Classification of Signature-only Signature Models

Zhengjun Cao

Department of Mathematics, Shanghai University, China, 200444. zjcamss@163.com

Abstract We introduce a set of criterions for classifying signature-only signature models. By the criterions, we classify signature models into 5 basic types and 69 general classes. Theoretically, 21140 kinds of signature models can be deduced by appropriately combining different general classes. The result comprises almost existing signature models. We also contribute a lot of new signature models. Moreover, we find the three signature models, i.e., group-nominee signature, multi-nominee signature and threshold-nominee signature, are of great importance in light of our classification.

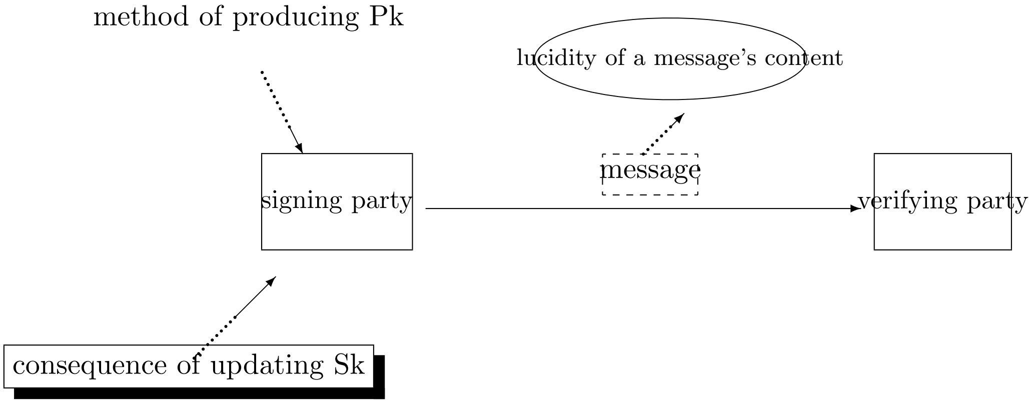
Keywords signing party, verifying party, lucidity of a message's content, method of producing Pk, consequence of updating Sk.

1 Introduction

There are about sixty digital signature models introduced in various environments. For example, multi-signature [1], threshold signature [2], group signature [3], threshold group signature [4], ring signature [5], linkable ring signature [6], threshold ring signature [7], proxy signature [8], multi-proxy signature [9], threshold proxy signature [10], proxy ring signature [11], proxy multi-signature [12], multi-proxy multi-signature [13], threshold proxy multi-signature [14], designated-verifier signature [15], multiple designated-verifier signature [16], nominative signature [17], undeniable signature [18], designated-confirmer signature [19], multiple designated-confirmer signature [19], blind signature [20], fair blind signature [21], restrictive blind signature [22], partially blind signature [23], restrictive partially blind signature [24], ID-based signature [25], forward-secure signature [26], designated-verifier proxy signature [27], nominative proxy signature [28], undeniable multi-signature [29], undeniable proxy multi-signature [30], blind multi-signature [31], threshold blind signature [32], threshold partially blind signature [33], group blind signature [34], threshold ring blind signature [35], proxy blind signature [36], ID-based ring signature [37], ID-based threshold ring signature [38], ID-based proxy signature [39], ID-based multi-proxy signature [31], ID-based threshold proxy signature [40], ID-based proxy ring signature [37], ID-based blind signature [41], ID-based restrictive blind signature [42], ID-based partially blind signature [43], ID-based restrictive partially blind signature [42], forward-secure group signature [44], forward-secure ring signature [45], forward-secure proxy signature [46], forward-secure blind signature [47], ID-based proxy blind signature [48], message recovery signature [49] and fail-stop signature [50]. These models have so various properties that they are difficult to understand even for a postgraduate majoring in cryptography.

Now, how to classify these models? Is it difficult to introduce any other signature models? Surprisingly, they are only a fraction of signature models. We find there are numerous models according to our criterions for classification.

It's well known that a general signature scheme comprises five absolutely necessary elements: signing party, verifying party, message, signer's public key and signer's secret key. We find that the formation of signing party and each signer's ability are often considered in practice. The formation of verifying party and each verifier's ability are often considered, too. We also consider whether the content of a message is known to the signing party. Except that, we often consider the method of producing Pk and the consequence of updating Sk.



Our contributions We draw five absolutely necessary elements in a general signature model (signature-only signature). They are signing party, verifying party, lucidity of a message's content, method of producing Pk and consequence of updating Sk. By the criterions, we classify signature models into five basic *types* and 69 general *classes*. As a result, theoretically, 21140 *kinds* of signature models can be deduced by appropriately combining different general classes. We will give a representation of all these models. Moreover, we find three important signature models according to our classification. They are group-nominee signature, multi-nominee signature and threshold-nominee signature.

The rest of the paper is organized as follows. Section 2 describes the result of classification of signature models based on our criterions. A method to represent all kinds of models is presented in section 3. Some conclusion remarks are given in section 4.

2 Classification of signature models

2.1 I-type: classification based on the signing party

In the above general signature model, the signing party should be treated an entity instead of a person. In practice, either one person or multiple persons can act the role. In view of that whether the identity of the signing party should be kept in secret and the signing authority should be delegated to others, we have the following classification.

2.1.1 The signing authority is not delegated to others

A_0 The signing party is acted by *somebody*. His identity is *open*.

A_1 The signing party is acted by *a group of persons*. Their identities are *open*.

A_2 The signing party is acted by any members ((t, n)-threshold) among a group of persons. *They* sign messages *on behalf of* the group.

A_3 The signing party is acted by any member among a group of persons. *He* anonymously signs messages *on behalf of* the group. Given a valid signature, *only* an authority center can reveal the identity of the signer.

A_4 The signing party is acted by any members ((t, n)-threshold) among a group of persons. *They* anonymously sign messages *on behalf of* the group. Given a valid signature, *only* an authority center can reveal the identities of the signers.

A_5 The signing party is acted by any member among a group of persons. *He* anonymously signs messages *on behalf of* the group. Given a valid signature, *nobody* can reveal the identity of the signer. Further, it is computational *hard* to decide whether two different signatures were issued by the same signer.

A_6 The signing party is acted by any member among a group of persons. *He* anonymously signs messages *on behalf of* the group. Given a valid signature, *nobody* can reveal the identity of the signer. But it is *easy* to decide whether two different signatures were issued by the same signer.

A_7 The signing party is acted by any members ((t, n)-threshold) among a group of persons. *They* anonymously sign messages *on behalf of* the group. Given a valid signature, *nobody* can reveal the identities of the signers. Further, it is computational *hard* to decide whether two different signatures were issued by the same signers.

A_8 The signing party is acted by any members ((t, n)-threshold) among a group of persons. *They* anonymously sign messages *on behalf of* the group. Given a valid signature, *nobody* can reveal the identities of the signers. But it is *easy* to decide whether two different signatures were issued by the same signers.

2.1.2 The signing authority is delegated to others

Case 1: One original signer

A_9 The signing party is acted by a proxy person designated by the original signer. *He* signs messages *on behalf of* the original signer. His identity is *open*.

A_{10} The signing party is acted by any person among a group of proxy persons designated by the original signer. *He* anonymously signs messages *on behalf of* the original signer. Given a valid signature, *only* an authority center can reveal the identity of the signer.

A_{11} The signing party is acted by all proxy persons designated by the original signer. *They* sign messages *on behalf of* the original signer. Their identities are *open.*

A_{12} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the original signer. *They* sign messages *on behalf of* the original signer.

A_{13} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the original signer. *They* anonymously sign messages *on behalf of* the original signer. Given a valid signature, *only* an authority center can reveal the identities of the proxy signers.

A_{14} The signing party is acted by any person among a group of proxy persons designated by the original signer. *He* anonymously signs messages *on behalf of* the original signer. Given a valid signature, *nobody* can reveal the identity of the signer. Further, it is computational *hard* to decide whether two different signatures were issued by the same signer.

A_{15} The signing party is acted by any person among a group of proxy persons designated by the original signer. *He* anonymously signs messages *on behalf of* the original signer. Given a valid signature, *nobody* can reveal the identity of the signer. But it is *easy* to decide whether two different signatures were issued by the same signer.

A_{16} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the original signer. *They* anonymously sign messages *on behalf of* the original signer. Given a valid signature, *nobody* can reveal the identities of the signers. Further, it is computational *hard* to decide whether two different signatures were issued by the same signers.

A_{17} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the original signer. *They* anonymously sign messages *on behalf of* the original signer. Given a valid signature, *nobody* can reveal the identities of the signers. But it is *easy* to decide whether two different signatures were issued by the same signers.

Case 2: Multiple original signers

A_{18} The signing party is acted by any proxy person designated by the multiple original signers. *He* signs messages *on behalf of* the *multiple* original signers. His identity is open.

A_{19} The signing party is acted by all proxy persons designated by the multiple original signers. *They* sign messages *on behalf of* the *multiple* original signers. Their identity are open.

A_{20} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the multiple original signers. *They* sign messages *on behalf of* the *multiple* original signers.

A_{21} The signing party is acted by any proxy person designated by the multiple original signers. *He* anonymously signs messages *on behalf of* the *multiple* original signers. Given a valid signature, *only* an authority center can reveal the identity of the proxy signer.

A_{22} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the multiple original signers. *They* anonymously sign messages *on behalf of* the *multiple* original signers. Given a valid signature, *only* an authority center can reveal the identity of the proxy signers.

A_{23} The signing party is acted by any member among a group of proxy persons designated by the multiple original signers. *He* anonymously signs messages *on behalf of* the *multiple* original signers. Given a valid signature, *nobody* can reveal the identity of the signer. Further, it is computational *hard* to decide whether two different signatures were issued by the same proxy signer.

A_{24} The signing party is acted by any member among a group of proxy persons designated by the multiple original signers. *He* anonymously signs messages *on behalf of* the *multiple* original signers. Given a valid signature, *nobody* can reveal the identity of the signer. But it is *easy* to decide whether two different signatures were issued by the same proxy signer.

A_{25} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the multiple original signers. *They* anonymously sign messages *on behalf of* the *multiple* original signers. Given a valid signature, *nobody* can reveal the identities of the signers. Further, it is computational *hard* to decide whether two different signatures were issued by the same proxy signers.

A_{26} The signing party is acted by any members ((t, n)-threshold) among a group of proxy persons designated by the multiple original signers. *They* anonymously sign messages *on behalf of* the *multiple* original signers. Given a valid signature, *nobody* can reveal the identities of the signers. But it is *easy* to decide whether two different signatures were issued by the same proxy signers.

2.2 II-type: classification based on the verifying party

Usually, the verifying party in the general signature model can be acted by a person or multiple persons. We also consider whether the verifying party has the ability to check the validity of a given signature and prove it to others. Therefore, we have the following classification.

2.2.1 The verifying party can directly check the validity of a given signature

B_0 The verifying party is acted by *anybody.* He can *check* the validity of a given signature and *prove* it to others.

B_1 The verifying party is acted by a *designated person.* He can *check* the validity of a given signature but *cannot prove* it to others.

B_2 The verifying party is acted by *any member* among a group of *designated persons.* He can *check* the validity of a given signature but *cannot prove* it to others.

B_3 The verifying party is acted by *all* members of a group of *designated persons.* They can *check* the validity of a given signature but *cannot prove* it to others.

B_4 The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* They can *check* the validity of a given signature but *cannot prove* it to others.

B_5 The verifying party is acted by *a designated person.* He can *check* the validity of a given signature and *prove* it to others.

B_6 The verifying party is acted by *any member* among a group of *designated persons.* He can *check* the validity of a given signature and *prove* it to others.

B_7 The verifying party is acted by *all* members of a group of *designated persons.* They can *check* the validity of a given signature and *prove* it to others.

B_8 The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* They can *check* the validity of a given signature and *prove* it to others.

2.2.2 Only with the help of the signing party, the verifying party can check the validity of a given signature

B_9 The verifying party is acted by *anybody.* Only with the help of the signing party, he can *check* the validity of a given signature and *prove* it to others.

B_{10} The verifying party is acted by *anybody.* Only with the help of the signing party, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{11} The verifying party is acted by*a designated person.* Only with the help of the signing party, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{12} The verifying party is acted by *any member* among a group of *designated persons.* Only with the help of the signing party, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{13} The verifying party is acted by *all designated persons.* Only with the help of the signing party, they can *check* the validity of a given signature. But they *cannot prove* it to others.

B_{14} The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* Only with the help of the signing party, they can *check* the validity of a given signature. But they *cannot prove* it to others.

B_{15} The verifying party is acted by *a designated person.* Only with the help of the signing party, he can *check* the validity of a given signature and *prove* it to others.

B_{16} The verifying party is acted by *any member* among a group of *designated persons.* Only with the help of the signing party, he can check the validity of a given signature and *prove* it to others.

B_{17} The verifying party is acted by *all designated persons.* Only with the help of the signing party, they can *check* the validity of a given signature and *prove* it to others.

B_{18} The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* Only with the help of the signing party, they can *check* the validity of a given signature and *prove* it to others.

2.2.3 Only with the help of a confirmer (not the signing party), the verifying party can check the validity of a given signature

B_{19} The verifying party is acted by *anybody.* Only with the help of a confirmer, he can *check* the validity of a given signature and *prove* it to others.

B_{20} The verifying party is acted by *anybody.* Only with the help of a confirmer, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{21} The verifying party is acted by *a designated person.* Only with the help of a confirmer, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{22} The verifying party is acted by *any member* among a group of *designated persons.* Only with the help of a confirmer, he can *check* the validity of a given signature. But he *cannot prove* it to others.

B_{23} The verifying party is acted by *all designated persons.* Only with the help of a confirmer, they can *check* the validity of a given signature. But they *cannot prove* it to others.

B_{24} The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* Only with the help of a confirmer, they can *check* the validity of a given signature. But they *cannot prove* it to others.

B_{25} The verifying party is acted by *a designated person.* Only with the help of a confirmer, he can *check* the validity of a given signature and *prove* it to others.

B_{26} The verifying party is acted by *any member* among a group of *designated persons.* Only with the help of a confirmer, he can *check* the validity of a given signature and *prove* it to others.

B_{27} The verifying party is acted by *all designated persons.* Only with the help of a confirmer, they can *check* the validity of a given signature and *prove* it to others.

B_{28} The verifying party is acted by any members ((t, n)-threshold) among a group of *designated persons.* Only with the help of a confirmer, they can *check* the validity of a given signature and *prove* it to others.

2.3 III-type: classification based on the lucidity of a message's content

In view of that whether the content of the message to be signed is known to the signing party and whether the verifying party can link a pair of message and signature to the identity of a requester, we have:

C_0 The content of the message to be signed is *known* to the signing party.

C_1 The content of the message submitted by a requester is *not known* to the signing party. Given a pair of message and signature, he *cannot* link it to the identity of the requester.

C_2 The content of the message submitted by a requester is *not known* to the signing party. Given a pair of message and signature, he *can* link it to the identity of the requester *with the help of* an authority center.

C_3 The content of the message submitted by a requester is *not known* to the signing party. But *the choice of message* is restricted and must conform to certain rules. Given a pair of message and signature, he *cannot* link it to the identity of the requester.

C_4 The content of the message submitted by a requester is *not known* to the signing party. But *the choice of message* is restricted and must conform to certain rules. Given a pair of message and signature, he *can* link it to the identity of the requester *with the help of* an authority center.

C_5 The content of the message submitted by a requester is *not known* to the signing party. But *a part of the message* contains pre-agreed information (agreed by the signing party and the requester) is *unblinded.* Given a pair of message and signature, he *cannot* link it to the identity of the requester.

C_6 The content of the message submitted by a requester is *not known* to the signing party. But *a part of the message* contains pre-agreed information (agreed by the signing party and the requester) is *unblinded.* Given a pair of message and signature, he *can* link it to the identity of the requester *with the help of* an authority center.

C_7 The content of the message submitted by a requester is *not known* to the signing party. But *a part of the message* contains pre-agreed information (agreed by the signing party and the requester) is *unblinded. The choice of message* is restricted and must conform to certain rules. Given a pair of message and signature, he *cannot* link it to the identity of the requester.

C_8 The content of the message submitted by a requester is *not known* to the signing party. But *a part of the message* contains pre-agreed information (agreed by the signing party and the requester) is *unblinded. The choice of message* is restricted and must conform to certain rules. Given a pair of message and signature, he *can* link it to the identity of the requester *with the help of* an authority center.

2.4 VI-type: classification based on the method of producing Pk

In view of that whether the user's Pk can be directly derived from his identity, we have

D_0 The user's Pk *must* be *authenticated* and publicly *issued* by an authority center.

D_1 The user's Pk can be *directly* derived from his identity.

2.5 V-type: classification based on the consequence of updating Sk

Considering the user's secret key should be updated regularly, we have

E_0 All data of old Pk should be disaffirmed after updating Sk.

E_1 Only a fraction of data of old Pk should be disaffirmed after updating Sk. (Here, the time token in some schemes should be treated a datum of Pk.)

3 Representation of digital signature models

By above analysis, we obtain five basic types and 69 general classes. Hence, we represent all signature models as follows:

$$A_iB_jC_kD_\alpha E_\beta \qquad (0 \le i \le 26, 0 \le j \le 28, 0 \le k \le 8, 0 \le \alpha \le 1, 0 \le \beta \le 1)$$

(**Standard model**) If $i = j = k = \alpha = \beta = 0$, we get

representation	name	literature
$A_0B_0C_0D_0E_0$	digital signature	[51]

3.1 I-sort signature models

If only one subscript among i, j, k, α, β does not equal 0, theoretically, we obtain

$$26 + 28 + 8 + 1 + 1 = 64$$

kinds of I-sort signature models. As a consequence, we have

representation	name	literature
$A_1B_0C_0D_0E_0$	multi-signature	[1]
$A_2B_0C_0D_0E_0$	threshold signature	[2]
$A_3B_0C_0D_0E_0$	group signature	[3]
$A_4B_0C_0D_0E_0$	threshold group signature	[4]
$A_5B_0C_0D_0E_0$	ring signature	[5]
$A_6B_0C_0D_0E_0$	linkable ring signature	[6]
$A_7B_0C_0D_0E_0$	threshold ring signature	[7]
$A_8B_0C_0D_0E_0$	linkable threshold ring signature	[6]
$A_9B_0C_0D_0E_0$	proxy signature	[8]
$A_{10}B_0C_0D_0E_0$	multi-proxy signature	[9]
$A_{11}B_0C_0D_0E_0$	proxy group signature	[?]
$A_{12}B_0C_0D_0E_0$	threshold proxy signature	[10]
$A_{13}B_0C_0D_0E_0$	threshold proxy group signature	[?]
$A_{14}B_0C_0D_0E_0$	proxy ring signature	[11]
$A_{15}B_0C_0D_0E_0$	linkable proxy ring signature	[?]
$A_{16}B_0C_0D_0E_0$	threshold proxy ring signature	[?]
$A_{17}B_0C_0D_0E_0$	linkable threshold proxy ring signature	[?]
$A_{18}B_0C_0D_0E_0$	proxy multi-signature	[12]
$A_{19}B_0C_0D_0E_0$	multi-proxy multi-signature	[13]
$A_{20}B_0C_0D_0E_0$	threshold proxy multi-signature	[14]
$A_{21}B_0C_0D_0E_0$	proxy group multi-signature	[?]
$A_{22}B_0C_0D_0E_0$	threshold proxy group multi-signature	[?]
$A_{23}B_0C_0D_0E_0$	proxy ring multi-signature	[?]
$A_{24}B_0C_0D_0E_0$	linkable proxy ring multi-signature	[?]
$A_{25}B_0C_0D_0E_0$	threshold proxy ring multi-signature	[?]
$A_{26}B_0C_0D_0E_0$	linkable threshold proxy ring multi-signature	[?]

Remark 1 Throughout the paper, the labels [?] in literature column mean that we have not found any literatures by now. It should be stressed that we filled in the table by search names, which are directly taken from the result of our analysis. So, it is very possible to drop some literatures. If that, contact us, please. We will react favorably.

representation	name	literature
$A_0B_1C_0D_0E_0$	designated-verifier signature	[15]
$A_0B_2C_0D_0E_0$	group designated-verifier signature	[?]
$A_0B_3C_0D_0E_0$	multiple designated-verifier signature	[16]
$A_0B_4C_0D_0E_0$	threshold designated-verifier signature	[?]
$A_0B_5C_0D_0E_0$	nominee signature	[17]
$A_0B_6C_0D_0E_0$	group nominee signature	[?]
$A_0B_7C_0D_0E_0$	multi-nominee signature	[?]
$A_0B_8C_0D_0E_0$	threshold nominee signature	[?]
$A_0B_9C_0D_0E_0$	undeniable signature	[18]
$A_0B_{10}C_0D_0E_0$	non-transferred undeniable signature	[?]
$A_0B_{11}C_0D_0E_0$	designated-verifier undeniable signature	[?]
$A_0B_{12}C_0D_0E_0$	group designated-verifier undeniable signature	[?]
$A_0B_{13}C_0D_0E_0$	multiple designated-verifier undeniable signature	[?]
$A_0B_{14}C_0D_0E_0$	threshold designated-verifier undeniable signature	[?]
$A_0B_{15}C_0D_0E_0$	nominee undeniable signature	[?]
$A_0B_{16}C_0D_0E_0$	group nominee undeniable signature	[?]
$A_0B_{17}C_0D_0E_0$	multi-nominee undeniable signature	[?]
$A_0B_{18}C_0D_0E_0$	threshold nominee undeniable signature	[?]
$A_0B_{19}C_0D_0E_0$	confirming signature	[19]
$A_0B_{20}C_0D_0E_0$	non-transferable confirming signature	[?]
$A_0B_{21}C_0D_0E_0$	designated-verifier confirming signature	[?]
$A_0B_{22}C_0D_0E_0$	group designated-verifier confirming signature	[?]
$A_0B_{23}C_0D_0E_0$	multiple designated-verifier confirming signature	[?]
$A_0B_{24}C_0D_0E_0$	threshold designated-verifier confirming signature	[?]
$A_0B_{25}C_0D_0E_0$	nominee confirming signature	[?]
$A_0B_{26}C_0D_0E_0$	group nominee confirming signature	[?]
$A_0B_{27}C_0D_0E_0$	multi-nominee confirming signature	[?]
$A_0B_{28}C_0D_0E_0$	threshold nominee confirming signature	[?]

representation	name	literature
$A_0B_0C_1D_0E_0$	blind signature	[20]
$A_0B_0C_2D_0E_0$	fair blind signature	[21]
$A_0B_0C_3D_0E_0$	restrictive blind signature	[22]
$A_0B_0C_4D_0E_0$	fair restrictive blind signature	[?]
$A_0B_0C_5D_0E_0$	partially blind signature	[23]
$A_0B_0C_6D_0E_0$	fair partially blind signature	[?]
$A_0B_0C_7D_0E_0$	restrictive partially blind signature	[24]
$A_0B_0C_8D_0E_0$	fair restrictive partially blind signature	[?]
$A_0B_0C_0D_1E_0$	ID-based signature	[25]
$A_0B_0C_0D_0E_1$	forward-secure signature	[26]

Remark 2 For convenience, we replace the notions of *nominative signature* [17] and *designated confirmer signature* [19] with *nominee signature* and *confirming signature*, respectively.

3.2 II-sort signature models

If three subscripts among i, j, k, α, β just equal 0, theoretically, we obtain

$$26 \times (28 + 8 + 1 + 1) + 28 \times (8 + 1 + 1) + 8 \times (1 + 1) + 1 \times 1 = 1285$$

kinds of II-sort signature models. But $A_0B_0C_0D_1E_1$ is dissociable (the forward-secure property is inconsistent with the ID-based property). Therefore, we have 1284 II-sort signature models. We list some models in the following table.

representation	name	literature
$A_9B_1C_0D_0E_0$	designated-verifier proxy signature	[27]
$A_9B_5C_0D_0E_0$	nominee proxy signature	[28]
$A_1B_9C_0D_0E_0$	undeniable multi-signature	[29]
$A_9B_9C_0D_0E_0$	undeniable proxy signature	[?]
$A_{18}B_9C_0D_0E_0$	undeniable proxy multi-signature	[30]
$A_{20}B_9C_0D_0E_0$	undeniable threshold proxy multi-signature	[?]
$A_1B_0C_1D_0E_0$	multiple blind signature	[31]
$A_2B_0C_1D_0E_0$	threshold blind signature	[32]
$A_2B_0C_5D_0E_0$	threshold partyially blind signature	[33]
$A_3B_0C_1D_0E_0$	group blind signature	[34]
$A_7B_0C_1D_0E_0$	threshold ring blind signature	[35]
$A_9B_0C_1D_0E_0$	proxy blind signature	[36]
$A_{10}B_0C_1D_0E_0$	multi-proxy blind signature	[?]
$A_{12}B_0C_1D_0E_0$	threshold-proxy blind signature	[?]
$A_1B_0C_0D_1E_0$	ID-based multi-signature	[?]
$A_5B_0C_0D_1E_0$	ID-based ring signature	[37]
$A_7B_0C_0D_1E_0$	ID-based threshold ring signature	[38]
$A_9B_0C_0D_1E_0$	ID-based proxy signature	[39]
$A_{10}B_0C_0D_1E_0$	ID-based multi-proxy signature	[31]
$A_{12}B_0C_0D_1E_0$	ID-based threshold proxy signature	[40]
$A_{14}B_0C_0D_1E_0$	ID-based proxy ring signature	[37]
$A_0B_0C_1D_1E_0$	ID-based blind signature	[41]
$A_0B_0C_2D_1E_0$	ID-based fair blind signature	[?]
$A_0B_0C_3D_1E_0$	ID-based restrictive blind signature	[42]
$A_0B_0C_5D_1E_0$	ID-based partially blind signature	[43]
$A_0B_0C_7D_1E_0$	ID-based restrictive partially blind signature	[42]
$A_3B_0C_0D_0E_1$	forward-secure group signature	[44]
$A_5B_0C_0D_0E_1$	forward-secure ring signature	[45]
$A_9B_0C_0D_0E_1$	forward-secure proxy signature	[46]
$A_0B_0C_1D_0E_1$	forward-secure blind signature	[47]

3.3 III-sort signature models

If two subscripts among i, j, k, α, β just equal 0, theoretically, we obtain

$$(26 \times 28 \times 8 + 26 \times 28 \times 2 + 26 \times 8 \times 2 + 26 \times 1) + (28 \times 8 \times 2 + 28 \times 1) + (8 \times 1) = 8206$$

kinds of III-sort signature models. But $A_?B_?C_?D_1E_1$ is dissociable (the forward-secure property is inconsistent with the ID-based property). Therefore, we have

$$8206 - 26 - 28 - 8 = 8144$$

kinds of III-sort signature models. We list some models in the following.

representation	name	literature
$A_9B_0C_1D_1E_0$	ID-based proxy blind signature	[48]
$A_{10}B_0C_1D_1E_0$	ID-based multi-proxy blind signature	[?]
$A_{12}B_0C_1D_1E_0$	ID-based threshold proxy signature	[?]

3.4 IV-sort signature models

If only one subscript among i, j, k, α, β equals 0, theoretically, we have

$$26 \times 28 \times 8 \times 2 = 11648$$

kinds of IV-sort signature models because the forward-secure property is inconsistent with the ID-based property. But we have not found such a signature scheme in literatures by now.

Remark 3 In 1993, K. Nyberg and R. Ruepple [49] proposed a message recovery signature scheme. If a verifier should use his secret key to recover the encrypted message, then the message recovery signature scheme is a hybrid of encryption and authentication. If a verifier can unconditionally recover the encrypted message, the recoverable property is negligible. Therefore, we not consider the message recovery property in our general signature model.

Remark 4 In 1990, Pfitzmann and Waidner [50] introduce a fail-stop signature scheme. Essentially, we can take it as a forward-secure signature scheme because the signer's secret key is updated irregularly.

3.5 Three significant I-sort signature models

By the above representation of signature models, theoretically, we have

$$1 + (26 + 28 + 8 + 1 + 1) + 1284 + 8144 + 11648 = 21140$$

kinds of signature models. It's obvious that the 64 kinds I-sort signature models are more significant than the others. Up to now, we find only 27 kinds of them in literatures. Among the remainder 37 models, we think the three models, group-nominee signature, multi-nominee signature and threshold-nominee signature, are of great importance in light of our classification. They can be applied to the following cases, separately.

The millionaire John signs his testament and ensures that only lawyer Alice can verify and prove the signature. In the case, a nominee signature scheme should be used. If John fears that the only nominee Alice might betray him after his death, he could select a group of nominees, including the counselor Bob, the assistant Clare and a friend Dave. Anyone of them can verify and prove the signature. *Group-nominee signature* is an answer to this problem.

Anna signs her witness submitted to the local curia and ensures that all nine jurors jointly verify and prove the signature. A *multi-nominee signature* scheme can be used in the case. If she ensures that at least seven members of the nine jurors jointly verify and prove the signature, she should make a *threshold-nominee signature*.

4 Conclusion

In the paper, we introduce a set of criterions for classifying signature models. Theoretically, 21140 kinds of signature models are obtained. The result comprises almost existing signature models. Interestingly, a lot of new signature models are found. Since they are too numerous to list in the paper, we only give a method to represent them. We think the proposed criterions are helpful to understand numerous signature schemes in literatures. Moreover, the technique developed in the paper encourages us to hunt more scientific criterions for classification in the future.

References

[1] K. Itakura and K. Nakamura, A public key cryptosystem suitable for digital multisignatures, NEC Research and Development, 71, 1983, pp. 1-8.

[2] Y. Desmedt and Y. Frankel, Threshold cryptosystems, Advances in Cryptology, Crypto'89, LNCS 435, Springer, pp. 457-469.

[3] D. Chaum and E. van Heyst. Group signatures. Advances in Cryptology-Eurocrypt'91, LNCS 950, Springer, pp. 257-265.

[4] J. Camenisch. Efficient and generalized group signatures. Eurocrypt97, LNCS 1233, Springer, pp. 465-479.

[5] R.Rivest, A. Shamir, and Y.Tauman. How to leak a secret. Advances in Cryptology-Asiacrypt 2001, LNCS 2248, Springer, pp. 552-565.

[6] J. K. Liu, V. K. Wei, and D. S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). ACISP 2004, LNCS 3108, Springer, pp. 325-335.

[7] E. Bresson, J. Stern, and M. Szydlo. Threshold Ring Signature sand Applications to Ad-hoc Groups. Advances in Cryptology-CRYPTO 2002, LNCS 2442, Springer, pp. 465-480.

[8] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. IEICE Trans. Fundamentals, Sep. 1996, Vol. E79-A, No. 9, pp. 1338-1353.

[9] J. Hwang, and C.H. Shi, A simple multi-proxy signature scheme, Communications of the CCISA, Vol. 8, No. 1, 2001, pp. 88-92.

[10] K. Zhang, Threshold Proxy Signature Schemes, Proc. Information Security Workshop (ISW'97), LNCS 1396, Springer, pp. 282-290.

[11] F.G. Zhang, R. Safavi-Naini and C.Y. Lin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/104, http://eprint.iacr.org/2003/104

[12] L. Yi, G. Bai and G. Xiao, Proxy multi-signature scheme: A new type of proxy signature scheme, Electronic Letters, Vol.36, No.6, 2000, pp. 527-528.

[13] J. Hwang, and C.H. Chen, A New multi-proxy multi-signature scheme, 2001 National Computer Symposium: Information Security, Taiwan, pp. 1019–1026.

[14] S.F. Tzeng, C.Y. Yang, M.S. Hwang. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Future Generation Computer Systems archive Volume 20 , Issue 5 (June 2004) table of contents Special issue: Computational chemistry and molecular dynamics, pp. 887-893.

[15] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated Verifier Proofs and Their Applications. Advances in Cryptology-Eurocrypt'96, LNCS 1070, Springer, pp. 143-154.

[16] Ching Yu Ng, Willy Susilo, Yi Mu, Universal Designated Multi Verifier Signature Schemes, Proceedings of the International Workshop on Security in Networks and Distributed Systems (SNDS 2005), Japan, IEEE Press, pp. 305-309.

[17] S.J.Kim, S.J.Park and D.H. Won, Zero-knowledge nominative signatures, Proc. of PragoCrypt'96, International Conference on the Theory and Applications of Cryptology, pp. 380-392.

[18] D. Chaum and H. van Antwerpen. Undeniable signatures. CRYPTO'89, LNCS 435, Springer, pp. 212-216.

[19] D. Chaum. Designated confirmer signatures. Eurocrypt'94, LNCS 950, Springer, pp. 86-91.

[20] D. Chaum. Blind signatures for untraceable payments. Crypto'82, New York: Plenum Press, 1983. pp. 199-203.

[21] Stadler M., Piveteau J.-M. and Camenisch J.. Fair Blind Signatures. EUROCRYPT'95, LNCS 921, Springer-Verlag, pp. 209-219.

[22] S. Brands, Untraceable Off-line cash in wallet with observers, Advances in Cryptology-Crypto'93, LNCS 773, Springer, pp. 302-318.

[23] Masayuki Abe, Eiichiro Fujisaki, How to Date Blind Signatures, Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology'96, pp. 244-251.

[24] G. Maitland and C. Boyd, A provably secure restrictive partyially blind signature scheme, PKC 2002, LNCS 2274, Springer, pp. 99-114.

[25] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto'84, LNCS 196, Springer, pp. 47-53.

[26] M. Bellare and S.K. Miner. A forward-secure digital signature scheme. Advances in Cryptology-Crypto'99, LNCS 1666, Springer, pp. 431-448.

[27] Guilin Wang. Designated-Verifier Proxy Signature Schemes. Security and Privacy in the Age of Ubiquitous Computing (IFIP/ SEC 2005), Springer, pp. 409-423.

[28] H.U. Park and I.Y. Lee, A digital nominative proxy signature scheme for mobile communication,Proc. of ICICS 2001, International Conference on Information and Communications Security, LNCS 2229, Springer, pp. 451-455.

[29] Sung-Hyun Yun, Hyung-Woo Lee: The Undeniable Multi-signature Scheme Suitable for Joint Copyright Protection on Digital Contents. PCM (3) 2004, pp. 402-409.

[30] JiGuo Li, ZhenFu Cao, YiChen Zhang. Nonrepudiable proxy multi-signature scheme, Journal of Computer Science and Technology archive Volume 18 , Issue 3 (May 2003) pp. 399-402.

[31] Xiaofeng Chen, Fangguo Zhang, and Kwangjo Kim. ID-based Multi-Proxy Signature and Blind Multisignature from Bilinear Pairings. In KIISC conference 2003, Korea, August 17, 2003, pp. 11-19.

[32] W. Juang, C. Lei, Blind threshold signatures based on discrete logarithm, Proc. Second Asian Computing Science Conference on Programming, Concurrency and Parallelism, Networking and Security, LNCS 1179, Springer, New York, 1996, pp. 172-181.

[33] W.S. Juang, C.L. Lei. Partyially blind threshold signatures based on discrete logarithm, Computer Communications 22 (1999), pp. 73-86.

[34] Anna Lysyanskaya and Zulfikar Ramzan. Group Blind Digital Signatures: A Scalable Solution to Electronic Cash. Financial Cryptography, Second International Conference, 1998, LNCS 1465, Springer, pp. 184-197.

[35] Tony K. Chan, Karyin Fung, Joseph K. Liu, and Victor K. Wei. Blind Spontaneous Anonymous Group Signatures for Ad Hoc Groups. Security in Ad-hoc and Sensor Networks, First European Workshop, ESAS 2004, LNCS 3313, Springer, pp. 82-94.

[36] Zuowen Tan, Zhuojun Liu and Chunming Tang. A proxy blind signature scheme based on DLP. Journal of Software, 2003,14(11), pp. 1931-1935.

[37] A. K. Awasthi and Sunder Lal, Id-based ring signature and proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive, Report 2004/184, http://eprint.iacr.org/2004/184.

[38] Sherman S.M. Chow, Lucas C.K. Hui, and S.M. Yiu. Identity Based Threshold Ring Signature. Cryptology ePrint Archive, Report 2004/179, http://eprint.iacr.org/2004/179.

[39] Jing Xu, Zhenfeng Zhang, Dengguo Feng. ID-Based Proxy Signature Using Bilinear Pairings. Cryptology ePrint Archive, Report 2004/206, http://eprint.iacr.org/2004/206.

[40] Jing Xu, Zhenfeng Zhang, and Dengguo Feng. Identity Based Threshold Proxy Signature. Cryptology ePrint Archive, Report 2004/250, http://eprint.iacr.org/2004/250.

[41] Fangguo Zhang, Kwangjo Kim: ID-Based Blind Signature and Ring Signature from Pairings. ASIACRYPT 2002, pp. 533-547.

[42] Xiaofeng Chen , Fangguo Zhang and Shengli Liu. ID-based Restrictive Partyially Blind Signatures. Cryptology ePrint Archive, Report 2005/319, http://eprint.iacr.org/2005/319.

[43] S.M. Chow, C.K. Hui, S.M. Yiu and K.P. Chow, Two improved partyially blind signature schemes from bilinear pairings, ACISP 2005, LNCS 3574, Springer, pp. 316-328.

[44] Dawn Xiaodong Song. Practical Forward Secure Group Signature Schemes. Proceedings of the 8th ACM conference on Computer and Communications Security, 2001, ACM Press, pp. 225-234.

[45] Joseph K. Liu and Duncan S. Wong. Solutions to Key Exposure Problem in Ring Signature. Cryptology ePrint Archive, Report 2005/427, http://eprint.iacr.org/2005/427.

[46] Ming-Yang Chen, A Research of Forward Secure Proxy Signature Scheme, Master's Thesis, 2003, etdncku.lib.ncku.edu.tw/ETD-db.

[47] Dang Nguyen Duc, Iung Hee Cheon, Kwangjo Kim. A forward-secure blind signature scheme based on the strong RSA Assumption. Information and Communications Secureity'2003, ICICS 2003, Springer, pp. 11-21.

[48] Zheng Dong, Huang Zheng, Kefei Chen, Weidong Kou. ID-Based Proxy Blind Signature, 18th International Conference on Advanced Information Networking and Applications (AINA'04) Volume 2, 380, 2004.

[49] K. Nybergk, R. Rueppelra. "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem" Advances in Cryptology-Crypto'93, Spinger, pp. 182-193.

[50] Birgit Pfitzmann, Michael Waidner. Fail-stop signatures and their application. Proc. of 9th Worldwide Congress on Computer and Communications Security and Protection (Securicom'91), pp. 145-160.

[51] W.Diffie and M.E.Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, IT-22, 6, 1976, 644–654.

Appendix: some literatures on I-sort signature models

• **Multi-signature** In 1983, Itakura and Nakamura [1] introduced the model. In a multi-signature scheme, plural signers can jointly and efficiently sign an identical message.

• **Threshold signature** In 1989, Y. Desmedt and Y. Frankel [2] introduced the model. A (t, n) threshold signature allows t or more members of the group cooperate to generate a signature on behalf of the group.

• **Group signature** In 1991, Chaum and van Heijst [3] introduced the model. A group signature scheme allows any member of a group to digitally sign a document in a manner such that a verifier can confirm that it came from the group, but does not know which individual in the group signed the document. The protocol allows for the identity of the signer to be discovered, in case of disputes, by a designated group authority that has some auxiliary information.

• **Threshold group signature** In 1997, Camenisch [4] introduced the model. A (t, n) threshold group signature scheme is a generalization of group signature, in which only t or more members from a given group with n members can represent the group to generate signatures anonymously and the identities of signers of a signature can be revealed in case of dispute later.

• **Ring signature** In 2001, Rivest, Shamir and Tauman [5] introduced the model. A ring signature can be considered as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism against signer's anonymity. It allows any member of a group to sign a message such that the resulting signature does not reveal the identity of the group member who actually created the signature (anonymity) and no one can tell if two signatures are created by the same signer (unlinkability).

• **Linkable ring signature** The notion of linkable ring signature, introduced by Liu et al. [6] in 2004, is a variant of ring signature. It allows anyone to determine whether two signatures have been issued by the same group member (linkability).

• **Threshold ring signature** In 2002, E. Bresson, J. Stern, and M. Szydlo [7] introduced the model. In a threshold ring signature scheme, any group of t entities spontaneously conscript arbitrarily $n - t$ entities to generate a publicly verifiable t-out-of-n signature on behalf of the whole group, yet the actual signers remain anonymous.

• **Linkable threshold ring signature** In 2004, Liu et al. [6] introduced the model.

• **Proxy signature** In 1996, Mambo, Usuda and Okamoto [8] introduced the model. It enables a proxy signer to sign messages on behalf of an original signer. Proxy signature schemes have been shown to be useful in many applications. For example, a manager can delegate his secretaries to sign documents when he is on vacation.

• **Multi-proxy signature** In 2001, J. Hwang, and C.H. Shi [9] introduced the model. It allows an original signer delegate its signing power to a specified proxy group while ensuring individual accountability of each participant signer.

• **Threshold proxy signature** In 1997, Zhang and Kim [10] introduced the model. A (t, n) threshold proxy signature scheme enables an original signer to delegate the signature authority to a proxy group of n member such that t or more than t proxy signers can cooperatively sign messages on behalf of the original signer.

• **Proxy ring signature** In 2003, Zhang et al [11] introduced the model. It can be viewed as the combination of proxy signature and ring signature. It should satisfy all the requirements of general proxy signature, beside, it should satisfy the additional requirements: Signer ambiguity, i.e., the adversary (include the original signer) cannot tell the identity of the signer.

• **Poxy multi-signature** In 2000, L. Yi et al. [12] introduced the model. In a proxy multi-signature scheme, an original signer group can authorize one person as its proxy signer. For example, there is a dispute between some employees and the employer. All employees want to depute a famous lawyer as their agent. So, the lawyer is authorized to act on behalf of them.

• **Multi-proxy multi-signature** In 2001, J. Hwang, and C.H. Chen [13] introduced the model. In a multi-proxy multi-signature scheme, the original group is able to authorize a group of proxy signers as its agent. The authorization agreement should be reached by all of signers in the original group. Only with the cooperation of all signers in the original group, the proxy group is able to generate a proxy signature on behalf of the original group.

• **Threshold proxy multi-signature** In 2004, Tzeng et al. [14] introduced the model. In such model, any t or more of the proxy singers can cooperatively sign messages on behalf of the original group.

• **Designated-verifier signature** In 1996, Jakobsson, Sako and Impagliazzo [15] introduced the concept of designated-verifier signature (DVS) scheme. A DVS scheme makes it possible for a prover Alice to convince a designated verifier Bob that she has signed a statement so that Bob cannot transfer the signature to a third party Dave. Moreover, Alice can prove to Dave that a simulated signature was not created by Bob, while she can not disavow her own signatures.

• **Multiple designated-verifier signature** In [15], Jakobsson, Sako and Impagliazzo also suggested an extension of their protocol to multiple designated-verifiers. It allows the signer choose to sign a message for some designated verifiers.

• **Nominee signature** In 1996, S.J.Kim, S.J.Park and D.H.Won introduced the nominee signature (they called it nominative signature), in which only the nominee can verify and prove the validity of given signatures.

• **Undeniable signature** In 1989, Chaum and V. Antwerpen [18] introduced the model. It is a non-self-authenticating signature scheme, where signatures can only be verified with the signer's consent. However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the disavowal protocol in addition to the normal components of signature and verification.

• **Confirming signature** In 1994, Chaum [19] introduced the model (he called it designated-confirmer signature). A confirming signature allows certain designated partyies to confirm the authenticity of a document without the need for the signer's input. At the same time, without the aid of the designated partyies, it is not possible to verify the authenticity of a given document. Chaum also developed implementations of designated confirmer signatures with one or more confirmers.

- **Blind signature** In 1983, Chaum [20] introduced the model. It allows a person to get a message signed by another partyy without revealing any information about the message to the other partyy. Blind signatures have numerous uses including anonymous access control and digital cash.

- **Fair blind signature** In 1995, M. Stadler, J.M. Piveteau and J. Camenisch [21] introduced the model. In comparison with a blind signature scheme, a fair blind signature scheme has the additional property that a trusted entity can deliver information allowing the signer to link his view of the protocol and the message-signature pair.

- **Restrictive blind signature** In 1993, Brands [22] introduced the model. It allows a recipient to receive a blind signature on a message not known to the signer but the choice of message is restricted and must conform to certain rules.

- **Partially blind signature** In 1996, Abe and Fujisaki[23] introduce the model. A partially blind signature scheme allows the signer to inoculate a non-removable common information into his blind signature. This common information may represent the date or the amount of e-cash. Due to its untraceablility and partyial blindness property, the partially blind signature plays an important role in many e-commerce applications.

- **Restrictive partially blind signature** In 2002, Maitland and Boyd [24] introduced the model in order to incorporating the restrictive property into a partially blind signature scheme.

- **ID-based signature** In public key cryptosystem, each user has two keys, a private key and a public key. The binding between the public key and the identity of a user is obtained via a digital certificate. As a consequence, this system requires a large amount of storage when the number of users increase rapidly. In 1984, Shamir [25] asked for ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting.

- **Forward-secure signature** In 1999, M. Bellare and S.K. Miner [26] introduced a forward-secure signature scheme. The secret signing key is updated at regular intervals so as to provide a forward security property. That means compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be useful to mitigate the damage caused by key exposure without requiring distribution of keys.