Taxonomie digitaler Signaturkonzepte[2]

Holger Petersen[1] · Markus Michels · Patrick Horster

Theoretische Informatik und Informationssicherheit
Technische Universität Chemnitz-Zwickau
Straße der Nationen 62, 09111 Chemnitz
E-Mail: {hpe,mmi,pho}@informatik.tu-chemnitz.de

Zusammenfassung

In diesem Beitrag werden Konzepte digitaler Signaturverfahren klassifiziert. Dabei werden Verifikations-, Verbindlichkeits- , Blindungs- sowie Mehrparteienkonzepte unterschieden. Außerdem betrachten wir Systeme, bei denen Generierung oder Verifikation mehrerer Signaturen in einem Schritt zusammengefaßt werden. Die hier getroffene Auswahl orientiert sich an bereits existierenden Konzepten und wurde erweitert. Die vorgestellten Unterscheidungen lassen sich weiter verfeinern. Die Konzepte lassen sich kombinieren und führen so zu einer Großzahl möglicher Signaturkonzepte. Weiterhin werden die aus der Literatur bekannten Signaturkonzepte in die Klassifikation eingebettet.

1 Einleitung

Bei einer konventionellen digitalen Signatur wird eine Nachricht von einem Unterzeichner mit Hilfe eines geheimen Schlüssels signiert, so daß ein beliebiger Überprüfer – der Verifizierer – in der Lage ist, die Authentizität der Nachricht unter Verwendung des authentischen öffentlichen Schlüssels des Signierers zu überprüfen.

Eine konventionelle digitale Signatur soll bei elektronischen Daten die Funktionalität einer *eigenhändigen Unterschrift* möglichst gut abbilden. Natürlich ist dieses nicht in jeder Hinsicht möglich. Die eigenhändige, handschriftliche Unterschrift hat die Funktion der schriftlichen Zustimmung zum Inhalt eines Dokuments (Abschlußfunktion). Durch ihre Charakteristik ist die Verbindung zwischen dem Unterzeichner und dem unterschriebenen

[1]derzeitige Adresse: Ecole Normale Supérieure, Laboratoire d'informatique, 45, rue d'Ulm, F-75230 Paris Cedex 05, Frankreich, E-Mail: Holger.Petersen@ens.fr

[2]appeared in Proc. Digitale Signaturen, Darmstadt, Vieweg Verlag, (1996).

Dokument auch im Nachhinein für Dritte verifizierbar (Echtheits- und Beweisfunktion). Ein durch eine digitale Signatur unterzeichnetes Dokument muß eindeutig dem Unterzeichner zuordbar sein (Identitätsfunktion), d.h. die Authentizität des Unterzeichners ist verifizierbar. Die Zustimmung zum Inhalt des Dokuments, der bei einem handschriftlichen Dokument eventuell auch noch nachträglich geändert oder ergänzt werden kann, ist durch die *Integrität* einer digitalen Signatur im hohem Maße gewährleistet.

In Anwendungsfällen ist es häufig sinnvoll, anstelle der konventionellen digitalen Signatur ein modifiziertes Konzept digitaler Signaturen einzusetzen. Bei einem Blindungskonzept werden Parameter so modifiziert, daß sie für den Unterzeichner der Nachricht nicht sichtbar sind. So können zur Anonymitätswahrung Blindungskonzepte eingesetzt werden. Bei Mehrparteienkonzepten wird die Anzahl der benötigten Unterzeichner und Verifizierer erhöht, so daß diese nur gemeinsam in der Lage sind eine digitale Signatur zu generieren bzw. zu verifizieren. Dies kann zur Unterstützung von Geschäftsabläufen dienen, bei denen mehrere Personen dem Inhalt eines Dokuments zustimmen müssen. Daneben kann die Menge der möglichen Verifizierer einer digitalen Signatur eingeschränkt werden, was zu unterschiedlichen Verifizierkonzepten führt. Bei einem Verbindlichkeitskonzept wird die dauerhafte Überprüfbarkeit einer digitalen Signatur eingeschränkt, was in unterschiedlichen Abstufungen möglich ist.

Die Verifizier- und Verbindlichkeitskonzepte bezeichnen wir zusammenfassend als Eigenschaftskonzepte. Zusammen mit den Blindungs- und Mehrparteienkonzepten ergibt sich die in Abbildung 1 dargestellte Taxonomie von Signaturkonzepten.

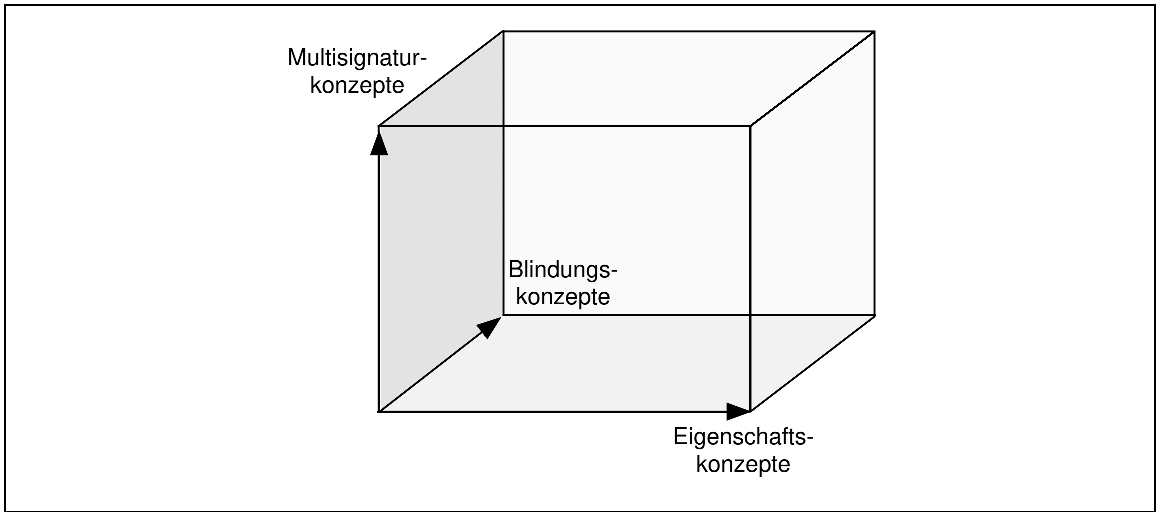

Abbildung 1: Taxonomie von Signaturkonzepten

Die hier getroffene Auswahl der Aspekte orientiert sich an bereits existierenden Konzepten und wurde erweitert. Die bei den einzelnen Konzepten vorgestellten Unterscheidungen können weiter verfeinert werden. Die Verfeinerung ist ein dynamischer Prozeß, der 20 Jahre nach Erfindung der Public-Key-Kryptographie sicherlich noch nicht als abgeschlossen angesehen werden kann. Insofern ist die hier gezeigte Klassifizierung als Bestandsaufnahme und nicht als statische Taxonomie aufzufassen. Sie ermöglicht eine systematische, maßgeschneiderte Herleitung unterschiedlicher Signaturkonzepte für die jeweilige Anwendung.

2 Notation

Eine *digitales Signaturverfahren* besteht aus folgenden Bestandteilen [15]:

- Einem *Nachrichtenraum*, der die Menge der möglichen Nachrichten m spezifiziert.
- Einem *Schlüsselgenerierungsalgorithmus*, der die Systemparameter sowie jedem Unterzeichner ein oder mehrere asymmetrische Schlüsselpaare (x, y) erzeugt. Die geheimen Schlüssel werden mit x, die öffentlichen Schlüssel mit y bezeichnet.
- Einem *Signieralgorithmus* $\mathcal{S}$, der die *digitale Signatur* $\sigma := \mathcal{S}(x, m)$ zur Nachricht m erzeugt.
- Einem *Verifikationsalgorithmus* $\mathcal{V}$, mit dem die digitale Signatur überprüft wird, sein Resultat beschreibt das Prädikat $V(y, m, \sigma) \in \{true, false\}$.
- Einem *Sicherheitsparameter* t, der die Größe relevanter Parameter beeinflußt, wie etwa die Länge der Signatur oder die Größe des verwendeten Moduls.

In der Regel liegen die Nachrichten in einem Redundanzschema R, wie etwa einer natürlichen Sprache. Die Algorithmen $\mathcal{S}$ und $\mathcal{V}$ müssen für jedes Signaturverfahren existieren und effizient berechenbar sein. Das Tupel (m, σ) wird als *signierte Nachricht* bezeichnet. Der Signieralgorithmus $\mathcal{S}$ kann derart probabilistisch sein, daß er bei mehrmaligem Signieren der gleichen Nachricht m unterschiedliche Signaturen erzeugt. Dabei ist ein Pseudozufallsgenerator integraler Bestandteil des Signieralgorithmus.

Es lassen sich zwei Arten von Signaturverfahren unterscheiden:

1. *Signaturverfahren mit Anhang*, die sich dadurch auszeichnen, daß die Nachricht zur Verifikation explizit benötigt wird und daher dem Verifizierer bekannt sein muß.
2. *Signaturverfahren mit Nachrichtenrückgewinnung*, die sich dadurch auszeichnen, daß die Nachricht aus der Signatur berechnet wird und daher dem Verifizierer nicht explizit mitgeteilt werden muß.

Während in den Signaturverfahren mit Nachrichtenrückgewinnung stets die Originalnachricht unterschrieben wird, kann bei den Signaturverfahren mit Anhang auch der Hashwert einer Nachricht unterschrieben werden. Dies hat den Vorteil, daß eine Signatur bei langen Nachrichten effizienter generiert und verifiziert werden kann. Zusätzlich können die Schwächen, die durch eine eventuell vorhandene mathematische Struktur des Signatursystems in der Signatur vorhanden ist, zerstört werden.

Der Verifizierer muß den öffentlichen Schlüssel des Signierers authentisch kennen, um die Authentizität der signierten Nachricht zu prüfen. Um dies zu gewährleisten, ist die Authentizität des öffentlichen Schlüssels y des Signierers etwa durch eine Signatur einer *Zertifizierungsinstanz* auf y und weitere Parameter (etwa Gültigkeitdauer, Identität des Signierers) zu gewährleisten. Dieses wird *Zertifikat* genannt. Ein Signaturverfahren wird durch Angabe der Algorithmen zur Überprüfung der Zeritifkate, der *Systemparametererzeugung, Schlüsselerzeugung, Signaturgenerierung* und *Signaturverifikation* beschrieben.

Konventionelles Signaturkonzept

Wird in der Praxis von digitalen Signaturen gesprochen, so ist zumeist das konventionelle Signaturkonzept von Diffie und Hellman gemeint [11], das sich durch folgende Eigenschaften auszeichnet:

1. *Jeder* Systembenutzer, der den öffentlichen, authentischen Schlüssel des Signierers kennt (der Verifizierer), kann eine gegebene Signatur auf Gültigkeit überprüfen.
2. Die Überprüfung ist dem Verifizierer *jederzeit* möglich.
3. Der Signierer *kennt* die zu unterzeichnende *Nachricht.*
4. Der Signierer *kennt* die generierte *Signatur.*
5. Die *Identität des Signierers* ist dem Verifizierer bekannt.
6. Zur Signaturgenerierung ist *ein* Signierer erforderlich.
7. Zur Signaturverifikation ist genau *ein* Verifizierer erforderlich.
8. Der Signierer signiert die Nachricht *selbst.*
9. Der Signierer *generiert* die Signatur auf Ressourcen, denen er vertraut (etwa, daß sie seinen geheimen Schlüssel nicht kompromittieren).
10. Der Verifizierer überprüft die Signatur *selbst.*

Das Prinzip eines konventionellen digitalen Signaturverfahrens wird in Abbildung 2 verdeutlicht.

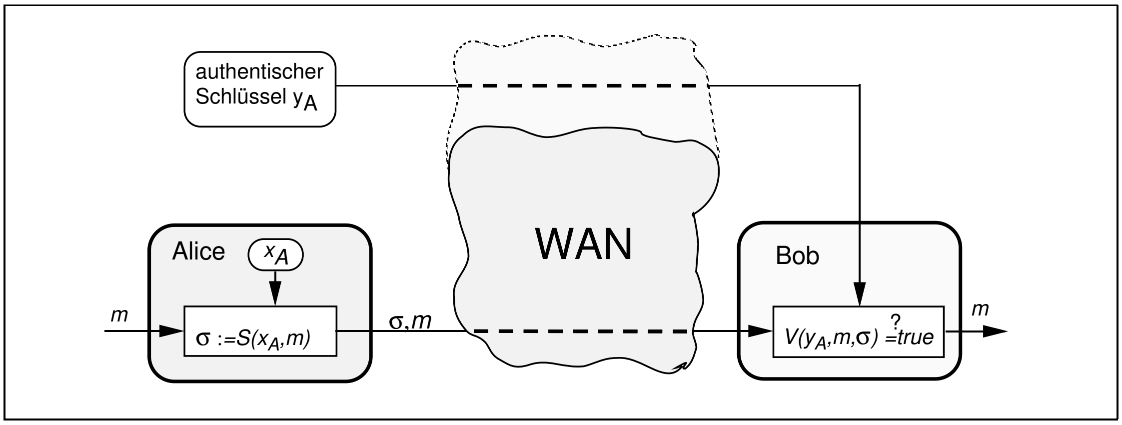

Abbildung 2: Prinzip eines konventionellen digitalen Signaturverfahrens

Durch Modifikation dieser Eigenschaften lassen sich eine Vielzahl alternativer Signaturkonzepte herleiten. Die Eigenschaftskonzepte modifizieren die ersten beiden Eigenschaften, die Blindungskonzepte die dritte und vierte sowie die Mehrparteienkonzepte die fünfte bis siebte Eigenschaft. Die achte und neunte Eigenschaft werden durch das Konzept der Proxy-Signaturen sowie die Signaturen mit ausgelagerter Berechnung modifiziert. Die letzte Eigenschaft wird bei den Signaturen mit ausgelagerter Verifikation modifiziert.

3 Eigenschaftskonzepte

Die Eigenschaftskonzepte, durch die die beiden ersten Eigenschaften des konventionellen Signaturkonzepts modifiziert wird, lassen sich in Verifizier- und Verbindlichkeitskonzepte unterscheiden, die miteinander kombiniert werden können.

Verifizierkonzepte

Diese Konzepte zeichnen sich dadurch aus, daß ein autorisierter Verifizierer die Signatur überprüfen oder die übermittelte Nachricht lesen kann.

1. *Konventionelle Signatur:* Die Überprüfung der Signatur ist durch jeden Systembenutzer möglich.

2. *Empfängerspezifische Signatur:* Die Überprüfung der Signatur ist nur dem autorisierten Verifizierer möglich [17].

3. *Signierte Verschlüsselung:* Das Lesen der Nachricht ist nur dem autorisierten Empfänger, die Überprüfung der Signatur ist durch jeden Systembenutzer möglich [31]. Hierbei muß sichergestellt werden, daß die Signatur zu einem gegebenen Chiffrat nicht unbemerkt durch eine Signatur eines anderen Systemteilnehmers ersetzt werden kann, d.h. es muß ein mathematischer Zusammenhang zwischen den Signaturparametern und dem Chiffrat bestehen, den der autorisierte Empfänger überprüfen kann.

4. *Verschlüsselte Signatur:* Das Lesen der Nachricht sowie die anschließende Überprüfung der Signatur sind nur dem autorisierten Empfänger möglich [31].

Die Verifizierkonzepte werden in Abbildung 3 zusammengefaßt.

Signatur / **Nachricht**	von jedem verifizierbar	nur vom ausgezeichneten Verifizierer überprüfbar
von jedem lesbar	herkömmliche digitale Signatur	empfängerspezifische digitale Signatur
nur vom ausgezeichneten Empfänger lesbar	signierte Verschlüsselung	verschlüsselte Signatur

Abbildung 3: Verifizierkonzepte

Umwandlung einer Signatur

Bei einigen Anwendungen kann eine nachträgliche Umwandlung einer Signatur in eine konventionelle digitale Signatur sinnvoll sein, um die Nichtabstreitbarkeit (Non-Repudiation) der Signatur gegenüber einer dritten Person zu erreichen. Dabei sind folgende Umwandlungsstufen möglich:

1. *Keine Umwandlung möglich:* Der Signierer verwendet ein Signaturverfahren, das keine Umwandlung erlaubt.

2. *Selektive Umwandlung:* Der Signierer erlaubt dem Verifizierer die Umwandlung einer einzelnen Signatur bzw. einer festen Menge von Signaturen, um diese gegenüber einer dritten Person zu beweisen. Dies stellt ihre Nichtabstreitbarkeit sicher [28]

3. *Totale Umwandlung:* Der Signierer ermöglicht die totale Umwandlung aller von ihm für einen speziellen Verifizierer geleisteten Signaturen.

4. *Globale Umwandlung:* Der Signierer ermöglicht die totale Umwandlung aller von ihm jemals geleisteten Signaturen für ausgezeichnete Verifizierer.

Verbindlichkeitskonzepte

Diese Konzepte modifizieren die zweite Eigenschaft des konventionellen Signaturkonzepts. Der Signierer kann entscheiden, ob und wann die Überprüfung einer digitalen Signatur einem Verifizierer möglich sein soll. Dies führt zu unterschiedlichen Verbindlichkeitskonzepten, die in der Regel die Beweisfunktion der digitalen Signatur abschwächen.

1. *Interaktiver Beweis:* Die Gültigkeit der Signatur wird durch einen interaktiven Beweis, wie etwa einen Zero-Knowledge-Beweis, gezeigt. Insbesondere gibt hierbei der Signierer die Signatur nicht preis. Hierdurch kann sich lediglich der Verifizierer von der Authentizität der Nachricht überzeugen. Er erhält keine Beweismittel, die er zum Beweis gegenüber einer dritten Person benötigen würde. Dadurch ist der Beweis für den Signierer nicht bindend - er kann zu einem späteren Zeitpunkt die Teilnahme verweigern oder den Beweis absichtlich falsch ausführen, ohne daß ihm dieses nachgewiesen werden kann. Daher eignet sich das Konzept nur zur Authentitätssicherung einer augenblicklichen Willensäußerung [14].

2. *Unleugbare Signatur:* Die Signatur wird interaktiv verifiziert, wobei der Unterzeichner eine geleistete Signatur nicht ableugnen kann, sofern er am Verifikationsprotokoll teilnimmt. Seine Teilnahme bei der Verifikation kann jedoch nicht erzwungen werden, daher muß eine organisatorische Regelung (etwa eine Strafe) für den Fall getroffen werden, daß er hierfür nicht verfügbar ist [6].

3. *Designated Confirmer Signatur:* Hierbei handelt es sich um ein Signaturprotokoll, bei dem drei Parteien involviert sind. Der Signierer signiert die Nachricht mit einer unleugbaren Signatur und schickt die Signatur an einen Verifizierer. Zur Verifikation der Signatur wird die Hilfe eines Confirmers benötigt, der Informationen über die Signatur vom Signierer erhalten hat. Es wird angenommen, daß der Confirmer verfügbar ist. Daher ist die Verbindlichkeit einer einmal geleisteten Signatur

sichergestellt. Der Verifizierer alleine kann jedoch nicht uneingeschränkt zu jedem Zeitpunkt die Korrektheit einer Signatur beweisen [5].

4. *Konventionelle Signatur:* In folge der Kenntnis aller Systemparameter ist ein Verifizierer in der Lage, die Korrektheit einer signierten Nachricht gegenüber Dritten zu beweisen.

Die Verbindlichkeitskonzepte werden in Abbildung 4 zusammengefaßt, wobei ein interaktiver Beweis keine und eine konventionelle Signatur hohe Verbindlichkeit gewährleisten soll.

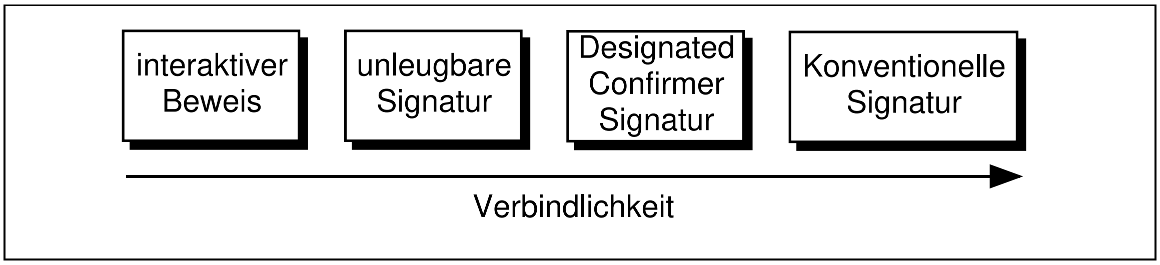

Abbildung 4: Verbindlichkeitskonzepte

Umwandlung einer Signatur

Der Signierer könnte an einer Umwandlung einer unleugbaren Signatur bzw. einer Designated Confirmer Signatur in eine konventionelle digitale Signatur interessiert sein. Hierfür sind folgende Umwandlungskonzepte möglich:

1. *Keine Umwandlung möglich:* Ein Verifizierer kann die Gültigkeit einer unleugbaren Signatur gegenüber einer dritten Person nicht beweisen.

2. *Keine Umwandlung vorgesehen:* Der Signierer verwendet ein Signaturverfahren, das keine Umwandlung vorsieht. Durch geeignete Protokollvarianten können sich jedoch gleichzeitig mehrere Verifizierer von der Korrektheit der geleisteten Signatur überzeugen [6].

3. *Selektive Umwandlung:* Der Signierer ermöglicht die Umwandlung einer einzelnen Signatur bzw. einer festgelegten Menge von Signaturen durch Bekanntgabe zusätzlicher geheimer Parameter [1].

4. *Totale Umwandlung:* Der Signierer ermöglicht die Umwandlung aller von ihm geleisteten unleugbaren Signaturen durch Bekanntgabe zusätzlicher geheimer Parameter [1].

4 Blindungskonzepte

Bei blinden Signaturen existieren drei Parteien: Der *Notar*, der eine Nachricht oder verdeckte Nachricht signiert, der *Besitzer* der aufgedeckten Nachricht und der *Verifizierer*, der die Signatur zur aufgedeckten Nachricht überprüft. Der Verifizierer und der Notar können eine Person sein. Es ergeben sich folgende Blindungskonzepte:

1. *Konventionelle Signatur:* Der Signierer erfüllt die Funktionalität vom Notar und Besitzer der Nachricht, d.h. er kennt die Nachricht und die Signatur.

2. *Verdeckte Signatur:* Bei diesem Konzept lassen sich in zwei Typen unterscheiden [18]:

   (a) *Nachrichtenverdeckende Signaturen:* Der Notar erfährt bei der Unterzeichnung die Nachricht nicht, er kann die Signatur jedoch anhand der Signaturparameter wiedererkennen.

   (b) *Parameterverdeckende Signaturen:* Der Notar erfährt bei der Unterzeichnung die Signaturparameter nicht, er kann die Signatur jedoch anhand der Nachricht wiedererkennen.

3. *Schwach blinde Signatur:* Die Nachricht und die Signaturparameter werden verdeckt, so daß der Notar die Signatur nur noch anhand der unverdeckten Parameter identifizieren kann [18].

4. *Restriktiv stark blinde Signatur:* Die Nachricht besitzt eine feste Struktur, die sich auf die geblindete Nachricht überträgt. Die Struktur ist somit invariant unter der Blindung. Ansonsten besitzt sie die Eigenschaften einer stark blinden Signatur [3].

5. *Stark blinde Signatur:* Die Nachricht und alle Signaturparameter werden verdeckt, so daß für den Notar keine Relation zwischen der blind unterschriebenen und einer aufgedeckten signierten Nachricht herstellbar ist [4].

6. *Vergeßlich übertragene, blinde Signatur:* Vergeßliche Übertragungsprotokolle zeichnen sich dadurch aus, daß der Sender nicht weiß, welche Werte der Empfänger wirklich erhält. Bei vergeßlich übertragenen Signaturen *bezüglich der Nachrichten* erhält der Empfänger eine Signatur zu einer Nachricht aus einer Anzahl von Nachrichten. Der Signierer weiß nach Ablauf des Protokolls nicht, zu welcher Nachricht der Empfänger eine Signatur kennt. Bei vergeßlich übertragenen Signaturen *bezüglich der Schlüssel* erhält der Empfänger eine Signatur zu einer bestimmten Nachricht, die mit einem geheimen Schlüssel aus einer Anzahl geheimer Schlüssel signiert ist. Der Signierer weiß nach Ablauf des Protokolls nicht, mit welchem Schlüssel die dem Empfänger bekannte Signatur zur Nachricht generiert wurde [8].

Die unterschiedlichen Blindungskonzepte werden in Abbildung 5 verdeutlicht.

Aufhebung der Blindungseigenschaft

Hierbei wird eine geblindete digitale Signatur in eine konventionelle Signatur überführt. Bei den ersten drei Konzepten ist die Aufhebung der Blindungseigenschaft implizit gegeben. Wir besschränken uns daher auf die Betrachtug der letzten drei Blindungskonzepte.

1. *Aufhebung nicht möglich:* Die stark blinde Signatur kann nicht nachträglich in eine konventionelle Signatur überführt werden [4].

2. *Selektive Aufhebung der Blindung:* Hierbei kann die Aufhebung mit Hilfe bzw. ohne Hilfe des Besitzers geschehen:

Signatur Nachricht	offen	verdeckt
offen	herkömmliche digitale Signatur	parameter-verdeckende Signatur
verdeckt	nachrichten-verdeckende Signatur	schwach/ stark blinde Signatur

Abbildung 5: Blindungskonzepte

(a) *Mit Hilfe des Besitzers:* Der Besitzer der Nachricht kann die Blindung durch Bekanntgabe von Protokolldaten gegenüber dem Notar aufdecken. Dies geschieht jedoch freiwillig und kann vom Notar nicht erzwungen werden. Daher läßt sich dieses Konzept nur dann anwenden, wenn der Besitzer ein Interesse an der Aufhebung der Blindung hat.

(b) *Ohne Hilfe des Besitzers:* Die Blindung einer stark blinde Signatur kann von einem Treuhänder im Falle eines Betrugsverdachtes aufgehoben werden, so daß der Notar den Zusammenhang zwischen der von ihm unterschriebenen und der vorgelegten signierten Nachricht erkennen kann. Das Konzept wird als *fair blinde Signatur* bezeichnet [33].

3. *Totales Aufheben der Blindung:* Die Blindung aller blinden Signaturen eines Besitzers können von einem Treuhänder aufgehoben werden, unabhängig davon, welcher Notar unterzeichnet hat.

5 Mehrparteiensignaturkonzepte

Im konventionellen Signaturkonzept wird ein Signierer zur Generierung einer Signatur und ein Verifizierer zu ihrer Überprüfung benötigt. In einigen Anwendungen ist es erforderlich, daß *mehrere* Signierer eine Signatur gemeinsam generieren bzw. *mehrere* Verifizierer gemeinsam eine gegebene Signatur auf Gültigkeit überprüfen. Diese Konzepte werden unter dem Oberbegriff *Mehrparteiensignaturkonzepte* zusammengefaßt. Sie wirken sich auf die Parametererzeugung, Schlüsselerzeugung, Signaturgenerierung und Verifikation aus:

1. *Systemparametererzeugung:* Diese werden üblicherweise von einer Zertifizierungsinstanz für alle Systembenutzer einheitlich erzeugt. Es sind jedoch auch Mehrparteienkonzepte denkbar, bei denen mehrere Benutzer gemeinsam die Systemparameter erzeugen bzw. nur gemeinsam Kenntnis von diesen haben.

2. *Schlüsselerzeugung:* Beim konventionellen Signaturkonzept hat jeder Benutzer ein eigenes Schlüsselpaar. Dieses kann bei Mehrparteiensignaturverfahren etwa so mod-

ifiziert werden, daß die Teilnehmer einer Gruppe ein gemeinsames Gruppenschlüsselpaar besitzen.

Es ist sinnvoll, zwischen *Gruppen-* und *Nichtgruppen*signaturverfahren zu unterscheiden. Ein Gruppensignaturverfahren zeichnet sich dadurch aus, daß n_1 Signierer bzw. n_2 Verifizierer eine Gruppe bilden, was durch einen gemeinsamen öffentlichen Gruppenschlüssel (nicht zu verwechseln mit einem gemeinsamen Sitzungsschlüssel) zum Ausdruck kommt. Der geheime Gruppenschlüssel wird unter den Teilnehmern aufgeteilt. Nun können $1 \leq t_1 \leq n_1$ Signierer eine Signatur (anonym) generieren bzw. $1 \leq t_2 \leq n_2$ Verifizierer eine Signatur überprüfen. In Nichtgruppensignaturverfahren gibt es keinen Gruppenschlüssel. t_1 Teilnehmer können gemeinsam eine Signatur generieren bzw. t_2 Teilnehmer gemeinsam verifizieren, wozu sie jeweils ihr eigenes Schlüsselpaar benutzen.

3. *Signaturgenerierung:* Führt zu Signaturverfahren mit Multisignaturgenerierung, etwa Multisignaturen oder Schwellwertsignaturverfahren.

4. *Signaturverifikation:* Führt zu Signaturverfahren mit Multiverifikation, wie etwa Schwellwertsignaturverfahren.

Nichtgruppenkonzepte

Beispiele für Nichtgruppensignaturverfahren sind Signaturverfahren mit Multisignaturgenerierung, auch *Multisignaturverfahren* genannt. Dieses Konzept zeichnet sich dadurch aus, daß t_1 Signierer die gleiche Nachricht gemeinsam signieren, wobei ihre Identität bekannt ist [20]. Sollen hingegen t_2 Verifizierer nur gleichzeitig in der Lage sein, eine Signatur zu verifizieren, so ergibt sich ein *Signaturverfahren mit Multiverifikation* [34]. Für den Fall $t_1 = t_2 = 1$ ergibt sich das konventionelle Signaturkonzept.

Gruppenkonzepte

In Gruppensignaturverfahren signieren t_1 bzw. verifizieren t_2 der $n_i, i \in \{1, 2\}$ Gruppenmitglieder eine Nachricht, wobei t_i fest gewählt wird. Ferner kann das Konzept nach der Anonymität der signierenden Gruppenmitglieder unterteilt werden. Hieraus ergeben sich drei *Signierkonzepte*. Es wird $t := t_1$ und $n := n_1$ gewählt.

1. *Gruppensignaturverfahren mit (t, n) nicht-anonymer Signaturgenerierung*, in dem mindestens t von n Signierern zur Generierung einer Signatur benötigt werden und bei denen der Verifizierer erfährt, welche Signierer eine bestimmte Signatur generiert haben [24].

2. *Gruppensignaturverfahren mit (t, n) anonymer Signaturgenerierung*, in dem mindestens t von n Signierern zur Generierung einer Signatur benötigt werden und bei denen der Verifizierer *nicht* erfährt, welche Signierer eine bestimmte Signatur generiert haben [10].

3. *Gruppensignaturverfahren mit (t, n) aufhebbarer, anonymer Signaturgenerierung*, in dem mindestens t von n Signierern zur Generierung einer Signatur benötigt werden

und bei denen der Verifizierer zunächst *nicht* erfährt, welche Signierer eine bestimmte Signatur generiert haben (vgl. [7] für t=1). Die Anonymität kann unter bestimmten Voraussetzungen aufgehoben werden:

(a) *Selektive Aufhebung:* Eine Gruppe bestimmt einen ausgezeichneten Systembenutzer als Gruppenleiter, der für eine einzelne Signatur im Zweifel die Identitäten der t Signierer aufdecken kann. Es hängt dann vom Anwendungsfall ab, ob er die Identitäten an den Verifizierer weitergibt und/oder ihm gegenüber auch beweist.

(b) *Totale Aufhebung:* Die totale Aufhebung der Anonymität ist ebenfalls denkbar, so daß für alle Signaturen feststellbar ist, von wem sie geleistet wurden.

Die Klassifikation der Signierkonzepte ist in Abbildung 6 zusammengefaßt.

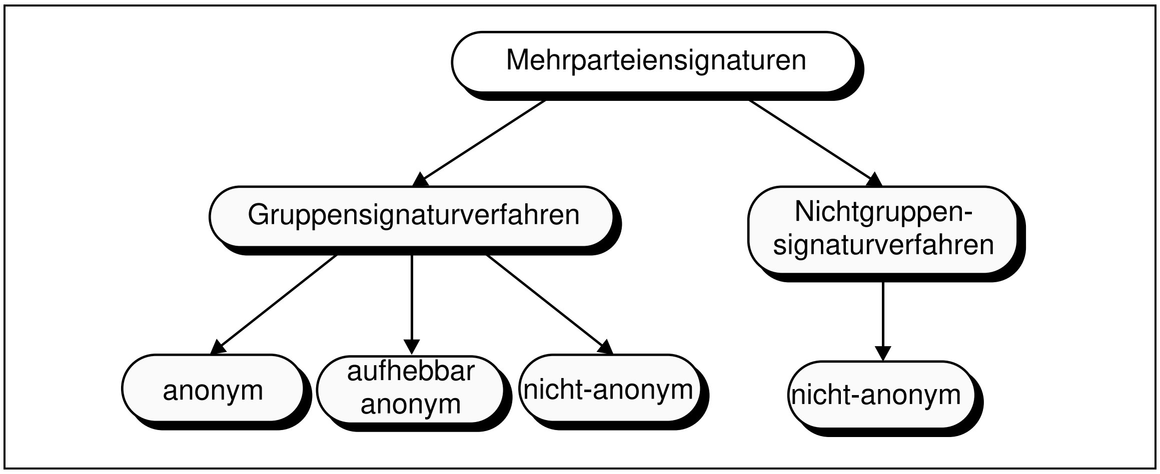

Abbildung 6: Signierkonzepte

In der Praxis wird der Fall $t = 1$ häufig gesondert betrachtet, da für ihn effiziente Realisierungen existieren. Der Fall $t = n$ existiert nur nicht-anonym, da hier alle n Teilnehmer der Gruppe unterzeichnen und somit nicht mehr anonym sind. Für $n_1 = n_2 = 1$ ergibt sich das konventionelle Signaturkonzept.

Ist n_1 gleich der Anzahl der Systembenutzer, so gibt es keine außenstehenden Verifizierer. Damit ist jeder Verifizierer Mitglied der Gruppe. Dieses Konzept eignet sich bei anonymer Signaturgenerierung etwa zur Einreichung einer anonymen Beschwerde, bei der die Gruppenteilnehmer die Information erhalten, daß t_1 ihrer Mitglieder eine bestimmte Beschwerde eingereicht haben, ohne sie jedoch namentlich zu kennen.

Abbildung 7 faßt die unterschiedlichen Konzepte tabellarisch zusammen. Die beiden ersten Spalten bezeichnen Signaturverfahren mit Nichtgruppen-Signaturgenerierung, die beiden ersten Zeilen Signaturverfahren mit Nichtgruppen-Signaturverifikation. Jedes Feld der Tabelle beschreibt ein Mehrparteiensignaturkonzept, so daß sich insgesamt 28 dieser Konzepte ergeben. So bezeichnet etwa das Feld A das bekannte Multisignaturkonzept, bei dem t_1 Signierer eine Nachricht gemeinsam unterzeichnen und das Feld B ein Gruppensignaturverfahren mit $(1, n_1)$ anonymer Signaturgenerierung und (t_2, n_2) anonymer Signaturverifikation.

Eine mögliche Erweiterung der Gruppenkonzepte besteht in der Ersetzung der t_1 aus n_1 Signierer bzw. t_2 aus n_2 Verifizierer durch beliebige inhomogene Kontrollstrukturen.

Mehrparteien-signatur konzepte		Anzahl der Signierer						
		nicht anonym			aufhebbar anonym		anonym	
		1	t_1	t_1 aus n_1	1 aus n_1	t_1 aus n_1	1 aus n_1	t_1 aus n_1
Anzahl der Verifizierer	1		A					
	t_2							
	1 aus n_2							
	t_2 aus n_2						B	

Abbildung 7: Mehrparteiensignaturkonzepte

So könnten etwa wahlweise $t_{1,1}$ aus $n_{1,1}$ Signierern oder $t_{1,2}$ aus $n_{1,2}$ Signierern, wobei diese Mengen nicht disjunkt sein müssen. Hierzu gibt es bisher noch keine Vorschläge.

6 Weitere Konzepte

Neben den bisher charakterisierten Konzepten wurden weitere Einzelkonzepte vorgeschlagen, die hier charakterisiert werden.

- *Proxy-Signaturen:* Der Signierer delegiert einen Stellvertreter, der für ihn Nachrichten unterzeichnen kann. Der Verifizierer kann die vom Stellvertreter geleistete digitale Signatur von einer eigenhändig geleisteten Signatur anhand des öffentlichen Schlüssels unterscheiden. Dies modifiziert die achte Eigenschaft des konventionellen Signaturkonzepts [25].

- *Verzögerte Signaturen:* Der Signierer leistet eine Blankosignatur, die später vom Verifizierer mit einer Nachricht einer speziellen Form ausgefüllt werden kann. Dies modifiziert die dritte Eigenschaft des konventionellen Signaturkonzepts.

- *Signaturverfahren mit stark begrenzter Signaturanzahl:* Der Signierer kann nur eine begrenzte Anzahl von Signaturen leisten (engl. signature scheme with bounded life-span) [9].

- *Signaturen mit ausgelagerter Berechnung:* Hierbei werden die achte und neunte Eigenschaft der konventionellen Signaturen modifiziert. Der Signierer verfügt selbst nicht über hinreichende Ressourcen und lagert die Signaturberechnung daher auf einen *nicht vertrauenswürdigen* Server aus. Dabei darf er zum einen seinen geheimen Schlüssel nicht preisgeben und muß andererseits in der Lage sein, das Resultat der ausgelagerten Berechnung zu verifizieren [26].

- *Signaturen mit ausgelagerter Signaturbildung:* Hierbei wird die achte Eigenschaft des konventionellen Signaturkonzepts modifiziert. Der Signierer lagert die Signaturberechnung auf einen *vertrauenswürdigen* Server aus, der seinen geheimen Schlüssel kennt.

- *Signaturen mit ausgelagerter Signaturverifikation:* Der Verifizierer verfügt selbst nicht über hinreichende Ressourcen und lagert die Signaturverifikation auf einen Server aus. Dabei muß er in der Lage sein, das Resultat der ausgelagerten Berechnung verifizieren zu können.

Die ersten drei sowie das sechste Konzepte lassen sich untereinander kombinieren, vom vierten und fünften Konzept kann eines wahlweise hinzugenommen werden. Dieses führt insgesamt zu 48 Konzepten.

7 Weitere Aspekte

Es lassen sich die mehrfache Generierung und Verifikation von Signaturen unterscheiden. Die mehrfache Generierung erlaubt die effiziente Generierung einer großen Anzahl von Signaturen durch den selben Signierer, etwa mittels Vorberechnung. Die gleichzeitige Überprüfung mehrerer Signaturen (Batch-Verifikation) durch einen Verifizierer soll die Überprüfung beschleunigen.

Batch-Generierung

Bei deterministischen Signaturverfahren im konventionellen Signaturkonzept, wie etwa dem RSA-Signaturverfahren, kann die Batch-Generierung von Signaturen erfolgen, indem die Signierfunktion für mehrere Signaturen zusammengefaßt wird [13]. Bei probabilistischen Signaturverfahren kann die Generierung der Pseudozufallszahlen und der aus ihnen abgeleiteten Berechnungen, wie z.B. Exponentiationen, durch einen Vorberechnungsalgorithmus vereinfacht werden. Dabei muß darauf geachtet werden, daß beispielsweise die Auswahl von Pseudozufallszahlen aus Effizienzgründen nicht so stark eingeschränkt wird, daß hierdurch Unsicherheiten beim verwendeten Signaturverfahren resultieren.

Batch-Verifikation

Zur Batch-Verifikation werden die Signaturparameter der einzelnen Signaturen mit zufälligen Faktoren gewichtet und anschließend geeignet zusammengefaßt, so daß sie gemeinsam überprüft werden können. Durch die Gewichtung wird ein Angriff über einen linearen Zusammenhang zwischen den Signaturparametern mit hoher Wahrscheinlichkeit vereitelt [27].

Sicherheitsebenen

Neben den unterschiedlichen Signaturkonzepten lassen sich unterschiedliche Sicherheitsebenen, auf denen ein Signaturverfahren implementiert werden kann, unterscheiden.

1. *Heuristisch sicher:* Es sind keine effizienten Algorithmen zum Brechen des Verfahrens bekannt. Beispiele hierfür sind das RSA- oder das ElGamal-Signaturverfahren [31, 12].

2. *Komplexitätstheoretisch sicher:* Die Sicherheit ist auf ein komplexitätstheoretisch schweres Problem reduzierbar. Zur Verfügung stehen hier etwa das Faktorisierungsproblem oder das diskrete Logarithmusproblem [15].

3. *Informationstheoretisch sicher:* Die Sicherheit beruht nicht auf kryptographischen Annahmen. One-time Signaturen bzw. Fail-stop Signaturen sind typische Beispiele hierfür [23, 30].

Wünschenswert sind effiziente und gleichzeitig informationstheoretisch sichere Verfahren. Es existieren jedoch keine praxisrelevanten Verfahren, stattdessen bieten die meisten praktisch eingesetzten Verfahren lediglich heuristische Sicherheit. Dabei besteht ein Dualismus zwischen der Sicherheit und dem Aufwand der Verfahren, der in der Praxis meistens zugunsten der Effizienz entschieden wird (etwa beim weltweit eingesetzten RSA- oder DSA-Verfahren).

Zusammenfassung

Wir haben eine Klassifizierung digitaler Signaturverfahren nach den unterschiedlichen Konzepten vorgenommen. Dabei konnten wir drei Verifizierkonzepte zusammen mit vier Arten ihrer Umwandlung, insgesamt also *9 Verifizierkonzepte* unterscheiden. Ferner wurden drei Verbindlichkeitskonzepte vorgestellt, die zusammen mit den vier Umwandlungsmöglichkeiten zu *neun Verbindlichkeitskonzepten* führen. Für die Blindung digitaler Signaturen ergeben sich sechs Blindungskonzepte, zusammen mit vier Deanonymisierungskonzepten ergeben sich *15 Blindungskonzepte.* Ferner ergeben sich *28 Mehrparteiensignaturkonzepte* sowie *sechs* weitere Konzepte, die nicht in die bisherigen Klassen einzuordnen sind und die untereinander kombiniert zu 48 weiteren Konzepten führen. Da alle Konzepte miteinander kombinierbar sind, ergeben sich theoretisch etwa 1.6 Millionen Konzepte digitaler Signaturverfahren. Bei Betrachtung dieser riesigen Anzahl ist zu berücksichtigen, daß ein hoher Prozentsatz dieser Konzepte praktisch bisher keine Anwendung besitzt. Es sind erst knapp über 30 Konzepte in der Literatur beschrieben worden, die durch Problemstellungen aus dem täglichen Leben motiviert waren. Andererseits ermöglicht der systematische Zugang zu der Vielzahl von Konzepten erst die Entwicklung anwendungsbezogener, maßgeschneideter Signaturkonzepte und deren Realisierungen, wie es etwa im Falle des Konzepts der blinden Multisignaturen der Fall war, das gewinnbringend in einem neuen Wahlverfahren Verwendung fand [19]. Es ist eine zukünftige Aufgabe, weitere interessante Anwendungen auf der Basis eines der neuen Konzepte zu finden.

Literatur

[1] J.Boyar, D.Chaum, I.Damgard, T.Pedersen, „Convertible undeniable signatures“, Lecture Notes in Computer Science 537, Advances in Cryptology: Proc. Crypto '90, Springer Verlag, (1991), S. 189–205.

[2] C.Boyd, „Digital multisignatures“, in H.J.Beker, F.C.Piper „Cryptography and Coding“, Clarendon Press, Oxford, (1989), S. 241–246.

[3] S.Brands, „Untraceable Off-Line Cash in Wallets with Observers“, Lecture Notes in Computer Science 773, Advances in Cryptology: Proc. Crypto '93, Springer Verlag, (1994), S. 302 – 318.

[4] D.Chaum, „Blind signatures for untraceable payments“, Advances in Cryptology: Proc. Crypto ’82, Plenum Press, (1983), S. 199–203.

[5] D.Chaum, „Designated Confirmer Signatures“, Lecture Notes in Computer Science 950, Advances in Cryptology: Proc. Eurocrypt’94, Springer Verlag, (1995), S. 86–91.

[6] D.Chaum, H.van Antwerpen, „Undeniable Signatures“, Lecture Notes in Computer Science 435, Advances in Cryptology: Proc. Crypto ’89, Springer Verlag, (1990), S. 212–216.

[7] D.Chaum, E.van Heijst, „Group signatures“, Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt ’91, Springer Verlag, (1992), S. 257–265.

[8] L.Chen, „Oblivious Signatures“, Lecture Notes in Computer Science 875, Proc. Computer Security–ESORICS’94, Springer Verlag, (1994), S. 161–172.

[9] O.Delos, J.J.Quisquater, „An Identity-Based Signature Scheme with Bounded Life-Span“, Lecture Notes in Computer Science 839, Advances in Cryptology: Proc. Crypto’93, Springer Verlag, (1995), S. 83–94.

[10] Y.Desmedt, Y.Frankel, „Threshold cryptosystems“, Lecture Notes in Computer Science 435, Advances in Cryptology: Proc. Crypto’89, Springer Verlag, (1990), S. 307–315.

[11] W.Diffie, M.Hellman, „New directions in cryptography“, IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November, (1976), S. 644–654.

[12] T.ElGamal, „A public key cryptosystem and a signature scheme based on discrete logarithms“, IEEE Transactions on Information Theory, Vol. IT-30, No. 4, Juli, (1985), S. 469–472.

[13] A.Fiat, „Batch RSA“, Lecture Notes in Computer Science , Advances in Cryptology: Proc. Crypto ’89, Springer Verlag, (1990), S. 175–185.

[14] S.Goldwasser, S.Micali, C.Rackoff, „Knowledge complexity of interactive proofs“, Proc. of the 17th ACM Symposium on Theory of Computing, Providence, RI, 6.–8. Mai, New York: Association for Computer Machinery, (1985), S. 291–304.

[15] S.Goldwasser, S.Micali, R.Rivest, „A secure digital signature scheme“, SIAM Journal on Computing, Vol. 17, 2, (1988), S. 281–308.

[16] L.Harn, S.Yang „Group-oriented undeniable signature schemes without the assistance of a mutually trusted party“, Lecture Notes in Computer Science 718, Advances in Cryptology: Proc. Auscrypt ’92, Springer Verlag, (1992), S. 133–142.

[17] P.Horster, M.Michels, H.Petersen, „Das Meta-ElGamal Signaturverfahren und seine Anwendungen“, Proc. VIS’ 95, Rostock, DuD Fachbeiträge, Vieweg Verlag, (1995), S. 207–228.

[18] P.Horster, M.Michels, H.Petersen, „Hidden signature schemes based on the discrete logarithm problem and related concepts“, Proc. Communications and Multimedia Security, Chapman & Hall, September, (1995), S. 162–177.

[19] P.Horster, M.Michels, H.Petersen, „Blind multisignature schemes and their relevance to electronic voting“, Proc. 11th Annual Computer Security Applications Conference, IEEE Press, Dezember, (1995), S. 149–156.

[20] K.Itakura, K.Nakamura, „A public key cryptosystem suitable for digital multisignatures“, NEC J. Res. Dev. 71, Oktober, (1983).

[21] M.Jakobsson, K.Sako, R.Impagliazzo, „Designatred Verifier Proofs and Their Applications“, Lecture Notes in Computer Science 1070, Advances in Cryptology: Proc. Eurocrypt '96, Springer Verlag, (1996), S.143–154.

[22] L.M.Kohnfelder, „On the Signature Reblocking Problem in Public-Key Cryptosystems“, CACM, Vol. 21, No. 2, (1978), S.179.

[23] L.Lamport, „Constructing digital signatures from a one-way function“, Technical Report SRI International, CSL 98, (1979).

[24] C.M.Li, T.Hwang, N.Y.Lee, „Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders“, Lecture Notes in Computer Science 950, Advances in Cryptology: Proc. Eurpcrypt '94, Springer Verlag, (1995), S. 194–204.

[25] M.Mambo, K.Usuda, E.Okamoto, „Proxy Signatures for Delegating Signing Operation“, 3rd ACM Conference on Computer and Communications Security, ACM Press, (1996), S. 48–57.

[26] T.Matsumoto, K.Kato, H.Imai, „Speeding up secret computations with insecure auxiliary devices“, Advances in Cryptology: Proc. Crypto '88, Lecture Notes in Computer Science 403, 1988, S. 497–506.

[27] D.Naccache, D.M'Raihi, S.Vaudenay, D.Raphaeli, „Can D.S.A. be improved? – Complexity Trade-Offs with the Digital Signature Standard“, Lecture Notes in Computer Science 950, Advances in Cryptology: Proc. Eurocrypt '94, Springer Verlag, (1995), S. 77–85.

[28] K.Nyberg, R.Rueppel, „Message recovery for signature schemes based on the discrete logarithm problem“, Vorabdruck, erscheint in Designs, Codes and Cryptography, (1994), 15 Seiten.

[29] T.P.Pedersen, „Distributed provers with applications to undeniable signatures“, Lecture Notes in Computer Science 547, Advances in Cryptology: Proc. Eurocrypt '91, Springer Verlag, (1992), S. 221–242.

[30] B.Pfitzmann, M.Waidner, „Fail-stop signatures und ihre Anwendungen“, Verläßliche Informationssysteme: VIS '91, Informatik Fachberichte 271, Springer Verlag, (1991), S. 289–301.

[31] R.L.Rivest, A.Shamir, L.Adleman, „A method for obtaining digital signatures and public-key cryptosystems“, Comm. of the ACM, Vol. 21, (1978), S. 120–126.

[32] M.de Soete, J.Quisquater, K.Vedder, „A signature with shared verification scheme“, Lecture Notes in Computer Science 435, Advances in Cryptology: Proc. Crypto '89, Springer Verlag, (1989), S. 253–262.

[33] M.A.Stadler, J.-M.Piveteau, J.L.Camenisch, „Fair blind signatures“, Lecture Notes in Computer Science 921, Advances in Cryptology: Proc. Eurocrypt '95, Springer Verlag, (1995), S. 209–219.

[34] S.M.Yen, C.S.Laih, „Multi-Signature for specified groups of verifiers“, (1995), Vorabdruck, 10 Seiten.