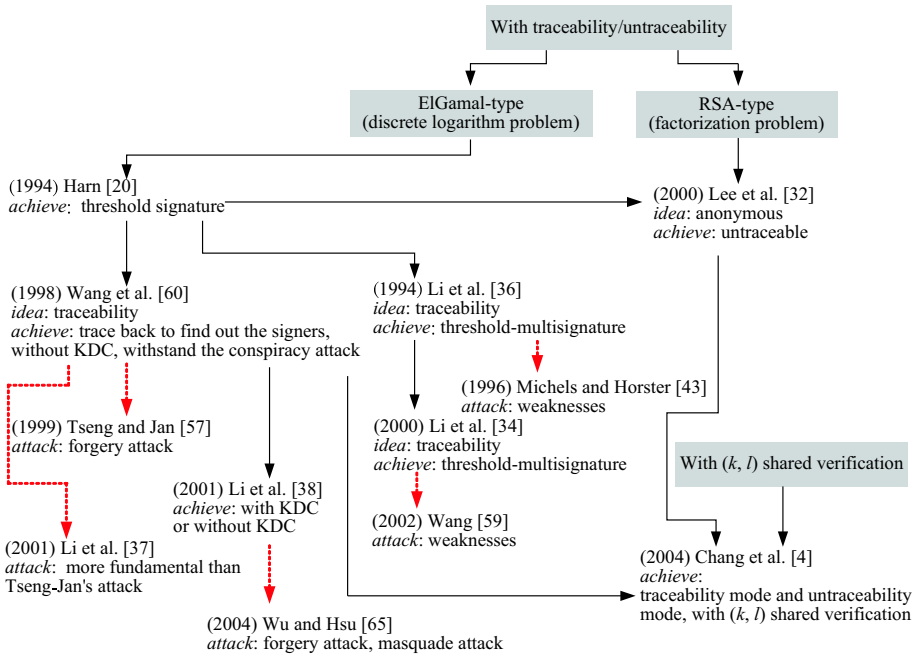

Figure 4: Classify with traceability/untraceability

public keys to the individual groups and participants, respectively. By using the Lagrange interpolation formula, t participants in the signing group and k participants in the verifying group have the ability to compute a common session key shared between the two groups by using their shadows and the opposite group's public key. The common session key is used to ensure the communication between the two groups. Any t or more participants in the signing group can use their shadows to generate their individual signatures and hand over these individual signatures to a clerk. Then, the clerk can verify theses individual signatures and combine these t valid individual signatures to generate a threshold signature on behalf of the signing group. On the other hand, any k or more participants in the verifying group have the ability to collaborate to verify the threshold signature.

Unfortunately, Hsu et al. [23], Tseng et al. [58], Wang et al. [63] separately proved that Wang et al.'s schemes are not robust enough against forgery and that something is wrong with the verification of threshold signatures because the common session keys are the same for different threshold signature. Anyone can obtain the signing group's secret key from two valid threshold signatures. They separately proposed improved schemes on Wang et al.'s schemes.

Based on Elliptic curve ElGamal-type (elliptic curve discrete logarithm problem) in Figure 5, in 2004, Chang et al. [3] pointed out that Hsu et al.'s improved scheme has the following disadvantages in practice.

1) The SDC must take part in the generation of each individual signature and threshold signature as well as the distribution of fresh session keys to all the participants.

2) Because the numbers of the secret keys are different in two groups, the signing group and the verifying group cannot exchange their roles with each other.

3) The SDC must initialize the system and generate the parameters.

4) High computational complexities to compute discrete logarithm problem.

Their scheme not only can live up to the requirements an ideal (t, n) threshold-authenticated encryption scheme with (k, l) threshold-shared verification should but also can get rid of the disadvantages mentioned above. Hence, Their scheme is more practical and efficient in real-world applications than Hsu et al.'s scheme. They brought up the new additional requirements as follows:

- The SDC is necessary in the scheme.
- The signing group and the verifying group can exchange their roles with each other.
- The signing group can determine which members in the verifying group can cooperatively verify the signature, not only restrict on the threshold value k.

At the same time, Chen et al. [8] and Chen [11] separately proposed an improved on Hsu et al.'s scheme. In [3], [8] and [11], the threshold signature is generated by t members in the group and then the clerk encrypt the message singed by t members in the group. When the verifying group receives the ciphertext, at least k members in the verifying group must cooperatively decrypt it and then verify the signature with the plaintext. To be mentioned, [3] the process of encryption in their scheme is

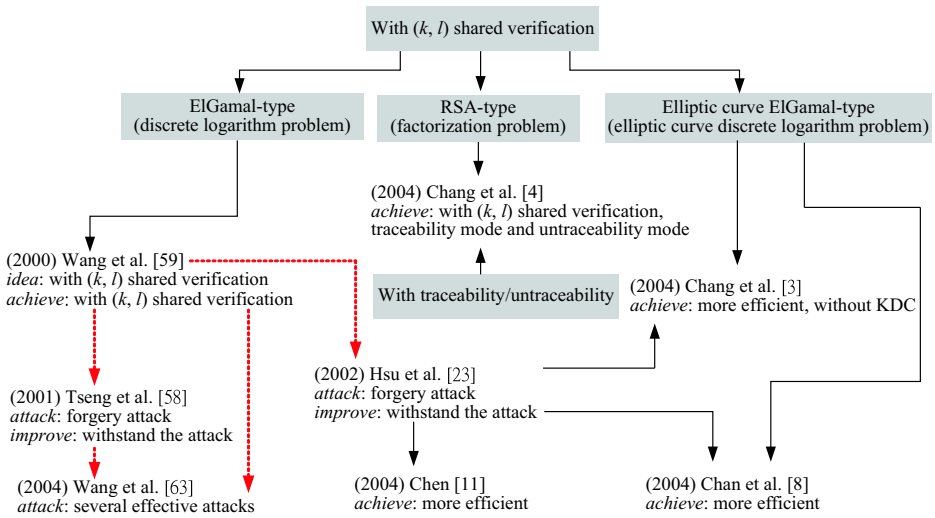

Figure 5: Classify with (k, l) shared verification

based on [67]. The members in the verifying group can be designated by using the designated members' public keys. In fact, three schemes belong to authenticated encryption scheme. However, in [8] and [11], SDC is needed and the threshold value k is fixed.

(t, n) Threshold Signature with Distinguished Signing Authorities

In most of the threshold signature schemes we introduced before, all discretionary signatories must sign the whole document for constructing a valid group signature. For the sake of labor division and responsibility-sharing inherent in the group works, every discretionary signatory within the group might be required to sign or read the partial document instead of the whole document in certain applications. A (t, n) threshold signature with distinguished signing authorities has the following requirement.

- The signing document can be divided into any t smaller subdocuments in such a way that each subdocument is meaningful and will be signed as a unit by one discretionary signatory.
- Every signatory has the same knowledge domain that covers the subjects within the signing document.

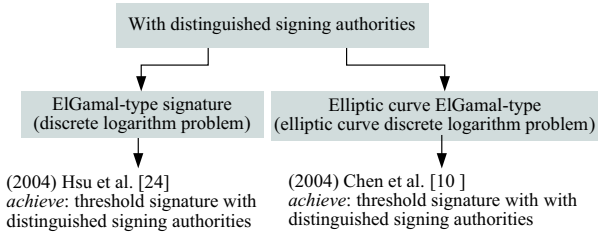

Figure 6: Classify with distinguished signing authorities

Based on ElGamal-type (discrete logarithm problem) in Figure 6, in 2004, Hsu et al. [24] gave the idea into a threshold signature. At the same time, based on Elliptic curve ElGamal-type (elliptic curve discrete logarithm problem) in Figure 6, Chen et al. [10] proposed a (t, n) threshold signature with distinguished signing authorities and provides authenticated encryption.

The remainder of this paper is organized as follows. In Section 2 , we introduce the related works. The first threshold signature scheme proposed by Desmedt and Frankel is reviewed. Then, we go over Chang et al.'s schemes, which are the least papers and give us the comments to develop an ideal threshold signature scheme. In Section 3, we shall give the comparisons in term of requirements, security analysis, performance. Finally, in Section 4 and 5, we conclude thesis and indicate some future research directions, respectively.

2 Related Works

We have introduced the some requirements for a threshold signature in Section 1. In the following sections, we review Desmedt and Frankel's scheme [15], which is the first proposed. For the (t, n) threshold signature schemes with (k, l) shared verification and (t, n) threshold signature schemes with Traceability/Untraceabilit, we review Chang et al.'s schemes [3, 4], which are the latest issues for the above two topics.

2.1 Desmedt and Frankel's (t, n) Threhsold Signature

Before reviewing the first threshold signature proposed by Desmedt and Frankel. We need to know that how the secret shares (shadows) hold by every participant can be combined into the group secret key? All the threshold-related schemes are based on the Shamir's secret sharing scheme [53]. Here, we first show that the process of Shamir's secret sharing scheme in advance.

Shamir's secret sharing scheme
An uni-variate polynomial $y = f(x)$ of degree $t-1$ is uniquely defined by t points (x_i, y_i) with distinct x_i. Let $s = f(0)$ be the secret to be shared and $x_1, x_2, \cdots, x_n$ be n distinct numbers which are publicly known to everyone. Then the secret holder (dealer) delivers secret shares $y_1, y_2, \cdots, y_n$ to every participant over a secret channel. At least t participants are enough to use the Lagrange interpolating polynomial to recover the secret. With the knowledge of the set of t points (x_i, y_i), the $t-1$ degree polynomial $f(x)$ can be uniquely determined as

$$f(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j}$$

Since $s = f(0)$, the shared secret can be expressed as

$$s = f(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{0 - x_j}{x_i - x_j}$$

The notation $G_s = \{u_{s1}, u_{s2}, \cdots, u_{sn}\}(|G_s| = n)$ is defined as the signing group of n signers and $g_s(|g_s| = t \leq n)$ as any subset of t signers. Desmedt and Frankel's scheme can be divided into three phases: (1) parameters generating phase, (2) individual signature generating phase, and (3) threshold signature generating and verifying phase. In the parameters generating phase, the SDC generates the following system parameters:

$N = p \times q$	for p and q to be safe primes, let $p = 2p' + 1$ and $q = 2q' + 1$ where p', q' are primes. (N is public and p, q, p', q' are secret)
$\lambda(N)$	λ is the Carmichael.
d	the group secret key is an odd number d which is randomly chosen such that $\gcd(d, \lambda(N))$=1.
e	the group public key is e such that $ed = 1 \bmod \lambda(N)$.
$f(x)$	is a $t-1$ degree polynomial such that $f(0) = d - 1$.
x_{si}	is a public value for each u_{si}.

Then, the SDC distributes to each $u_{si} \in G_s$ a public integer x_{si} and a secret share K_{si}:

$$K_{si} = \frac{f_s(x_{si})/2}{[\prod_{\substack{j\in G_s \\ j\neq i}} (x_{si} - x_{sj})]/2} \bmod p'q' \qquad (1)$$

, where all the x_{si}'s are odd and all $f(x_{si})$'s are even.

In the individual signature generating phase, assume that t participants in $g_s \in G_s$ are to sign a message m. Each $u_{si} \in g_s$ generates a modified share $a_{i,g_s} = K_i \cdot (\prod_{j\in G_s, j\notin g_s}(0 - x_{sj}) \prod_{j\in gs, j\neq i}(x_{si} - x_{sj}))$ and then uses it to compute the signature $s_{m,i,g_s} = m^{a_{i,g_s}} \bmod n$.

In the threshold signature generating and verifying phase, a clerk combines those individual signatures s_{m,i,g_s} to create threshold signature $S_m = m \cdot \prod_{i\in g_s} s_{m,i,g_s} = m \cdot m^{d-1} = m^d \bmod n$. The receiver of S_m can check the correctness of S_m by verifying $m \stackrel{?}{=} (S_m)^e \bmod n$.

2.2 Chang et al.'s (t, n) Threhsold Signature with Traceability/Untraceability and (k, l) Shared Verification

The notation G_v ($|G_v = l|$) is defined as the verifying group of l verifiers and $g_v(|g_v| = k \leq l)$ as any subset of k verifiers in G_v. Their scheme consists of three phases: (1) parameters generating phase, (2) individual signature generating and verifying phase, and (3) threshold signature generating and verifying phase. In the parameters generating phase, the SDC generates the following system parameters:

$N, p, q, p', q', \lambda(N)$	are the same as those in Section 2.1.
W	is a public number such that $\gcd(W, \lambda(N)) = 1$.
α	is a secret primitive in both GF(p) and GF(q).
a, b, c, d	a and b are two numbers such that $\gcd(a, b) = 1$, and there are must be exactly two integers c and h such that $a \cdot c + b \cdot h = 1$ by the extended Euclidean algorithm[42].
$f_s(x) \bmod \lambda(N)$	is a $t-1$ degree polynomial such that $f_s(0) = d \cdot a \cdot c$ and $\gcd(d, \lambda(N)) = 1$.
$f_v(x) \bmod \lambda(N)$	is a $k-1$ degree polynomial such that $f_s(0) = d \cdot b \cdot h$.
x_{si}	n public and odd integers x_{si} with even $f_s(x_{si})$ for each participant $u_{si} \in G_s$.
x_{vi}	l public and odd integers x_{vi} with even $f_v(x_{vi})$ for each participant $u_{vi} \in G_v$.
$S = \alpha^d \bmod N$	is a G_s's secret key.
$Y = \alpha^{dW} \bmod N$	is a G_s's public key.
$H(\cdot)$	is a public collision-free one-way hash function.

Then, the SDC distributes to each $u_{si} \in G_s$ a secret key K_{si} and to each $u_{vi} \in G_v$ a secret key K_{vi}:

$$K_{si} = \alpha^{s_i} \bmod N, \quad \text{where } s_i = \frac{f_s(x_{si})/2}{[\prod_{\substack{j\in G_s \\ j\neq i}} (x_{si} - x_{sj})]/2} \bmod p'q'. \qquad (2)$$

$$K_{vi} = \alpha^{v_i} \bmod N, \quad \text{where } v_i = \frac{f_v(x_{vi})/2}{[\prod_{\substack{j\in G_v \\ j\neq i}} (x_{vi} - x_{vj})]/2} \bmod p'q'. \qquad (3)$$

The associated y_{si} for each $u_{si} \in G_s$:

$$y_{si} = \alpha^{-s_i \cdot W} \bmod N, \quad \text{where } s_i = \frac{f_s(x_{si})/2}{[\prod_{\substack{j\in G_s \\ j\neq i}} (x_{si} - x_{sj})]/2} \bmod p'q'.$$

In the individual signature generating and verifying phase, assume that t participants $u_{si} \in g_s$ are to sign a message m. Each u_{si} randomly chooses an integer r_{si} with $0 < r_{si} < N$, and computes $p_{si} = r_{si}^W \bmod N$. Then, u_{si} broadcasts p_{si} to the other $t-1$ participants in g_s. Once each u_{si} receives u_{sj} ($j = 1, 2, \cdots, t$ and $j \neq i$), she/he computes $P_s = \prod_{i \in g_s} p_{si} \bmod N$, $e = H(P_s, m)$, and $e_i = H(p_{si}, m)$. Then, each u_{si} uses her/his secret key K_{si} to generate her/his individual signature z_{si}:

$$z_{si} = r_{si} \cdot K_{si}^{\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \bmod N$$

After receiving (e, e_i, z_{si}, m), the clerk uses u_{si}'s public key y_{si} to compute a value $\widetilde{p_{si}}$

$$\widetilde{p_{si}} = z_{si}^W \cdot y_{si}^{\prod_{\substack{j \in G_s \\ j \notin g_s}} (x_{si} - x_{sj}) \cdot \prod_{\substack{j \in g_s \\ j \neq i}} (0 - x_{sj}) \cdot e} \bmod N$$

and checks $e_i \stackrel{?}{=} H(\widetilde{p_{si}}, m)$. If it holds, the individual signature z_{si} on the message m is valid. So the individual signature verifying mechanism is put into the individual signature-generating phase. If the signers would like to anonymous, the values e_i and $\widetilde{u_{si}}$ are omitted.

In the threshold signature generating and verifying phase, the clerk computes the threshold signature $Z_s = \prod_{i \in g_s} z_{si} \bmod N$. the threshold signature $\{e, Z_s\}$ of the message m is transmitted to G_v. To verify the group signature, any k out of the l verifiers in G_v should cooperate to authenticate the validity of the signature. Without loss of generality, assume that there are k participants $u_{v1}, u_{v2}, \cdots, u_{vk}$ in g_v. Each u_{vi} randomly chooses an integer r_{vi} with $0 < r_{vi} < N$ and computes $p_{vi} = r_{vi}^W \bmod N$ and z_{vi}

$$z_{vi} = r_{vi} \cdot K_{vi}^{\prod_{\substack{j \in G_v \\ j \notin g_v}} (x_{vi} - x_{vj}) \cdot \prod_{\substack{j \in g_v \\ j \neq i}} (0 - x_{vj}) \cdot e} \bmod N$$

Then, each u_{vi} transmits u_{vi} and z_{vi} to a clerk who can be randomly chosen from G_v to compute $P_v = \prod_{i \in g_v} p_{vi} \bmod N$ and $Z_v = \prod_{i \in g_v} z_{vi} \bmod N$. Afterwards, the threshold signature can be verified by using G_s's public key Y to compute a value $\widetilde{P_s} = (Z_s \cdot Z_v)^W \cdot (P_v)^{-1} \cdot Y^e \bmod N$. If Equation $e \stackrel{?}{=} H(\widetilde{U_s}, m)$ holds, the threshold signature $\{e, Z_s\}$ on the message m is valid.

2.3 Chang et al.'s (t, n) Threhsold Signature with (k, l) Shared Verification

We know that the threshold-related schemes are based on Shamir's secret sharing scheme, but how to remove the dealer in the secreting sharing? If the dealer can be removed in the system and the participants can cooperatively construct a common secret, then SDC can be also removed in the threshold signature schemes. Here, we first introduce Pedersen's distributed key generation scheme [51], which is based on verifiable secret sharing [16, 50].

Pedersen's distributed key generation scheme
Here, we use the same notations G_s, g_s, and u_{si} are the same as those in the above sections. Assume that each $u_{si} \in G_s$ want to construct a common secret without any dealer. Two large prime numbers p and q, where $q|p-1$, and a generator g of order q in $GF(p)$. Each u_{si} has a public integer x_i. Each u_{si} performs the following steps.

Step 1. Randomly choose a $(t-1)$th degree polynomial $f_i(x)$ over Z_q such that $f_i(x) = f_{i,0} + f_{i,1}x + \cdots + f_{i,t-1}x^{t-1}$, where $f_i(0) = f_{i,0} = d_i$.

Step 2. Send $y_{ij} = f_i(x_j)$ to u_{sj} ($\forall j \neq i$) in G_s secrectly and broadcast $g^{f_{i,l}}$ ($l = 1, 2, \cdots, t-1$) to all the others.

Step 3. Verify y_{ij} received from u_{sj} by checking $g^{y_{ij}} \stackrel{?}{=} \prod_{l=0}^{t-1} (x_j)^l \cdot (g^{f_{i,l}})$.

Let f be the polynomial $f(x) = f_1(x) + f_2(x) + \cdots + f_n(x)$ over Z_q. By constructing the share $y_i = \sum_{j=1}^{n} f_j(x_i)$, the common secret $d = \sum_{i=1}^{n} d_i$ the shared secret can be expressed as

$$d = f(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{0 - x_j}{x_i - x_j}.$$

The following are the notations used in Chang et al.'s scheme.

ID_{si}/ID_{vi}	are the identity of u_{si} and u_{vi}, respectively.
E	is an elliptic curve.
p	is an odd prime number.
F_p	is a finite field of p element.
α	is a base point on E.
q	is an order of α in E, which is an odd prime.

The scheme is comprised of four phases: (1) key generation phase, (2) individual signature generating and verifying phase, (3) threshold signature generating and encrypting phase, and (4) decrypting and threshold signature verifying phase.

In the key generation phase, each u_{si} in G_s and each u_{vi} in G_v to generate his/her private key, public key, and group public key. Each u_{si} in G_s performs the following steps:

Step 1. Randomly choose an integer d_{si}.

Step 2. Randomly choose a $(t-1)$th degree polynomial $f_{si}(x)$ over Z_q such that $f_{si}(x) = f_{si,0} + f_{si,1}x + \cdots + f_{si,t-1}x^{t-1}$, where $f_{si,0}, f_{si,1}, \cdots$, and $f_{si,t-1}$ are in Z_q. And $f_{si}(0) = f_{si,0} = d_{si}$. Then, send $f_{si}(ID_{sj})$ to u_{sj} ($\forall j \neq i$) in G_s over a secret channel and broadcast the check values $f_{si,l} \cdot \alpha_s$ ($l = 1, 2, \cdots, t-1$) to all the other participants in G_s.

After receiving $f_{si}(ID_{sj})$ from u_{si}, each u_{sj} verifies the validity of it by checking $f_{si}(ID_{sj}) \cdot \alpha \stackrel{?}{=} \sum_{l=0}^{t-1}(ID_{sj})^l \cdot (f_{si,l}\alpha_s)$. If it does not hold, reject u_{si}. Otherwise, each participant in G_s continues to perform the following steps.

Step 3. Compute his/her private key

$$K_{si} = \sum_{j=1}^{n} f_{sj}(ID_{si}) \tag{4}$$

Step 4. Compute G_s's public key $Q_s = \sum_{j=1}^{n} f_{sj,0} \cdot \alpha$ and his/her public key $Q_{si} = K_{si} \cdot \alpha$.

Similarly, each u_{vi} in G_v performs the above steps. The result of performing those steps is listed in the following: $K_{vi} = \sum_{j=1}^{l} f_{vj}(ID_{vi})$ and $Q_{vi} = K_{vi} \cdot \alpha$ are separately u_{vi}'s private key and public key; And $Q_v = \sum_{j=1}^{l} f_{vj,0} \cdot \alpha$ is G_v's public key.

In the individual signature generating and verifying phase, assume that t participants $u_{s1}, u_{s2}, \cdots, u_{st}$ in g_s are to sign a message m. Each u_{si} performs the following steps.

Step 1. Compute a value $e_{si} = K_{si} \cdot a_{si}$, where $a_{si} = \prod_{\substack{j \in G_s \\ j \neq i}} \frac{ID_{sj}}{ID_{sj} - ID_{si}}$.

Step 2. Randomly choose an integer w_i, where $1 \leq w_i \leq q-1$. Then, compute $R_{si} = w_i \cdot \alpha$ and broadcast it to the other participants in g_s. Compute a point $(X, Y) = \sum_{i \in g_s} R_{si} = \sum_{i \in g_s} w_i \cdot \alpha$.

Step 4. Compute the individual signature $\{r, s_i\}$ as $r = X - h(m) \bmod q$, $s_i = e_{si} \cdot r + w_i \bmod q$. To verify the correctness of the individual signature s_i, a participant may be randomly selected from G_s as a designated clerk. Except for verifying the individual signature, generating the threshold signature and encrypting the message, the clerk does not have any secret knowledge of the system.

Upon receiving the individual signature, the clerk uses u_{si}'s public key Q_{si} and a base point α to verify the individual signature by checking $R_{si} \stackrel{?}{=} s_i \cdot \alpha_s - r \cdot a_{si} \cdot Q_{si}$. If it holds, the individual signature $\{r, s_i\}$ on message m is valid.

In threshold signature generating and encrypting phase, the clerk combines t valid individual signatures $\{r, s_i\}$ into a threshold signature $\{r, s\}$ and encrypts m by using the elliptic curve ElGamal cryptosystem [56] as follows:

Step 1. Compute the signature $s = \sum_{i \in g_s} s_i \bmod q$. $\{r, s\}$ is a group signature on message m.

Step 2. Express m as the x-coordinate of a point P_m on E. Then, choose a random integer w_c, where $1 \leq w_c \leq q$.

Step 3. Compute B and the ciphertext C as $B = w_c \cdot \alpha_v \bmod q$, $C = P_m + w_c \cdot Q_v \bmod q$.

Step 4. Transfer $\{r, s\}$ and (B, C) to the verifying group G_v.

In the decrypting and threshold signature verifying phase, to verify the signature $\{r, s\}$, any k u_{vi} in G_v can cooperate to decrypt the ciphertext C to obtain message m and authenticate the validity of the signature. Without loss of generality, assume that each of k participants $u_{v1}, u_{v2}, \cdots, u_{vk}$ in g_v wants to use his/her own private key K_{vi} to collaboratively recover the message and authenticate the signature by performing the following steps.

Step 1. Compute a value $e_{vi} = B \cdot K_{vi} \cdot a_{vi}$, where $a_{vi} = \prod_{\substack{j \in G_v \\ j \neq i}} \frac{ID_{vj}}{ID_{vj} - ID_{vi}}$. Next, transfer e_{vi} to a clerk randomly selected from G_v.

Step 2. The clerk computes a point $P_m = C - \sum_{i \in g_v} e_{vi}$, and recover m from the x-coordinate of P_m.

Step 3. Compute $\hat{X} = r + h(m) \bmod q$, and compute the corresponding $\hat{Y}$-coordinate on E_s.

The signature can be verified by using the signing group's public key Q_s and the base point α by checking $(\hat{X}, \hat{Y}) \stackrel{?}{=} s \cdot \alpha - r \cdot Q_s$. If it holds, the signature $\{r, s\}$ on message m is valid.

3 Comparisons

After introducing many kinds of threshold signature schemes in Section 1, we know that each kind is designed for different situations. We assume that there is a (t, n) threshold signature scheme, which can provide all requirements we have discussed before, called an ideal (t, n) threshold signature scheme. In the following, we divide the requirements into R (requirement), M (mode), and E (efficiency) for an ideal (t, n) threshold signature.

[Requirement]

R1. (*threshold characteristic*) At least t or more participants in the group can collaborate to generate a valid signature on behalf of the group signature. The threshold group signature has the same properties as those in general signature as follows:

- (*correctness*) All signatures on any message generated by any subset of group members using signing algorithm will get accepted by verifying algorithm.
- (*unforgeability*) Group signature cannot be forged , restricted on threshold characteristic.

R2. (*withstand conspiracy-impersonation attack*) In a (t, n) threshold signature scheme, we cannot avoid t dishonest members to generate a threshold group signature since the goal of threshold signature schemes is to generate threshold group signature via t members' cooperation. But we have to restrict that t dishonest members cannot reveal the polynomial by the conspiracy attacks. Once the group the polynomial is revealed, anyone of t

Table 1: Summary of R1, R2, M1, M2, M3, M4, M5, M5.1, M5.2, and M6

	[15]	[4]	[3]
R1. (*threshold characteristic*)	Yes	Yes	Yes
R2. (*withstand conspiracy-impersonation attack*)	No	Yes	No
M1. (*signature characteristic*)	Yes	No	Maybe
M2. (*undeniable characteristic*)	No	No	No
M3. (*traceability*)	No	Yes	Yes
M4. (*untraceability*)	Yes	Yes	No
M5. ((k,l) *threshold-shard verification*)	No	Yes	Yes
M5.1 (*exchange roles*)	-	Yes	Yes
M5.2 (*dynamic threshold*)	No	No	No
M6. (*distinguished signing authorities*)	No	No	No

dishonest members who can masquerade any member in group to sign any message without taking any responsibility. We call this attack as conspiracy-impersonation attack.

[Mode]

According to different situations, the signing group can choose the following modes to handle.

M1. (*signature characteristic*) Any one who plays the role of a verifier can use the group's public key to verify the group signature.

M2. (*undeniable characteristic*) Without the cooperation of t members, a verifier or G_v cannot verify the validity of an alleged signature even if he knows group public key.

M3. (*traceability*) A group signature can be opened and real identities of signers can be revealed.

M4. (*untraceability*) Given a threshold group signature, identifying the real signers is computational hard for everyone.

M5. ((k,l) *threshold-shard verification*) At least k participants in the group can collaborate to verify a valid signature on behalf of the verifying group.

M5.1 (*exchange roles*) The signing group and the verifying group can exchange their roles with each other.

M5.2 (*dynamic threshold*) The dynamic type of threshold value t and k.

M6. (*distinguished signing authorities*) The signing document can be divided into any t smaller subdocuments in such a way that each subdocument is meaningful and will be signed as a unit by one discretionary signatory.

[Efficiency]

The efficiency of an ideal (t,n) threshold signature scheme is typically based on the following parameters.

E1. (*group key size*) The size of the group public key is independent of the size of the group.

E2. (*group signature size*) The size of a group signature is independent of the size of the group.

E3. (*share distribution center*) The SDC can be removed in the system.

E4. (*parameters*) The number of public and private parameters held by participants.

E5. (*computational complexity and communication cost*) The computational complexity and communication cost of signing, verifying and opening.

E6. (*membership*) The efficiency of setting system parameters, adding a new user in the system, and removing an old user from the system.

Let an ideal (t,n) threshold signature be a benchmark, we evaluate the schemes reviewed in Section 2 in the following tables.

From Table 1, the reviewed schemes satisfy R1. Assume that t dishonest members in g_s tries to mount conspiracy-impersonation attacks to reveal the polynomial. By Eq. (1), t dishonest members can use their shares K_is to reconstruct $f(x)$ by using Lagrange interpolating polynomial. Hence, once $f(x)$ is revealed, anyone who can paly a role as any member in the group to sign any message. Thus, [15] cannot satisfy R2. In [4], even if t dishonest members in g_s provide their shares K_{si}s in Eq. (2), the polynomials $f_s(x)$ still cannot be reconstructed. Hence, they cannot compute the victims u_{si}s' $f_s(ID_i)$s. For the same reason, $f_v(x)$ still cannot be reconstructed. Thus, [4] satisfies R2. In [3], they can provide K_{si} in Eq. (4) to reconstruct $f_s(x) = f_{s1}(x) + f_{s2}(x) + \cdots + f_{sn}(x)$. For the same reason, $f_v(x) = f_{v1}(x) + f_{v2}(x) + \cdots + f_{vl}(x)$ can be reconstructed. Thus, [3] cannot satisfy R2.

Anyone who plays the role of a verifier can use G_s's public key e to verify the group signature $m \stackrel{?}{=} (S_m)^e \bmod n$ in [15]. Thus, [15] provides M1. In [4], they uses the extended Euclidean algorithm to ensure the communication between G_s and G_v. In other words, no one can play the role of G_s to generate the signature or the role of G_v to verify the signature. Thus, [4] cannot provide M1. In [3], the message is signed and encrypted by G_v's public key. If the process of encryption is removed, anyone who plays the role of a verifier can use G_s's public key. In [15], [4], and [3], a verifier or G_v cannot verify the validity of an alleged signature without the cooperation of t members. So, they cannot provide M2. [15] does not provide the process of individual signature verifying, so it cannot satisfies M3. On the contrary, [4] and [3] satisfy M3. But [4] further provides M4. Only [4] and [3] discuss on threshold-shared verification, which provide M5 and M5.1. However, M5.2 does not be discuss in their schemes. Finally, [15], [4], and [3] does not provide M6.

Table 2: Summary of E1, E2, and E3

	[15]	[4]	[3]
E1. (*group key size*)	Yes	Yes	Yes
E2. (*group signature size*)	Yes	Yes	Yes
E3. (*share distribution center*)	Yes	Yes	No

From Table 2, no matter what the size of the group, the size of group public key e and the size of group signature S_m are bounded by $\lambda(N)$ and N in [15], respectively. In [4], the size of group public key Y is bounded by N and the size of group signature $\{e, Zs\}$ is bounded by the length of hash output and N. In [3], the size of group public key Q_{si} and the size of group signature $\{r, s\}$ is bounded by q. Thus, [15], [4], and [3] satisfy E1 and E2. [3] employs Pedersen's distributed key generation scheme to remove SDC, hence only [3] satisfies E3.

Table 3: Summary of E4

E4 (*parameters*)	u_{si} in G_s		u_{vi} in G_v	
	Public values	Private values	Public values	Private values
[15]	1	2	-	-
[4]	2	1	2	1
[3]	2	1	2	1

From Table 3, each $u_{si} \in G_s$ has one public value x_{si} and one private values K_{si} in [15], has two public vales x_{si}, y_{si} and one private value K_{si} in [4], has two public vales ID_{si}, Q_{si} and one private value K_{si} in [4]. For the same reason for each $u_{vi} \in G_v$ in [4] and [3].

To evaluate E4 and E5, we first define the following notations:

T_{RSA}	the time for computing exponent in RSA-type scheme.
T_{EC}	the time for computing multiply in Elliptic curve ElGamal-type scheme.
$u_{si} \longmapsto u_{sj}$	the communication from u_{si} to u_{sj} $(i \neq j)$ in g_s.
$u_{si} \longmapsto$clerk	the communication from u_{si} to clerk in G_s.
$G_s \longmapsto G_v$	the communication from G_s to G_v.
$u_{vi} \longmapsto$clerk	the communication from u_{vi} to clerk in G_v.

An elliptic curve $E(F_p)$ with a point $\alpha \in E(F_p)$ whose order is a 160-bit prime offers approximately the same level of security as the RSA scheme with a 1024-bit modulus N. [15] and [4] the RSA-type scheme, and we assume that the modulus N is around 1024-bit in their schemes. [29] has pointed out that computing $k\alpha$ requires an average of 29 1024-bit modular multiplications and computing $x^k \bmod N$ by doing repeated multiplications requires an average of 240 1024-bit modular multiplications. Thus, computing $k\alpha$ can be expected to be about 8 times faster than computing $x^k \bmod p$, i.e., $8T_{EC} = T_{RSA}$. In Table 4, we only compare the expensive operations T_{RSA} in the RSA-type scheme and T_{EC} in the elliptic curve ElGamal-type scheme.

From Table 3, Table 4 and Table 5, we lean E4 and E5 about the efficient of schemes.

For E6 (*membership*) in [15] and [4], when a new user enters the group, SDC needs to distribute the related parameters to each participant, but the group secret key is still the same. In [3], it is more complex than that in [15] and [4] because it needs to do Pedersen's distributed key scheme again, but it does not need SDC's support. However, three schemes do not focus on when an old user leaves from the system. Once a user leaves the system, all parameters needs to re-setup.

4 Future Works

Until now, there is no scheme can live up to an ideal threshold signature scheme. Let's think about how a scheme become an ideal threshold signature scheme. Similar to Chang et al.'s scheme [4], their scheme integrates modes M3 and M4 relies on the clerk. If the clerk is not only responsible for combing the individual signatures but also provides other services for different modes, an ideal threshold is neatly arranged to be formed. In the following Figure 7, the signing group has the ability to choose which mode M1/M2/M3/M4/M5/M6 they would like to execute.

According to different mode chosen by the signing group, the clerk performs steps for the mode. On the other hand, R1 and R2 cannot be broken. In [3], SDC is removed based on Pedersen's distributed key scheme. Obviously, all schemes based on Shamir's secret sharing scheme can easily become Pedersen's distributed key scheme to remove SDC. However, we have analyzed E6 in Section 3, a threshold signature scheme without SDC leads to more complex when a user enters the system. How to have both E3 and E6 is a topic for discussion.

Go a step further, does the threshold vale t or k can be dynamically changed (M5.2)? All schemes setups the threshold parameters first in the system initiation. According to the grade of a document to determine what the threshold value is, it is more practice in real-world applications.

5 Conclusions

In many of new forms of communication, a digital signature is essential. The signer of the conventional digital signature schemes is usually a single user. However, the responsibility of signature schemes needs to be shared from time to time. Threshold signature combines signature and secret sharing for the security level of a document. It is practice in real-word applications. In this

Table 4: Summary of E5

E5 (*computational complexity*)	Individual signature generating (and verifying)	Group signature generating and verifying
[15]	$t\ T_{RSA}$	T_{RSA}
[4]	$3t\ T_{RSA}$	$4t\ T_{RSA}$
[3]	$4t\ T_{EC}$	$t+4\ T_{EC}$

Table 5: Summary of E5

E5 (*communication cost*)	$u_{si} \longmapsto$clerk	$G_s \longmapsto G_v$	$u_{vi} \longmapsto$clerk
[15]	$t-1 \times \|N\|$	$t-1 \times \|N\| + \|m\|$	-
[4]	$t \times (2\|h\| + \|N\| + \|m\|)$	$\|h\| + \|N\| + \|m\|$	$k \times 2\|N\|$
[3]	$3t \times \|q\|$	$4 \times \|q\|$	$k \times \|q\|$

paper, we have introduce the history of threshold signature schemes. Based on different requirements, each kind of threshold signature schemes is developed. It is exhilarating, to develop an ideal threshold signature schemes.

References

[1] G. B. Agnew, B. C. Mullin, and S.A. Vanstone, "Improved digital signature scheme based on discrete exponentiation," *Electronics Letters*, vol. 26, no. 14, pp. 1024–1025, 1990.

[2] C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[3] T. Y. Chang, C. C. Yang, and M. S. Hwang, "Threshold signature for group communications without shared distribution center," *Future Generation Computer Systems*, vol. 20, no. 6, pp. 1013–1021, 2004.

[4] T. Y. Chang, C. C. Yang, and M. S. Hwang, "Threshold untraceable signature for group communications," *IEE Proceedings-Communications*, vol. 15, no. 2, pp. 179–184, 2004.

[5] S. W. Changchien and M. S. Hwang, "A batch verifying and detecting multiple RSA digital signatures," *International Journal of Computational and Numerical Analysis and Applications*, accepted (Feb. 18, 2002) and to appear.

[6] D. Chaum, "Zero-knowledge undeniable signatures," in *Advances in Cryptology, Eurocrypt'90*, pp. 458–464, 1990.

[7] D. Chaum and H. Van Antwerpen, "Undeniable signatures," in *Advances in Cryptology, Crypto'89*, pp. 212–216, 1989.

[8] T. S. Chen, "A specifiable verifier group-oriented threshold signauture scheme based on the elliptic curve cryptosystem," *Computer Standard & Interfaces*, vol. 27, no. 1, pp. 33–38, 2004.

[9] T. S. Chen, "A threshold signature scheme based on the elliptic curve cryptosystem," *Applied Mathematics and Computation*, vol. 162, no. 3, pp. 1119–1134, 2005.

[10] T. S. Chen, K. H. Huang, and Y. F. Chung, "A division-of-labor-signature (t, n) threshold-authenticated encryption scheme with message linkage based on the elliptic curve cryptosystem," in *IEEE International Conference on e-Technology, e-Commerce and e-Service, EEE '04*, pp. 106–112, 2004.

[11] T. S. Chen, K. H. Huang, and Y. F. Chung, "A practical authenticated encryption scheme based on the elliptic curve crytosystem," *Computer Standard & Interfaces*, vol. 26, no. 5, pp. 461–469, 2004.

[12] X. Cheng, J. Liu, and X. Wang, "An identity-based signature and its threshold version," in *19th International Conference on Advanced Information Networking and Applications, AINA 2005*, vol. 1, pp. 973–977, 2005.

[13] Y. Desmedt, "Society and group oriented cryptography," in *Advances in Cryptology, CRYPTO'87*, pp. 120–127, 1987.

[14] Y. Desmedt and Y. Frankel, "Threshold cryptosystem," in *Advances in Cryptology, CRYPTO'89*, pp. 307–315, 1989.

[15] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Advances in Cryptology, CRYPTO'91*, pp. 457–469, 1991.

[16] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proc. 28th IEEE Symp. FOCS*, pp. 427–437, 1987.

[17] R. Gennaro, H. Krawczyk, and T. Rabin, "RSA-based undeniable signature," in *Advances in Cryptology, Crypto'97*, pp. 132–148, 1997.

[18] L. C. Guillou and J. J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge," in *Advances in Cryptology, Crypto'88*, pp. 216–231, 1988.

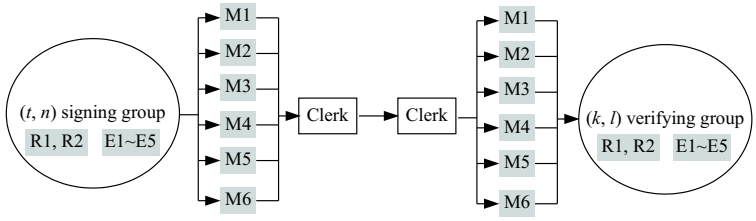

Figure 7: An ideal threshold signature scheme

[19] T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithms," in *Auscrypt'92*, pp. 16–21, 1992.

[20] L. Harn, "Group-oriented (t, n) threshold signature and digital multisignature," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, no. 5, pp. 307–313, 1994.

[21] L. Harn and S. Yang, "Group-oriented undeniable signature schemes with out the assistance of a mutually trusted party," in *Advances in Cryptology, AUSCRYPT'92*, pp. 133–142, 1992.

[22] P. Horster, M. Michels, and H. Peterson, "Comment: Digital signature with (t, n) shared verification based on discrete logarithms," *IEE Electronics Letters*, vol. 31, no. 14, p. 1137, 1995.

[23] C. L. Hsu, T. S. Wu, and T. C. Wu, "Improvements of threshold signature and authenticated encryption for group communications," *Information Processing Letters*, vol. 81, no. 1, pp. 41–45, 2002.

[24] C. L. Hsu, T. S. Wu, and T. C. Wu, "Group-oriented signature scheme with distinguished signing authorities," *Future Generation Computer Systems*, vol. 20, no. 5, pp. 865–873, 2004.

[25] M. S. Hwang, C. C. Lee, and Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, 2002.

[26] M. S. Hwang, C. C. Lee, and Eric J. L. Lu, "Cryptanalysis of the batch verifying multiple DSA-type digital signatures," *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287–288, 2001.

[27] M. S. Hwang, I. C. Lin, and K. F. Hwang, "Cryptanalysis of the batch verifying multiple RSA digital signatures," *Informatica*, vol. 11, no. 1, pp. 15–19, 2000.

[28] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.

[29] N. Koblitz, A. Menezes, and S. A. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 9, no. 2/3, pp. 173–193, 2000.

[30] S. K. Langford, "Weaknesss in some threshold cryptosystems," in *Advances in Cryptology, Crypto'96*, pp. 74–82, 1996.

[31] N. Y. Lee and T. Hwang, "Group-oriented undeniable signature schemes with a trusted center," *Computer Communications*, vol. 22, no. 8, pp. 730–734, 1999.

[32] N. Y. Lee, T. Hwang, and C. M. Li, "(t, n) threshold untraceable signatures," *Journal of Information Science and Engineering*, vol. 16, no. 6, pp. 835–845, 2000.

[33] W. B. Lee and C. C. Chang, "Comment: Digital signature with (t, n) shared verification based on discrete logarithms," *IEE Electronics Letters*, vol. 31, no. 3, pp. 176–177, 1995.

[34] C. M. Li, T. Hwang, N. Y. Lee, and J. J.Tsai, "(t, n) threshold-multisignature schemes and generalized-multisignature scheme where suspected forgery implies traceability of adversarial shareholders," *Cryptologia*, vol. 24, no. 3, pp. 250–268, 2000.

[35] C. M. Li, T. Hwang, and N. Y. Lee, "Remark on the threshold RSA signature scheme," in *Advances in Cryptology, CRYPTO'93*, pp. 413–420, 1993.

[36] C. M. Li, T. Hwang, and N. Y. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders," in *Advances in Cryptology, Eurocrypt'94*, pp. 194–204, 1994.

[37] Z. C. Li, C. K. Hui, K. P. Chow, C. F. Chong, W. W. Tsang, and H. W. Chan, "Security of Wang et al.'s group-oriented (t, n) threshold signature schemes with traceable signers," *Information Processing Letters*, vol. 80, no. 6, pp. 295–298, 2001.

[38] Z. C. Li, J. M. Zhang, J. Luo, W. Song, and Y. Q. Dai, "Group-oriented (t, n) threshold digital signature schemes with traceable signers," in *Electronic Commerce Techniques, the Second International Symposium, ISEC 2001*, pp. 57–69, 2001.

[39] C. H. Lin, C. T. Wang, and C. C. Chang, "A group-oriented (t, n) undeniable signature scheme without trusted center," in *First Australian Conference, ACISP'96*, pp. 266–274, 1996.

[40] L. S. Liu, C. K. Chu, and W. G. Tzeng, "A threshold GQ signature scheme," *Applied Cryptography and Network Security*, vol. 2846, pp. 137–150, 2003.

[41] R. X. Lu, Z. F. Cao, and Y. Zhou, "Threshold undeniable signature scheme based on conic," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 165–177, 2005.

[42] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[43] M. Michels and P. Horster, "On the risk of disruption in several multiparty signature schemes," in *Asiacrypt'96*, pp. 334–345, 1996.

[44] K. Miyazaki and K. Takaragi, "A threshold digital signature scheme for a smart card based system," *IEICE Transactions on Fundamentals*, vol. E84-A, no. 1, pp. 205–213, 2001.

[45] S. Miyazaki and K. Sakurai, "Distributed protocols for the Nyberg-Rueppel signature," in *Proc. Society Conference of IEICE Engineering Sciences Society*, p. 122, 1998.

[46] National Institute of Satndards and Technology (NIST), "The digital sinature standard proposed by NIST," *Communications of the ACM*, vol. 35, no. 7, pp. 36–40, 1992.

[47] K. Ohta and T. Okamoto, "A digital multi-signature scheme based on the Fiat-Shamir scheme," *Asiacrypt'91*, pp. 75–79, 1991.

[48] T. Okamoto, "A digital multisignature scheme using bijective public-key cryptosystems," *ACM Tranactions on Computer Systems*, vol. 6, no. 8, pp. 432–441, 1988.

[49] C. Park and K. Kurosawa, "New ElGamal type threshold digital signature scheme," *IEICE Transactions on Fundamentals*, vol. E79-A, no. 1, pp. 86–93, 1996.

[50] T. P. Pedersen, "Non-interactive and information-theoretic verifiable secret sharing," in *Advances in Cryptology, CRYPTO'91*, pp. 129–140, 1991.

[51] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Advances in Cryptology, EUROCRYPT'91*, pp. 522–526, 1991.

[52] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[53] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[54] Z. Shao, "Improvement of threshold signature using self-certified public keys," *Improvement of Threshold Signature Using Self-certified Public Keys*, vol. 1, no. 1, pp. 26–33, 2005.

[55] P. C. Su, Henry K. C. Chang, and E. H. Lu, "ID-based threshold digital signature schemes on the elliptic curve discrete logarithm problem," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 757–772, 2005.

[56] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory.* Prentice Hall, 2002.

[57] Y. M. Tseng and J. K. Jan, "Attack on threshold signature schemes with traceable signers," *Information Processing Letters*, vol. 71, no. 1, pp. 1–4, 1999.

[58] Y. M. Tseng, J. K. Jan, and H. Y. Chien, "On the security of generalization of threshold signature and authenticated encryption," *IEICE Transactions on Fundamentals*, vol. E84-A, no. 10, pp. 2606–2609, 2001.

[59] C. T. Wang, C. C. Chang, and C. H. Lin, "Generalization of threshold signature and authenticated encryption for group communications," *IEICE Transactions on Fundamentals*, vol. E83-A, no. 6, pp. 1228–1237, 2000.

[60] C. T. Wang, C. H. Lin, and C. C. Chang, "Research note threshold signature schemes with traceable signers in group communications," *Computer Communications*, vol. 21, no. 8, pp. 771–776, 1998.

[61] G. Wang, S. Qing, M. Wang, and Z. Zhou, "Threshold undeniable RSA signature scheme," in *Information and Communications Security (ICICS 2001), LNCS 2229*, pp. 220–231, 2001.

[62] G. Wang, J. Zhou, and R. H. Deng, "On the security of the Lee-Hwang group-oriented undeniable signature schemes," in *Trust and Privacy in Digital Business: First International Conference*, p. 289, 2004.

[63] S. Wang, G. Wang, F. Bao, and J. Wand, "Security notes on generalization of threshold signature and authenticated encryption," *IEICE Transactions on Fundamentals*, vol. E87-A, no. 12, pp. 3443–3446, 2004.

[64] T. S. Wu and C. L. Hsu, "Threshold signature scheme using self-certified public keys," *Journal of Systems and Software*, vol. 67, no. 2, pp. 89–97, 2003.

[65] T. S. Wu and C. L. Hsu, "Cryptanalysis of group-oriented (t, n) threshold digital signature schemes with traceable signers," *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 477–481, 2004.

[66] T. S. Wu, C. L. Hsu, H. Y. Lin, and P. S. Huang, "Improvement of the Miyazaki-Takaragi threshold digital signaure scheme," *Information Processing Letter*, vol. 88, no. 4, pp. 183–186, 2003.

[67] C. C. Yang, T. Y. Chang, J. W. Li, and M. S. Hwang, "Simple generalized group-oriented cryptosystems using ElGamal cryptosystem," *International Journal of Informatica*, vol. 14, no. 1, pp. 111–120, 2003.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also

the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor and chairman of the department of Management Information Systems, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 100 articles on the above research fields in international journals.

Ting-Yi Chang received the B.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001, and his M.S. in Department and Graduate Institute of Computer Science and Information Engineering from CYUT, in 2003. He is currently pursuing his Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications.