Verlusttolerante elektronische Brieftaschen*

Michael Waidner, Birgit Pfitzmann

Abstrakt: *Will man mit einem Zahlungssystem sowohl über ein Kommunikationsnetz als auch off-line Zahlungen durchführen können, so ist man auf „elektronische Brieftaschen", sichere Geräte, die für die Rechtmäßigkeit digitaler Zahlungen garantieren, angewiesen. Neben der Verläßlichkeit der physikalischen Sicherheitstechnik ist bei diesen vor allem die Tolerierung von Verlusten oder vollständigen Ausfällen, mit denen ohne Fehlertoleranzmaßnahmen ein Verlust von Geld verbunden wäre, ein Problem. Wir untersuchen die prinzipiellen Möglichkeiten für solche Verlusttoleranzmaßnahmen, wobei wir neben der Sicherheit auch den Datenschutz der Teilnehmer berücksichtigen, und geben einige Verfahren hierzu an. Es zeigt sich, daß mit dem Prinzip der markierten Standardwerttransaktionen verläßliche Verlusttoleranzverfahren konstruiert werden können, die die sonstigen Eigenschaften elektronischer Brieftaschen kaum beeinträchtigen.*

1 Motivation

Mit der Einführung eines neuen Kommunikationssystems durch die Deutsche Bundespost, des ISDN (integrated services digital network), wird zugleich die Grundlage für die Einführung eines offenen digitalen Systems gelegt, das potentiell allen Benutzern des ISDN zugänglich sein und spezielle Dienste anbieten soll. Möglich wären reine Informationsdienste, etwa in der Nachfolge von Bildschirmtext, die ihren Benutzern spezielle Datenbanken zugänglich machen, die Verbreitung von POS-Terminals oder „elektronische Marktplätze" [Riha_85, TuCh_85], die ihren Teilnehmern das Anbieten und Bestellen von Waren, das Überweisen von Geld, kurz das Abwickeln von Rechtsgeschäften verschiedenster Art erlauben.

Diese Rechtsgeschäfte müssen einerseits in der gewohnten Rechtssicherheit abgewickelt werden können. Andererseits könnte die Integration vieler zuvor getrennter Dienste in einem offenen System einem Beobachter das Erstellen von Persönlichkeitsbildern erlauben. Da rein juristische Regelungen den Datenschutz der Teilnehmer am offenen System nicht überprüfbar garantieren können, kommt nur eine technisch unterstützte Anonymisierung in Frage [PWP_87].

Eine der Grundvoraussetzungen für das Abwickeln vieler Rechtsgeschäfte über ein offenes digitales System ist die Existenz eines sicheren und anonymen digitalen Zahlungssystems. Um eine Zahlung lediglich durch Austausch von Information rechtssicher leisten zu können, muß für die Gültigkeit dieser Zahlung ein Dritter garantieren.

Werden an die Kommunikation zwischen dem garantierenden Dritten und den Zahlungspartnern keine speziellen Anforderungen gestellt, so kann man ihn als zentrale Instanz im Zahlungssystem, als „Bank" wählen, mit der für jede Zahlung mindestens einer der Zahlungspartner kommunizieren muß (on-line Systeme). Für diesen Fall sind Zahlungssysteme bekannt, deren Sicherheit und Anonymität rein auf kryptographischen Techniken beruhen [BüPf_86, Chau_85, PWP_87].

Sollen Zahlungen jedoch auch off-line, also von Teilnehmer zu Teilnehmer ohne Einschalten Dritter erfolgen können, so bleibt nur der Rückgriff auf „elektronische Brieftaschen" (electronic wallet, [EvGY_84]), tragbare und hinreichend billige sichere Geräte, die für die Gültigkeit der Zahlungen garantieren. Die Literatur kennt hierzu einige Vorschläge, teils nicht-anonymer [EvGY_84], teils anonymer [BüPf_86, PWP_87] Art. Man könnte elektronische Brieftaschen hinsichtlich ihrer Funktion als Miniaturfilialen einer Bank auffassen, die jeweils genau ein Konto verwalten, nämlich das ihres Besitzers.

Zahlungssysteme, die auf sicheren Geräten basieren, haben gegenüber den nur auf kryptographischen Techniken beruhenden Systemen jedoch auch einige gravierende Nachteile:

- Die Eigenschaft „sicher" eines Gerätes bedeutet, daß das Gerät
  - einerseits gewisse Informationen enthält und verarbeitet, die vom Betreiber des Systems vorgegeben werden, aber zur Gewährleistung der Betrugssicherheit vor dem Besitzer des Gerätes verborgen bleiben müssen (Ausforschungssicherheit), da dieser sonst selbst Geräte nachbauen könnte, und
  - andererseits gewisse Informationen über den Besitzer erhält, die aus Datenschutzgründen und aus Gründen der Betrugssicherheit der Besitzer vor dem Betreiber verborgen bleiben müssen (keine Trojanischen Pferde, [PoKl_78]).

  Geräte, die zumindest die Ausforschungssicherheit vor dem Besitzer garantieren sollen, werden in der Praxis unter dem Namen „Chipkarte" bereits eingesetzt, z.B. zur Zugangskontrolle oder als intelligente Telefonwertkarte [Schr_86, Wein_84]. Dennoch ist unserer Meinung nach höchst ungewiß, ob Geräte, auf deren Ausforschungssicherheit Verlaß ist, physikalisch realisierbar sind.

* Dies ist eine geringfügig überarbeitete Fassung unseres Beitrages zur „3rd International Conference on Fault-Tolerant Computing-Systems", 9. bis 11. September 1987, Bremerhaven

Ein sicheres Gerät muß sich (seiner Einsatzweise entsprechend) im Besitz seines Benutzers befinden, so daß dieser die physikalische Kontrolle über sein Gerät hat und dieses (insbesondere auch während sein Gerät gerade arbeitet) beliebig manipulieren und beobachten kann. Jede Verarbeitung von Information bewirkt aber zwangsläufig einen Energietransport innerhalb des Gerätes. Um ein Messen der Energietransporte (z.B. über elektromagnetische Abstrahlung) zu verhindern, muß das Gerät hinreichend gut abgeschirmt werden. Da ein Besitzer auch versuchen kann, sein Gerät durch zerstörendes Messen auszuforschen, muß ein sicheres Gerät zudem bemerken, wenn seine Schutzmechanismen von außen beeinträchtigt werden. In einem solchen Fall (und auch, wenn seine Funktion aufgrund eines internen Fehlers beeinträchtigt ist) muß das sichere Gerät sich selbst sofort unbrauchbar machen, d.h. seine geheimen Informationen löschen.

Damit ist ein Wettlauf zwischen Konstrukteuren sicherer Geräte und der Meßtechnik festgeschrieben, den vermutlich keiner von beiden auf Dauer gewinnt.

Aber selbst wenn ihn die Konstrukteure gewönnen, so müßten sowohl die Banken als auch die Benutzer auf die Korrektheit der sicheren Geräte vertrauen können. Da von einem sicheren Gerät kaum nachgeprüft werden kann, daß es wirklich sicher ist (oder vielmehr war, denn es soll ja ausforschungssicher sein und würde eine solche Anzweiflung seiner Funktion mit einer sofortigen Aufgabe derselben honorieren), müßten die sicheren Geräte von Organisationen, denen alle Beteiligten vertrauen wollen, hergestellt werden. Damit das Vertrauen in die Organisationen etwas gerechtfertigter wird, sollten die sicheren Geräte nach allgemein bekannten und hinreichend auf Trojanische Pferde untersuchten Entwürfen und unter gegenseitiger Kontrolle aller Organisationen hergestellt werden.

Um den Beteiligten zu ermöglichen, ein vermeintlich sicheres Gerät als ein von den Organisationen hergestelltes und damit „echtes" zu verifizieren, müßte sich dieses „ausweisen". Zu diesem Zweck könnten die Organisationen eine Signaturfunktion [Denn_82, PlLe_86] wählen, sie allen Geräten hinzufügen und die zugehörende Testfunktion allgemein bekanntmachen. Ist garantiert, daß ein vermeintlich echtes Gerät keinen Kontakt mit anderen, echten Geräten hat, und kann es beliebige vorgegebene Werte korrekt unterschreiben, so kann es als echt betrachtet werden.

Trotz unserer starken Zweifel an der Realisierbarkeit sicherer Geräte wird deren Existenz im folgenden als gegeben angenommen. Dazu beachte man jedoch, daß ein sicheres Gerät zur Erfüllung der Ausforschungssicherheit im Gegensatz zu heutigen Chipkarten zumindest etwa dieselben Verarbeitungs- und Speicherfähigkeiten besitzen muß wie heutige PCs, da ansonsten vertrauliche Daten außerhalb des sicheren Gerätes verarbeitet werden müßten. Auch muß es zum Schutz seines Besitzers mittels eigener Tastatur und eigener Anzeige direkt mit ihm kommunizieren können, so daß es äußerlich eher einem Taschenrechner als einer heutigen Chipkarte gleichen wird.

- Auch sichere Geräte machen den Einsatz kryptographischer Verfahren nicht überflüssig, da elektronische Brieftaschen auch fähig sein sollen, über einen unsicheren Kanal, z.B. ein Kommunikationsnetz, zu kommunizieren, so daß eine gegenseitige Authentikation notwendig ist. Zahlungssysteme, die auf sicheren Geräten basieren, sind daher keinesfalls sicherer als solche, die rein auf kryptographischen Verfahren beruhen.
- Wird ein sicheres Gerät als elektronische Brieftasche verwendet, so bedeutet dies, daß mit dem Ausfall des Gerätes durch Verlust oder Fehler zunächst ein Verlust von Geld verbunden ist. Bei Systemen, die ohne sichere Geräte auskommen, tritt dieses Problem lediglich hinsichtlich der Daten der Systemteilnehmer (Bank und Teilnehmer) auf, gegen deren Verlust man sich aber durch Einsatz von Standardmethoden der Fehlertoleranz, z.B. mehrfaches Abspeichern, leicht schützen kann. Außerdem ist der Verlust eines als elektronische Brieftasche verwendeten sicheren Gerätes wahrscheinlicher als der eines gewöhnlichen Datenträgers, ebenso der Ausfall, da es sich schon aufgrund kleinster Fehler selbst unbrauchbar machen muß.

Die Behebung des dritten Nachteils unter Wahrung der Anonymität und Sicherheit, Verlusttoleranz genannt, ist der Gegenstand dieser Arbeit. Die Sicherheit der Geräte und der verwendeten kryptographischen Hilfsmittel wird als gegeben vorausgesetzt.

2 Zahlungen mit elektronischen Brieftaschen

Zu einem sicheren Gerät G bezeichne B_G dessen Besitzer. Jedes sichere Gerät hat nur einen Besitzer, aber ein Teilnehmer am Zahlungssystem kann natürlich mehrere sichere Geräte gleichzeitig verwenden.

Der Kontostand K_G von G sei ein in G gespeicherter Wert, der stets angeben soll, bis zu welcher Höhe B_G mittels G eine Zahlung vornehmen kann. Damit muß nicht zwischen sogenannten Kredit- und Debitkarten unterschieden werden.

Der Betreiber des Zahlungssystems werde Bank genannt.

Ein sicheres und anonymes Zahlungssystem mit elektronischen Brieftaschen sollte folgenden Anforderungen genügen:

Betrugssicherheit: Ein sicheres Gerät G verringert K_G um einen Betrag b ($b \geqslant 0$) genau dann, wenn B_G den Auftrag zu dieser Zahlung erteilt hat, wenn $b \leqslant K_G$ und wenn es sicher ist, daß ein anderes sicheres Gerät seinen Kontostand entsprechend um b erhöht.

Umgekehrt erhöht es K_G um b ($b \geqslant 0$) genau dann, wenn B_G den Auftrag zu diesem Empfang erteilt hat und wenn es sicher ist, daß ein anderes sicheres Gerät seinen Kontostand entsprechend um b verringert.

Aus diesen Forderungen läßt sich insbesondere ableiten, daß stets $K_G \geqslant 0$ gilt, falls dies zum Zeitpunkt der Initialisierung der Fall war. Solange nicht (mit Hilfe der Bank) Geld zwischen dem betrachteten Zahlungssystem und einem anderen transferiert wird, nimmt die Geldmenge im System (also die Summe aller K_G), keinesfalls zu; geht kein Gerät verloren, so ist sie sogar konstant.

Die Betrugssicherheit macht es insbesondere notwendig, daß fehlerhafte Geräte sicher ausfallen, d.h. wird ein Gerät defekt, so muß es dies selbst feststellen können und danach seine Funktionsfähigkeit verlieren (fail-stop processor, [Schn_83]). Damit unterscheidet sich ein Fehler nicht mehr prinzipiell von dem Verlust eines Gerätes.

Anonymität: Sind B_{G1} und B_{G2} Partner in einer Zahlung, so darf aus dem Wissen über das Zahlungssystem und die Zahlung weder B_{G1} zusätzliche Informationen über die Identität von B_{G2} bzw. G2 erhalten, noch umgekehrt B_{G2} über die von B_{G1} bzw. G1. Die Daten einer Zahlung

(Zeitpunkt, Beteiligte und Betrag) sowie der Zusammenhang zwischen verschiedenen Zahlungen müssen, wie dies bei Barzahlungen der Fall ist, vor der Bank vollständig verborgen bleiben.

Eventuelle Maßnahmen zur Tolerierung eines Fehlers oder des Verlustes eines Gerätes G sollten die Anonymität von B_G so wenig wie möglich und die aller anderen Teilnehmer überhaupt nicht beeinträchtigen.

Entscheidend für den Aufwand zur Anonymisierung ist, ob jemals Informationen über eine Zahlung von B_G außerhalb eines sicheren Gerätes von jemandem ungleich B_G wahrgenommen werden können.

Verwendet die Bank zur Interaktion mit sicheren Geräten ebenfalls ein (wenn auch sehr komplexes) sicheres Gerät, das Informationen auch vor ihr geheimhalten kann, so ist dies leicht zu verhindern; die Anonymisierung beschränkt sich darauf, die Kommunikation zwischen sicheren Geräten zu schützen.

Kann die Bank jedoch direkt mit sicheren Geräten interagieren, so kann sie evtl. als einzige Instanz sichere Geräte so nachahmen, daß sie die Daten erfährt, die ein Gerät zum Zwecke einer Transaktion von sich geben muß. In diesem Fall ist zu fordern, daß auch die Daten, die das Gerät G1 an ein anderes sicheres Gerät G2 weitergibt und die B_{G2} im Normalfall nicht erfährt, nicht allzuviel über den Besitzer B_{G1} aussagen.

Ebenfalls zu beachten ist, daß das Zahlungssystem keine Informationen über die Identität eines Teilnehmers verbergen kann, die auf anderem Wege bereits bekannt sind: Koppeln Teilnehmer B_{G1} und B_{G2} ihre Geräte zum Zwecke einer off-line-Zahlung direkt aneinander, so werden sie sich dabei natürlich sehen und bei späteren Gelegenheiten wiedererkennen können. Dasselbe gilt für Zahlungen über ein Kommunikationsnetz, das es dem Zahlungspartner oder auch Dritten (z.B. dem Netzbetreiber) erlaubt, die an einer Zahlung Beteiligten zu identifizieren. Um letzteres zu verhindern, muß für solche Zahlungen ein Datenschutz garantierendes Kommunikationsnetz [PfPW_86] verwendet werden.

Fähigkeit zu autonomen Zahlungen: Ein sicheres Gerät kann im Rahmen der oben genannten Bedingungen beliebig viele Zahlungen leisten und empfangen, ohne hierzu mit anderen als dem jeweiligen Partner kommunizieren zu müssen. Insbesondere ist zu einer Zahlung keine Kommunikation mit der Bank oder einer anderen zentralen Instanz erforderlich.

Diese Fähigkeit wird im folgenden als Autonomie bezeichnet.

Die Forderung nach Autonomie soll im folgenden als unabdingbar vorausgesetzt werden; ohne sie lassen sich andere, nur auf kryptographischen Verfahren beruhende und daher sicherere Zahlungssysteme konstruieren.

Das Grundschema eines auf sicheren Geräten basierenden Zahlungssystems, das die obigen Forderungen erfüllt, enthält folgende Teilprotokolle:

Initialisierung des sicheren Gerätes G durch die Bank und B_G

[1] Der Besitzer B_G legt der Bank ein „leeres" sicheres Gerät G vor, dessen Echtheit er bereits überprüft hat. G kann entweder ein neues oder aber ein altes Gerät B_G's sein, das ungültig wurde und jetzt neu initialisiert werden muß.

[2] Die Bank prüft ebenfalls die Echtheit von G und versorgt es mit einem allen Geräten gemeinsamen Schlüssel S eines symmetrischen Kryptosystems [Denn_82, Hors_85, LuRa_86], mit Hilfe dessen die Geräte später sicher und vertraulich miteinander kommunizieren können.

[3] B_G testet, ob die Bank G den richtigen Schlüssel S mitgeteilt hat (z.B. indem G den Wert des erhaltenen Schlüssels unter einer Einwegfunktion [Levi_85] ausgibt, den B_G mit dem bekannten Sollwert vergleichen kann) und G damit als von der Bank anerkanntes sicheres Gerät gilt.

[4] Die Bank legt den Anfangskontostand K_G fest.

[5] B_G versorgt G mit einem hinreichend langen Paßwort (PIN, personal identification number), das später B_G gegenüber G eindeutig ausweisen wird.

Zahlung von G1 an G2

[1] B_{G1} und B_{G2} koppeln ihre Geräte direkt oder über ein (Datenschutz garantierendes) Kommunikationsnetz aneinander.

[2] G1 und G2 authentizieren sich gegenseitig, d.h. jedes prüft, ob es sich beim Partner um ein von der Bank initialisiertes sicheres Gerät handelt.

Dies könnte etwa geschehen, indem sie sich gegenseitig mit S verschlüsselte Zufallszahlen senden und erwarten, daß diese in jeder Nachricht der laufenden Transaktion enthalten sind.

Eine Identifikation von G1 und G2 ist nicht notwendig und wird daher auch nicht vorgenommen.

[3] B_{G1} (bzw. B_{G2}) authentiziert sich durch Angabe seines Paßwortes gegenüber G1 (bzw. G2) als dessen rechtmäßiger Besitzer und erteilt einen Zahlungsauftrag (bzw. einen Empfangsauftrag) über einen Betrag b.

Dabei soll zwischen B_{G1} und G1 (bzw. B_{G2} und G2) eine direkte Kommunikation möglich sein, d.h. ein sicheres Gerät muß über eine eigene Tastatur und eine eigene Anzeige verfügen.

[4] G1 und G2 führen ein Austauschverfahren durch, das sichern soll, daß K_{G2} genau dann um b erhöht wird, wenn K_{G1} um b gesenkt wird, und das zumindest garantieren muß, daß die Erhöhung von K_{G2} nicht ohne Senkung von K_{G1} stattfindet.

Ein Beispiel eines solchen Austauschverfahrens ist im Text ausführlich beschrieben.

Ungültigwerden von G

[1] Nach einer von der Bank vorgegebenen Zeit wird ein sicheres Gerät G „ungültig", d.h. es erlaubt B_G keinerlei Transaktionen mehr, außer der, innerhalb einer ebenfalls von der Bank festgelegten Frist den sich in seinem Gerät befindlichen Restbetrag durch die Bank auf ein neues sicheres Gerät oder in ein anderes Zahlungssystem übertragen zu lassen.

Das neue sichere Gerät kann dabei natürlich auch das alte sein, nur daß dieses von der Bank neu initialisiert werden muß.

Protokollskizze 1 Grundschema für ein Zahlungssystem mit elektronischen Brieftaschen

Das Problem im Austauschverfahren in Schritt [4] des Zahlungsprotokolls, daß ein Gerät im Fall des Ausbleibens der letzten Nachricht nicht entscheiden kann, ob das andere die Transaktion abgeschlossen hat, kann in Anlehnung an [BüPf_86] folgendermaßen gelöst werden:

Falls die letzte Nachricht ausbleibt, so nimmt das Gerät G1, das sie erwartete, einen Blockierungszustand ein, aus dem es nur mit Hilfe der Bank wieder befreit werden kann. Ebenso handelt das andere Gerät G2, wenn die vorletzte Nachricht ausbleibt oder es am Senden der letzten Nachricht gehindert wird. (Bleibt eine frühere erwartete Nachricht aus, gilt die Transaktion als nicht ausgeführt.)

Wird der Bank ein blockiertes Gerät vorgelegt, so muß sie zunächst entscheiden können, ob auch das Partnergerät blockiert vorgelegt wurde. Dies kann in anonymer Weise anhand der in [2] ausgetauschten Zufallszahlen geschehen, die die Geräte zu diesem Zweck anzeigen müssen.

Sind beide Geräte vorgelegt, so läßt die Bank sie einfach die Transaktion zu Ende führen. Ist nur G1 vorgelegt, so ist die Transaktion aus Sicht von G2 beendet oder G2 ist verloren, so daß es in jedem Fall korrekt ist, die Transaktion auch auf G1 für gültig zu erklären. Hierzu muß G1 bereits alle für die Transaktion relevanten Daten besitzen (was auch sichert, daß B_{G2} der Zahlung zugestimmt hatte), d.h. die letzte Nachricht muß eine reine Quittungsnachricht sein. Ist nur G2 vorgelegt, so ist die Transaktion aus Sicht von G1 auf keinen Fall beendet, so daß die Bank sie auch auf G2 für ungültig erklärt.

Damit ist in jedem Fall ein Zustand erreicht, der auch bei korrekter Durchführung der Transaktion und evtl. anschließendem Verlieren eines Gerätes hätte auftreten können, so daß im folgenden Schritt [4] des Zahlungsprotokolls als unteilbar betrachtet werden kann.

Das Ungültigwerden eines Gerätes G ist theoretisch nicht notwendig, da G wie Bargeld eigentlich nur im Fehlerfall ausgetauscht werden muß. Da aber einerseits die Wahrscheinlichkeit eines erfolgreichen Angriffes gegen die Sicherheit des Gerätes (und auch der verwendeten Schlüssel) mit der Zeit immer größer wird und manche Verfahren zur Verlusttoleranz ein Ungültigwerden sowieso erforderlich machen, sei es hier bereits vorweggenommen.

Wie man leicht sieht, bedeutet ein Verlust des sicheren Gerätes G für B_G zunächst auch den Verlust des Kontoguthabens K_G, das in G verwaltet wird.

3 Prinzipielle Möglichkeiten zur Verlusttoleranz

Im folgenden wird versucht, ein betrugssicheres und anonymes Zahlungssystem mit sicheren Geräten verlusttolerant zu machen.

Unter dem Verlust eines sicheren Gerätes G soll dabei verstanden werden, daß der Besitzer B_G die Kontrolle über G verliert. Dabei ist es gleichgültig, ob er das Gerät verlegt oder ob es nur defekt wird (und aus Sicherheitsgründen keine Interaktionen mit der Umwelt mehr zuläßt).

Die Annahme der Betrugssicherheit impliziert, daß nach einem Verlust auch kein anderer die Kontrolle über G gewinnen kann. Nicht ausgeschlossen ist jedoch, daß B_G den Verlust nur vortäuscht, etwa in der Hoffnung, angeblich verlorenes Geld wiederzubekommen und zweimal ausgeben zu können oder um sein Gerät in aller Ruhe ausforschen zu können (daß er nach dem zerstörenden Ausforschen seines Gerätes mitzerstörtes Geld womöglich wiederbekommt, ist zwar ungerecht, bringt ihm aber keine Vorteile: er könnte ja auch vor dem Ausforschen sein Gerät bis auf einen sehr geringen Betrag, den er leicht verschmerzen kann, leeren).

Die erste Möglichkeit, sich gegen einen Verlust zu schützen, ist, diesen durch Fehlertoleranzmaßnahmen unwahrscheinlich zu machen:

Zum einen können die sicheren Geräte selbst intern beliebig fehlertolerant ausgelegt werden. Grenzen sind hier im wesentlichen durch die praktische Forderung, daß ein sicheres Gerät tragbar, also nicht allzu groß und schwer sein soll, gesetzt.

Zum anderen kann der Verlust eines sicheren Gerätes selbst maskiert werden, indem jeder Teilnehmer nicht nur ein Gerät, sondern z.B. gleich drei Geräte G_1, G_2, G_3 besitzt und für jede Transaktion stets zwei von drei Geräten benötigt werden. Ist (o.B.d.A.) G_1 verloren und war G_1 an der letzten Transaktion der drei Geräte zusammen mit G_2 beteiligt, so übernimmt G_3 den Zustand von G_2, so daß der Teilnehmer nun mit dem Paar (G_2, G_3) weiterhin Transaktionen vornehmen kann. (War G_1 an der letzten Transaktion nicht beteiligt, so ist nichts zu tun).

Ein solches 2-von-3-System ist hinsichtlich physikalischer Fehler sicher sinnvoll. Den Verlust eines Gerätes kann man damit allerdings selten tolerieren, da die 2-von3-Systemen eigene Annahme, daß Fehler unabhängig voneinander auftreten und Doppelfehler damit unwahrscheinlich sind, gerade hier nicht zutrifft. Verliert ein Teilnehmer eines seiner drei Geräte, so dürfte er zumindest ein anderes nicht weit vom ersten aufbewahrt haben, da er für jede Transaktion zwei Geräte benötigt, und damit häufig alle beide zusammen verlieren. Analoges gilt für n-von-m-Systeme (mit $n < m < 2n$), wo vermutlich häufig n Geräte gleichzeitig verloren gehen.

Im folgenden soll daher angenommen werden, daß ein Verlust von G stattgefunden und B_G damit die Kontrolle über G verloren hat.

Ein auf sicheren Geräten basierendes Zahlungssystem heiße verlusttolerant, wenn gilt:

> *Verliert B_G sein sicheres Gerät G, so kann er über K_G, zur Not mit einer gewissen „kleinen" Abweichung nach unten, deren Größe durch das Protokoll begrenzbar ist, innerhalb einer ebenfalls durch das Protokoll begrenzbaren Zeit wieder verfügen. Durch Vortäuschen eines Verlustes von G kann B_G seinen Besitz jedoch nicht vermehren.*

Offensichtlich muß zum Zwecke der Verlusttoleranz trotz des Verlustes eines sicheren Gerätes G rückgesetzt, d.h. ein früherer (tatsächlicher oder möglicher) Zustand wiederhergestellt werden können [AnLe_81]. Damit sind zwei Fragen für die Verlusttoleranz zu entscheiden:

1. Wie wird das rücksetzbare Objekt und dessen Zustand definiert?
2. Wo und wann wird die Rücksetzinformation gespeichert? Wird durch das Rücksetzen eines Gerätes dessen Zustand exakt rekonstruiert oder tritt eine Rücksetzabweichung auf?

Die prinzipiell möglichen Antworten auf diese Fragen werden im folgenden diskutiert. Dabei müssen die Forderungen aus Kapitel 2 weiterhin erfüllt werden.

Insbesondere darf, um die Betrugssicherheit zu wahren, die Rücksetzinformation nicht fälschbar sein. Dies gilt einerseits für den Besitzer, der durch Fälschen der Rücksetzinformation sein Gerät auf beliebige Kontostände setzen lassen könnte. Es gilt aber auch für die Bank, falls sie das Rücksetzen übernimmt. Zumindest sollte sie durch Fälschen Benutzern nicht mehr Schaden zufügen können, als diese im verlusttoleranzlosen System erlitten hätten.

3.1 Rücksetzbares Objekt

Geht G verloren, so ist B_G im wesentlichen daran interessiert, wieder über K_G zu verfügen, d.h. K_G wird den Hauptbestandteil des Zustandes ausmachen, auf den zurückgesetzt wird. Da das Gerät G als verloren betrachtet wird, muß dieser Zustand auf einem anderen Gerät G' von B_G installiert werden.

Im Gegensatz zu normalen Systemen, bei denen nach dem Rücksetzen der evtl. fehlerhafte Zustand keine Wirkung auf das weitere Systemverhalten mehr hat, ist dies hier, falls B_G nicht ganz ehrlich ist, nicht unbedingt garantiert: das sichere Gerät G könnte weiterhin intakt existieren und ermöglichen, den alten Zustand, also K_G, nach dem Rücksetzen auf G' zu verändern.

Um diesen Umstand zu berücksichtigen, darf als rücksetzbares Objekt nicht einfach das Gerät G, sondern muß die Folge (G, G',G'',...) von Gerät G, Ersatzgerät G' von G, Ersatzgerät G'' von G', usw. betrachtet werden. Die Transaktionen dieser Geräte könnten als von einem einzigen Gerät vorgenommen betrachtet, der Zustand der Geräte müßte zu einem einzigen zusammengefaßt werden. Da es aber sinnvoll erscheint, alle Geräte gleich zu behandeln, d.h. den Anfangszustand von $G^{a'}(a\in(')^*)$ nur von G^a abhängig zu machen, genügt es, statt der Folge ein Paar (G,G') zu betrachten.

Das aus solchen „Geräten" (G,G') bestehende Zahlungssystem muß weiterhin alle Anforderungen aus Kapitel 2 erfüllen, wobei statt K_G nun zu betrachten ist, über wieviel Geld B_G unter Verwendung beider Geräte verfügen kann. Dieser Wert werde mit $K_{(G,G')}$ bezeichnet. Zu den in Kapitel 2 angegebenen drei Teilprotokollen kommt dann noch ein weiteres hinzu:

Rücksetzen von G auf G'

Vor dem Rücksetzen von (G,G') ist stets $K_{(G,G')} = K_G$, d.h. B_G kann das sichere Gerät G' nicht verwenden.

[1] Geht G verloren, so meldet B_G dies der Rücksetzinstanz (i. allg. der Bank) und versorgt sie ggf. mit Rücksetzinformationen.

[2] Die Rücksetzinstanz setzt $K_{G'}$ auf einen Wert nahe K_G.

Protokollskizze 2 Grundschema für das Rücksetzen eines Gerätes G auf G'

Um zu verhindern, daß $K_{(G,G')}$ in Schritt [2] durch das Initialisieren von $K_{G'}$ zunimmt, muß vor dem Festsetzen von $K_{G'}$ das Verhalten von K_G nach dem Rücksetzen berücksichtigt werden. Die Möglichkeiten hierzu werden im folgenden Abschnitt diskutiert.

3.2 Abschätzung der Rücksetzabweichung

Da das sichere Gerät G auch nach dem Rücksetzen noch funktionsfähig sein kann, muß der Gesamtumfang der Transaktionen nach dem Rücksetzen hinreichend gut abschätzbar sein. Als Lösungen kommen zwei Verfahren in Betracht.

3.2.1 Rücksetzen ohne Wartefristen

Soll nach dem Verlust von G unverzüglich auf G' rückgesetzt werden können, so muß offensichtlich das Paar (G,G') ab dem Zeitpunkt des Rücksetzens wie aus zwei voneinander unabhängigen Geräten bestehend betrachtet werden, und es ist $K_{(G,G')} = (K_G + K_{G'})$.

Somit ist es zwingend, daß B_G vor dem Aktivieren von G' mit einem Anfangskontostand $K_{G'}$ freiwillig auf die Verfügungsgewalt über diesen Betrag $K_{G'}$ auf G verzichtet hat. Da dies jeweils gleichzeitig sowohl G bekannt werden muß (das die Einhaltung überwacht) als auch einer Instanz außerhalb von G (zum Rücksetzen), muß hierzu die Autonomie von G eingeschränkt werden. Solange G nicht verloren ist, kann B_G diese Rücksetzinformation beliebig oft ändern lassen und somit den möglichen Verlust selbst begrenzen.

Um diese Einschränkungen der Verfügungsgewalt und Autonomie für B_G so gering wie möglich zu halten, bietet sich zur „Zwischenlagerung" von $K_{G'}$ ein zweites sicheres Gerät G* von B_G an, an das $K_{G'}$ mit dem normalen Zahlungsprotokoll überwiesen wird. G* sollte aber zuverlässiger als G sein und B_G sollte es, um es nicht zu verlieren, nicht herumtragen können (d.h. es spielt die Rolle eines Safes zu Hause). Möchte B_G wieder über $K_{G'}$ verfügen, so kann er $K_{G'}$ an G zurücküberweisen. Geht G verloren, so besorgt er sich ein neues Gerät G' und überweist $K_{G'}$ von G* an G'.

Statt eines zweiten sicheren Gerätes G* kann zum „Zwischenlagern" von $K_{G'}$ auch die Bank verwendet werden, indem $K_{G'}$ auf ein Konto von B_G in einem anderen Zahlungssystem transferiert wird, oder indem B_G bei der Bank $K_{G'}$ in Form eines passiven Rücksetzpunktes in Verwahrung gibt [WaPf_87].

3.2.2 Änderungsaufzeichnung

Will man bei der Initialisierung von G' sämtliche jemals von G gemachten Transaktionen berücksichtigen, so erzwingt dies zum einen, eine vollständige Änderungsaufzeichnung (audit trail) aller sicheren Geräte vorzunehmen, und zum anderen, mit dem Rücksetzen, also Aktivieren von G', solange zu warten, bis G keine Transaktionen mehr vornehmen kann.

Da B_G mehrere sichere Geräte besitzen kann und zudem auch andere Zahlungssysteme neben dem hier besprochenen existieren können, ist eine Wartezeit bis zum Rücksetzen zumindest bei kleinen Beträgen i. allg. keine ernsthafte Beschränkung der Anwendbarkeit.

Die Forderung nach einer endlichen Wartezeit macht das bereits in Kapitel 2 beschriebene Ungültigwerden von G erforderlich, G' kann dann einfach als Nachfolger von G im Besitz von B_G betrachtet werden (Bild 1).

Statt die Lebenszeit eines Gerätes a priori zu begrenzen, könnte man auch versuchen, nur die Geräte ungültig werden zu lassen, die als verloren gemeldet sind, indem alle Geräte eine Liste aller verlorenen Geräte führen. Das Gerät G wäre ab dem Zeitpunkt ungültig, zu dem alle Geräte hiervon erfahren haben müßten. Um zu erwingen, daß

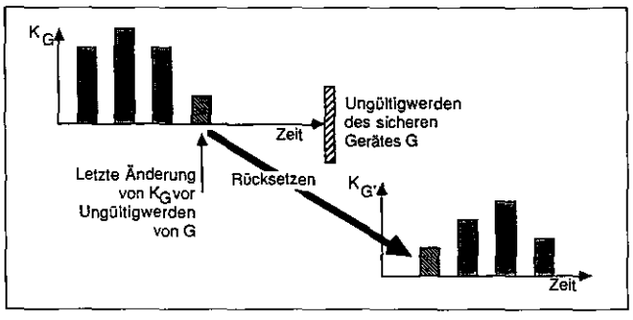

Bild 1 Eliminierung der Rücksetzabweichung durch Änderungsaufzeichnung

jedes nicht verlorene Gerät innerhalb einer bestimmten Frist von dem Ungültigwerden von G erfährt, müßte man allerdings wieder alle Geräte, die innerhalb dieser Frist die Liste nicht erhalten haben, ungültig werden lassen, so daß nichts gewonnen wäre.

Die Forderung nach Wahrung der Autonomie verbietet, die Änderungsaufzeichnung durch dritte, an der Transaktion nicht beteiligte Instanzen, etwa die Bank, vornehmen zu lassen.

Damit kommen als Aufzeichnende für eine Transaktion nur die direkt Beteiligten sowie deren spätere Kommunikationspartner in Frage.

Die Untersuchung der Möglichkeiten für eine verteilte Änderungsaufzeichnung stellen den Schwerpunkt dieser Arbeit dar. Sie sollen daher in einem eigenen Kapitel behandelt werden.

4 Verteilte Änderungsaufzeichnung

Im folgenden soll die in Kapitel 3.2.2 zuletzt diskutierte Möglichkeit zur Verlusttoleranz ohne Rücksetzabweichung genauer untersucht werden.

Hierzu wird zunächst in 4.1 nur die Sicherheit der Verfahren angestrebt, die Anonymität wird nachträglich in 4.2 hinzugefügt.

4.1 Betrugssichere verteilte Aufzeichnung

Im folgenden bezeichnet T(t, G1, G2, b) eine Zahlung zum Zeitpunkt t von G1 an G2 mit dem Betrag b. Um die Transaktion dokumentieren zu können, müssen sie beide Geräte jeweils so kennzeichnen, daß der Transaktionsaufzeichnung die Transaktion und das kennzeichnende Gerät (also G1 bzw. G2) eindeutig zu entnehmen sind.

Dazu benötigen die Geräte nun eine Identität, d.h. eine Nummer, die im nicht anonymen Fall von der Bank gewählt wird, um Eindeutigkeit zu gewährleisten, und direkt in der Aufzeichnung angegeben wird. Eine Transaktion ist dann eindeutig bestimmt durch die Identität G eines der beteiligten Geräte und ein von diesem eindeutig gewähltes Transaktionskennzeichen T_G.

4.1.1 Unsicherheit der einfachen Änderungsaufzeichnung

Die einfachste Form der verteilten Änderungsaufzeichnung (audit trail, [AnLe_81, Wein_84]) ist unter Abänderung der Protokollskizzen 1 und 2 in Protokollskizze 3 angegeben.

Zahlung von G1 an G2

[1–3] Wie in Protokollskizze 1
[4] Eigentlicher Transfer
  [4.1] G1 (bzw. G2) wählt sich ein Transaktionskennzeichen T_{G1} (bzw. T_{G2}), das die laufende Transaktion eindeutig kennzeichnet.
  [4.2] Wie [4] in Protokollskizze 1, aber G1 und G2 tauschen zusätzlich ihre Kennzeichen T_{G1} und T_{G2} aus.
  [4.3] G1 (bzw. G2) speichert den Änderungsvermerk (G2,b,T_{G2}) (bzw. (G1,-b,T_{G1})) in einer Liste ab.

Rücksetzen von G nach Verlustmeldung

[1] Zu einem bestimmten, von der Bank bestimmbaren Zeitpunkt wird G ungültig.
[2] Die Bank wartet, bis alle sicheren Geräte, mit denen G hätte Transaktionen vornehmen können, ebenfalls ungültig sind und erhält deren Änderungsaufzeichnungen.
[3] Die von allen sicheren Geräten erhaltene Änderungsaufzeichnung wird nach Einträgen (G,b,T) untersucht. Die gefundenen Änderungen werden ausgehend von der Initialisierung von K_G nachvollzogen und so K_G rekonstruiert.

Protokollskizze 3 Grundschema für die verteilte Änderungsaufzeichnung

Das obige Protokoll würde eine Transaktion genau dann aufzeichnen, wenn wenigstens eines der daran beteiligten Geräte nicht verloren ist. Bei nicht ganz ehrlichen Teilnehmern ist der Verlust von an einer Transaktion beteiligten Geräten allerdings nicht unabhängig: Erfährt der Zahlende, daß der Empfänger sein Gerät verloren hat, könnte dies eine günstige Gelegenheit sein, auch das eigene fortzuwerfen und so die Zahlung rückgängig zu machen.

Das Zahlungssystem hat allerdings auch einen wirklich gravierenden Sicherheitsmangel. Man betrachte vier Geräte G1, G2, G3, G4 und nehme folgenden Ablauf an (Bild 2).

- Die Geräte sind initialisiert mit
  $K_{G1} := b$ $(b>0)$, $K_G := 0$ für $G = G2, G3, G4$;
- Die Geräte vollziehen die Transaktionen
  T(1,G1,G2,b), T(2,G2,G3,b), T(3,G3,G4,b)
- Die Geräte G2 und G3 gehen verloren.

Nach obigem Protokoll werden dann G2 und G3 zurückgesetzt auf

- $K_{G2'} := b$,
  denn T(1,G1,G2,b) wird von G1 aufgezeichnet,
- $K_{G3'} := -b$,
  denn T(3,G3,G4,b) wird von G4 aufgezeichnet, aber T(2,G2,G3,b) ist verloren.

Damit sind die Nachteile dieses einfachen Ansatzes bereits offensichtlich: durch Rücksetzen wird $K_{G3'}$ auf einen negativen Wert gesetzt, d.h. es entsteht einerseits eine Rücksetzabweichung, was eigentlich verhindert werden sollte, und andererseits können sogar negative Kontostände auftreten.

Das Problem, diese auszugleichen, ist nicht sinnvoll zu lösen:

B_{G3} könnte mit Recht auf die Eigenschaft der Betrugssicherheit des Zahlungssystems hinweisen, die garantiert, daß K_{G3} niemals negativ werden kann. Vernünftigerweise kann man daher von B_{G3} nicht erwarten, daß er für die Schwäche des Aufzeichnungsverfahrens gerade steht. Garantiert das Zahlungssystem seinen Teilnehmern ein sehr hohes Maß an Anonymität, so könnte man B_{G3} hierzu

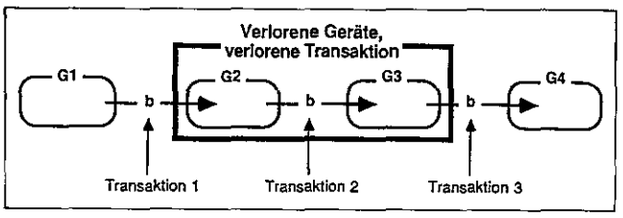

Bild 2 Verlust zweier aufeinanderfolgender Geräte

auch nur schwer zwingen. Tut man dies aber doch, so muß ein Teilnehmer im schlimmsten Fall alle Zahlungen, die sein sicheres Gerät jemals erhalten hat, beim Rücksetzen zurückgeben. Dies wäre sogar dann der Fall, wenn er gelegentlich Rücksetzpunkte analog zu 3.2.1 in Form von Überweisungen seines Gerätes an ein anderes seiner Geräte (oder Konten) erstellt hätte.

Setzt man aber, statt B_{G3} zu belasten, einfach $K_{G3}' := 0$, so führt die oben beschriebene Situation zu einer einfachen Betrugsmöglichkeit, indem die Beteiligten die Situation künstlich herbeiführen.

4.1.2 Sicherheit durch Weiterverteilung

Die Ursache für diese Rücksetzabweichung liegt darin, daß der Betrag von einem verlorenen Gerät zu einem anderen weitergegeben wurde, ohne daß dies der der Bank zugänglichen Änderungsaufzeichnung zu entnehmen ist.

Um solche Weiterleitungen entdecken zu können, muß man entweder die Aufzeichnungen über Transaktionen zwischen verlorenen Geräten retten oder zumindest den Zusammenhang zwischen Zahlungen an und Zahlungen von verlorenen Geräten herstellen können.

Soll keine Transaktion in der der Bank vorliegenden Änderungsaufzeichnung fehlen, so muß zwangsläufig jedes sichere Gerät die vollständige Änderungsaufzeichnung enthalten.

Diese Forderung ist jedoch nicht erfüllbar: zerfällt die Menge aller sicheren Geräte in zwei disjunkte Teilmengen M_1 und M_2, so daß keine Transaktionen zwischen Geräten aus M_1 und M_2 stattfinden, so kann aufgrund der Autonomie in einem Gerät aus M_1 keine Information über die Transaktionen der Geräte in M_2 gespeichert werden. Gehen alle Geräte in M_2 verloren, so können deren Transaktionen nicht nachvollzogen werden.

Die bestmögliche Annäherung an diese Forderung erhält man, indem die Geräte die Aufzeichnungen über Transaktionen durch Fluten (flooding, [Tane_81]) möglichst vollständig verteilen. Dieses Verfahren realisiert damit die maximale erreichbare Verlusttoleranz und garantiert, daß die Geldmenge im System konstant bleibt und keine negativen Kontostände auftreten. Leider ist jedoch der Speicheraufwand so groß, daß eine Realisierung bei der zu erwartenden Größe offener Systeme wenig realistisch erscheint, weshalb wir für eine genaue Diskussion dieses Verfahrens auf [WaPf_87] verweisen.

Will man den Speicherbedarf verringern, muß man die Verteilung der Aufzeichnungen über Transaktionen und damit auch die Menge der ohne Rücksetzabweichung tolerierbaren Verluste einschränken, was jedoch akzeptabel ist, solange unter allen Umständen die Geldmenge im System nicht zunimmt und keine negativen Kontostände auftreten. Diese Forderungen können durch Systeme erfüllt werden, bei denen von jeder Transaktion beide Änderungsvermerke immer gleichzeitig weitergegeben werden und mit einer Aufzeichnung, die ein Gerät belastet, immer auch genügend Aufzeichnungen, die die Einnahmen nachweisen, die diese Ausgabe ermöglichten, bei denen also zu jeder Transaktion überall auch ihre gesamte Vorgeschichte aufgezeichnet ist.

Da bei solchen Systemen jede für einen Benutzer wichtige Rücksetzinformation von dessen Gerät erzeugt wurde und damit von diesem authentiziert werden kann, sind die Benutzer auch gegen Änderungen der Rücksetzinformationen durch die Bank geschützt. Gegen Nichtbeachten wichtiger Informationen durch die Bank kann sich ein Benutzer durch gelegentliches Abspeichern seiner bisherigen Transaktionen weitgehend schützen [WaPf_87].

4.1.3 Markierte Standardwerttransaktionen

Eine Idee, wie man diese Weitergabe immer länger werdender Vorgeschichten vermeiden und dennoch die zu negativen Kontoständen führende Rücksetzabweichung beseitigen kann, kann man bei Betrachtung von Bild 2 wie folgt gewinnen: Es müßte erkennbar werden, daß G3 das Geld, das es ausgegeben hat, irgendwann eingenommen haben muß, und dementsprechend dürfte es keinem früheren Besitzer, in diesem Fall G2, zugeschrieben werden. Dazu muß aber der Begriff „dasselbe Geld" im Zahlungssystem ausdrückbar sein.

Um dies zu realisieren, führt man in das System „Banknoten" ein, beschränkt also die möglichen Transaktionen auf die Weitergabe markierter Standardwerte, wobei Banknoten verschiedener Nennwerte möglich sind. Das Rücksetzen eines Gerätes G bedeutet dann, daß die Bank feststellt, welche Banknoten G zum Verlustzeitpunkt besaß. Eine solche Banknote ist dadurch charakterisiert, daß sie mit dem Gerät G verloren ist und G das letzte Gerät war, an das sie weitergegeben wurde.

Um dies nachprüfen zu können, müssen auch Banknoten nach einer gewissen Zeit ungültig werden. Dies kann realisiert werden, indem das gesamte System gleichzeitig ungültig wird; es genügt aber, wenn die Banknoten ein Verfallsdatum tragen und spätestens beim Ungültigwerden des Gerätes an die Bank transferiert werden müssen.

Zudem müssen alle nicht verlorenen Geräte der Bank zum Rücksetzen mitteilen, ob und ggf. wann und an wen sie eine Banknote weitergegeben haben. Zu diesem Zwecke führt jedes Gerät G1 eine Weitergabeliste WL_{G1}, die zu jeder von G1 weitergegebenen Banknote einen Eintrag (G2,N,z) enthält, wobei G2 den Empfänger der Banknote, N die Banknote (und damit auch ihren Wert) und z den Zeitpunkt der Weitergabe kennzeichnet. Da nur interessiert, welche Weitergabe die letzte war, soll z nicht Datum und Uhrzeit angeben, sondern nur die Anzahl der früher schon stattgefundenen Weitergaben von N „zählen". Auf ein eigenes Transaktionskennzeichen T_{G2} kann verzichtet werden, da durch (N, z) die Transaktion bereits eindeutig bezeichnet ist.

Um diese Daten bei einer Transaktion weitergeben zu können, muß das Gerät G auch eine Besitzliste BL_G führen, die alle Banknoten, die es gerade besitzt, als Paare (N, z) enthält (ein expliziter Zähler K_G trägt nur zur Effizienz bei und wird daher im folgenden nicht mehr erwähnt).

Der Speicherbedarf eines sicheren Gerätes ist wie im einfachen, aber unsicheren Verfahren der einfachen Änderungsaufzeichnung (vgl. 4.1.1) im wesentlichen dadurch bestimmt, daß je Transaktion ein Vermerk gespeichert werden muß. Im Gegensatz zur einfachen Aufzeichnung entsprechen allerdings einer Zahlung hier mehrere Transaktionen, so daß sich die Zahl der zu speichernden Vermerke um einen kleinen Faktor erhöht. (Wählt man z.B. 20 Standardwerte der Größen 1, 2, ..., 2^{19}, so ist dieser Faktor ungefähr 10.)

Zum Rücksetzen muß die Bank zunächst anhand der ihr übergebenen BL_G-Listen entscheiden, welche Banknoten verloren gegangen sind, was am effizientesten durch „Abhaken" einer Bitleiste geschieht, wo jeder Banknote im System ein Bit zugeordnet ist. Damit bestimmt die Anzahl der Banknoten im System zugleich den Bedarf der Rücksetzprozedur an schnell zugreifbarem Speicher. Der Zeitaufwand für diesen Schritt ist proportional zur Anzahl aller Banknoten.

Sodann wird anhand der der Bank übergebenen Änderungsvermerke zu jeder verlorenen Banknote deren letzter Besitzer festgestellt. Dies erfordert, daß die Änderungsauf-

zeichnungen aller Geräte abgespeichert werden (wozu allerdings keine schnellen Speicher benötigt werden, so daß der für die Banknotenbitleiste vorgesehene Platz ausreichen wird). Der Zeitaufwand dieses Schrittes ist proportional zur Anzahl der Änderungsvermerke mal dem Logarithmus der Anzahl der verlorenen Banknoten.

Weigert sich ein Besitzer eines verlorenen Gerätes G, sein Gerät rücksetzen zu lassen, so hat er davon ersichtlich nur Nachteile. Ist umgekehrt G aber nicht verloren, so könnte sich B_G einen Vorteil davon versprechen, sein Gerät nach dessen Ungültigwerden absichtlich zu verlieren: B_G verliert nichts, denn G enthält keine Banknoten mehr (diese müssen vor Ungültigwerden von G bei der Bank eingereicht werden), G könnte aber durch Rücksetzen zufällig noch früher besessene Banknoten gutgeschrieben bekommen. Um diese die Verlusttoleranz störende Versuchung zu beseitigen, sollte das Gerät G selbst für B_G einen gewissen Wert darstellen und für B_G unbrauchbar werden, falls es nach Ungültigwerden nicht in begrenzter Zeit die Liste WL_G an die Bank sendet und dafür eine Quittung erhält.

Initialisierung des sicheren Gerätes durch die Bank und B_G

[1] Wie in Protokollskizze 1.

[2] Für die Erstbestückung von G mit Banknoten wird das normale Zahlungsprotokoll (s.u.) verwendet, wobei als Zahlender die Bank auftritt, von der angenommen wird, daß sie nicht verloren geht, und als Empfänger G.

Zahlung von G1 an G2

[1–3] Wie in Protokollskizze 1.

[4] Eigentlicher Transfer

[4.1] G1 sendet an G2 ein Paar (N,z) (aus BL_{G1}). Erhält G2 das Paar (N,z), so quittiert G2 und sendet (G2,N,z) an G1. Für die Gültigkeit der Zahlung gilt das für Protokollskizze 1 Gesagte entsprechend.

[4.2] G1 fügt (G2,N,z) in seine Liste WL_{G1}, G2 fügt (N,z+1) in seine Liste BL_{G2} ein.

Ungültigwerden und Rücksetzen von G1

[1] Die Bank sammelt ständig von allen nicht verlorenen, ungültig gewordenen sicheren Geräten G deren Listen WL_G ein. Wurde G noch nicht rückgesetzt, so kann G neu initialisiert werden.

[2] Um ein verlorenes sicheres Gerät G1 rücksetzen zu können, wartet die Bank dessen Ungültigwerden ab, dann die Zeit, bis alle Banknoten, die G1 haben könnte, ebenfalls ungültig sind, und zum Schluß, bis auch alle anderen Geräte G2, die diese Banknoten haben könnten, ungültig sind.

Geräte, die bereits ihre Liste WL_G der Bank übergeben haben, werden nicht zurückgesetzt.

[3] Nun werden G1 alle ungültig gewordenen Banknoten N zugeschrieben, für die gilt:

- N ist verloren, d.h. kein Gerät G2 hat N eingelöst, und
- (G1,N,z) taucht in einer Liste WL_{G2} auf und für alle weiteren Einträge (G3,N,z′) in Listen WL_{G4} gilt $z' < z$.

Protokollskizze 4 Verteilte Aufzeichnung: Standardwerttransaktionen

Das Verfahren garantiert:

a) Eine Banknote, die ein verlorenes Gerät G erhalten und nicht weitergegeben hat, erhält G genau dann gutgeschrieben, wenn das sichere Gerät, von dem G die Banknote erhalten hat, nicht ebenfalls verloren gegangen ist.

b) Durch Rücksetzen wird kein Kontostand auf einen negativen Wert gesetzt.
Dies ist bereits durch die Definition des Verfahrens (Protokollskizze 4) garantiert, da Geräten nur Banknoten gutgeschrieben, jedoch nicht weggenommen werden.

c) Durch Rücksetzen ändert sich die Geldmenge im Zahlungssystem nicht.
Genauer: Jede Banknote N wird nach ihrem Ungültigwerden entweder durch ein nicht verlorenes Gerät eingelöst oder wird genau einem Gerät beim Rücksetzen zugesprochen.

Das Verfahren garantiert keine feste obere Schranke für die Rücksetzabweichung, so daß diese Forderung der Verlusttoleranz nicht erfüllt ist. Da aber die Rücksetzabweichung den Besitz zum Verlustzeitpunkt nicht übersteigt, ist nun, im Gegensatz zu 4.1.1, das gelegentliche Erstellen von Rücksetzpunkten durch Überweisen eines Betrages im Sinne von 3.2.1 sinnvoll. Es genügt sogar, alle Banknoten von G an G* und zurück zu überweisen (vgl. a).

Die Verlusttoleranz des Verfahrens kann verbessert werden, indem neben der Übergabe der Informationen über die laufende Transaktion stets auch Information über alte Transaktionen weitergegeben wird, wobei die Ausbreitung dieser Informationen im Gegensatz zu der in 4.1.2 begrenzt werden kann (z.B. auf zehnmalige Weitergabe, wonach man für die weitergegebene Transaktion jeden Verlust von 10 Geräten tolerieren kann), ohne die Sicherheit zu gefährden.

Das Verfahren der markierten Standardwerte und seine Erweiterung garantiert die Betrugssicherheit wie in Kapitel 2 definiert, d.h. kein Benutzer verliert mehr als im verlusttoleranzlosen System, und die Geldmenge nimmt nicht zu.

Nicht garantiert ist jedoch, daß die Bank einem verlorenen Gerät G auch wirklich jede Banknote gutschreibt, die sie ihm nach Protokoll gutschreiben müßte, denn sie könnte behaupten, die Banknote sei von einem nicht verlorenen Gerät als ihm gehörend gemeldet worden, oder sie könnte für diese Banknote einen fiktiven Eintrag erzeugen, der „nachweist", daß die Banknote nach G noch an ein anderes Gerät (eines der Bank) transferiert wurde.

Mißtraut man der Bank und möchte diesen Zustand daher umgehen, muß zwangsläufig jede für G wichtige Rücksetzinformation anderer Geräte eine Authentikation von G enthalten. Hierzu muß das Verfahren, die verlorenen Banknoten festzustellen, geändert werden, und es muß bei jedem Transfer einer Banknote deren gesamte Vorgeschichte, d.h. alle ihre früheren Besitzer, mit übergeben werden. Für die genaue Realisierung sei auf [WaPf_87] verwiesen.

4.2 Anonymisierung der markierten Standardwerttransaktionen

In 4.1 wurde die verteilte Änderungsaufzeichnung lediglich unter dem Gesichtspunkt der Sicherheit betrachtet, die Anonymität blieb noch unberücksichtigt. Dies soll, im wesentlichen für das Verfahren der markierten Standardwerte (4.1.3), nun nachgeholt werden.

Wie schon für die Anonymität des verlusttoleranzlosen Systems (Kap. 2), so ist auch hier zu unterscheiden, ob die Informationen über Zahlungen außerhalb sicherer Geräte wahrgenommen werden können.

Geht man davon aus, daß ein sicheres Gerät nur mit von ihm geprüften echten Geräten kommuniziert und das gesamte Rücksetzprotokoll der Bank (Einsammeln der Weitergabelisten, Rücksetzen verlorener Geräte) ebenfalls von einem sicheren Bankgerät ausgeführt wird, das die Rücksetzinformationen auch vor der Bank geheimhält, so ist das in 4.1.3 beschriebene Verfahren bereits anonym.

Diese Betrachtungsweise setzt allerdings voraus, daß die Bankgeräte ebenso sicher gebaut werden können wie die „elektronischen Brieftaschen". Im Vergleich zu diesen müssen aber Bankgeräte um vieles leistungsfähiger und zuverlässiger sein und zudem viel komplexere Aufgaben übernehmen.

Somit werden einerseits die Entwürfe der Bankgeräte nur sehr schwer auf Trojanische Pferde zu untersuchen sein, andererseits werden die Geräte durch die gleichzeitige Forderung nach Ausforschungssicherheit und Zuverlässigkeit sicher um vieles teurer als normale Rechner.

Aus diesen Gründen soll im folgenden angenommen werden, daß die Bank direkt mit sicheren Geräten kommunizieren kann und auch das Rücksetzprotokoll ohne Hilfe sicherer Bankgeräte durchführt.

Das Verfahren der markierten Standardwerte basiert darauf, daß die Bank für verlorene Geräte G alle Einträge der Art (G, N, z) der WL-Listen erhält.

Erhielte sie diese Einträge aber wie in 4.1.3 für alle Geräte, so könnte sie das Geschehen im Zahlungssystem sehr genau nachvollziehen: zu jeder Banknote N könnte sie sämtliche Besitzer in der richtigen Reihenfolge feststellen, also insbesondere sehen, wer an wen Geld bezahlte und ungefähr wann.

Um der Bank dies zu verwehren, übergibt der Zahlungsempfänger G2 dem Zahlenden G1 die Daten (G2,N,z) nicht im Klartext, sondern verschlüsselt mit einem nur G2 und B_{G2} bekannten Schlüssel s_{G2} eines symmetrischen Kryptosystems [Denn_82, Hors_85, LuRa_86]. Ohne Kenntnis von s_{G2} kann damit die Bank die G2 betreffenden Einträge in WL-Listen nicht lesen; ist G2 nicht verloren, so gewinnt die Bank aus den WL-Listen folglich keine Information über G2.

Um ein Gerät G im Verlustfall rückzusetzen, erhält die Bank s_G von B_G und testet jeden Eintrag jeder WL-Liste daraufhin, ob er mit s_G verschlüsselt war.

Da die Transaktion selbst durch (N,z) bereits eindeutig gekennzeichnet ist, und die Tatsache, daß sie mit s_G verschlüsselt ist, bereits G eindeutig kennzeichnet, kann auf die explizite Angabe von G verzichtet werden. Um dann allerdings überhaupt noch erkennen zu können, ob mit s_G verschlüsselt wurde, muß entweder N Redundanz enthalten oder das Paar (N,z) vor der Verschlüsselung von G um einen hinreichend redundanten Teil r erweitert worden sein, d.h. statt s_G (G,N,z) kann s_G(r,N,z) mit einem in der Länge oder für andere Zwecke (s.u.) besser als G passenden Teil r verwendet werden.

Der einfachere Ansatz, die Einträge im Klartext abzuspeichern, aber durch die Geräte (anhand von Unterschriften der Besitzer verlorener Geräte) lokal auswählen zu lassen, welche Einträge für die Bank wichtig sind und dieser übermittelt werden müssen, ist unpraktikabel: einerseits kann die Bank selbst als Partner auftreten, so daß sie zumindest für ihre Geräte doch die volle Information bekommt; andererseits können zum Rücksetzen eines verlorenen Gerätes G auch Einträge wichtig sein, die Geräte sammelten, die vor dem Verlust von G ungültig wurden und die ihre Rücksetzdaten der Bank schon längst übermittelt haben.

Soweit ist also garantiert, daß die Bank den Einträgen der WL-Listen keine Informationen entnehmen kann, die sie nicht zum Rücksetzen benötigt. Doch sind diese Einträge nicht die einzigen Ansatzpunkte für die Bank, Informationen zu erhalten:

Zum einen könnte die Bank, wenn mit ihrer Hilfe von oder an G Banknoten aus einem anderen Zahlungssystem transferiert werden (z.B. zur Erstbestückung mit Banknoten, Einreichen ungültig gewordener Banknoten) oder sie als normaler Partner in einer Transaktion auftritt, mehr Information erhalten als im verlusttoleranzlosen System, da die Geräte nun Identitäten haben. Bei Transaktionen mit Geräten, die später rückgesetzt werden, ist dies aber gerade das Prinzip des Verfahrens und ansonsten ist es durch die Verschlüsselung der Transaktionsdaten verhindert. Um aber wenigstens zu vermeiden, daß die Bank bei einem rückgesetzten Gerät G den Zusammenhang zwischen der Identität des Gerätes und der seines Besitzers herstellen kann, sollte es nicht von einem nicht anonymen Konto von B_G „erstbestückt" worden sein.

Zum anderen sollte jedes sichere Gerät G nach seinem Ungültigwerden WL_G der Bank übersenden. Da G an jeder Transaktion, die in WL_G verzeichnet ist, als Zahlender beteiligt war, könnte die Bank durch eine Identifikation des Absenders von WL_G für diesen zumindest alle Zahlungen an verlorene Geräte nachvollziehen.

Um dies zu verhindern, muß die Übergabe von WL_G anonym erfolgen, d.h. die Bank kann zu einer erhaltenen Änderungsaufzeichnung nur feststellen, daß sie von einem sicheren Gerät stammte, nicht aber, von welchem.

Hierzu ist zu garantieren, daß stets eine gewisse Menge sicherer Geräte gleichzeitig ungültig ist, so daß die Bank aus dem Zeitpunkt der Übermittlung der Änderungsaufzeichnung nicht auf das übermittelnde Gerät schließen kann. Alle diese sicheren Geräte übersenden mittels eines Datenschutz garantierenden Kommunikationssystems der Bank anonym ihre Änderungsaufzeichnungen (evtl. sogar jeden Eintrag einzeln) und erhalten dafür von der Bank eine Quittung. Das Nichteintreffen der Quittung kann durch Wiederholen der Übersendung und im Notfall durch Klage gegen die Bank behandelt werden.

In einer zweiten Runde übersenden alle sicheren Geräte, die eine Quittung der Bank erhalten haben, der Bank nicht anonym, d.h. unter Verwendung der ihnen von ihrem jeweiligen Besitzer bei der Initialisierung zur Authentikation von Rücksetzinformationen gegebenen Signaturfunktion, eine entsprechende Nachricht, so daß die Bank entscheiden kann, welche sicheren Geräte ihre Änderungsinformation übersandt haben und welche zurückgesetzt werden müssen (oder wollen).

Das Datenschutz garantierende Kommunikationssystem ist einerseits sowieso sinnvoll und eine Voraussetzung für jedes anonyme digitale Zahlungssystem ohne sichere Geräte, kann aber andererseits auch speziell zu diesem Zweck kurzzeitig virtuell aufgebaut werden.

Initialisierung des sicheren Gerätes durch die Bank und B_G

[1] B_G wählt sich einen Wert s_G (als Schlüssel eines vorgegebenen symmetrischen Kryptosystems) und teilt s_G vertraulich G mit.

[2] Die Bank initialisiert G (Schlüssel S, Anfangsguthaben, ...).

[3] G bestätigt seinem Besitzer B_G die erhaltenen Werte, so daß B_G deren Korrektheit falls notwendig nachweisen kann.

[4] Für die Erstbestückung von G mit Banknoten wird das normale Zahlungsprotokoll (s.u.) verwendet, wobei als Zahlender G1 die Bank auftritt, von der angenommen wird, daß sie nicht verloren geht, und als Empfänger G.

Zahlung von G1 an G2

[1–3] Wie in Protokollskizze 1

[4] Eigentlicher Transfer

[4.1] G1 sendet an G2 ein Paar (N, z) (aus BL_{G1}). Erhält G2 das Paar (N, z), so quittiert G2, erweitert das Paar (N, z) um redundante Information r und sendet $s_{G2}(r, N, z)$ an G1.

Für die Gültigkeit der Zahlung gilt das für Protokollskizze 1 Gesagte entsprechend.

[4.2] G1 fügt $s_{G2}(r, N, z)$ in seine Liste WL_{G1}, G2 fügt (N, z+1) in seine Liste BL_{G2} ein.

Ungültigwerden und Rücksetzen von G1

[1] Die Bank sammelt ständig von allen nicht verlorenen, ungültig gewordenen sicheren Geräten G deren Listen WL_G ein:

[1.1] Alle ungültig gewordenen, nicht verlorenen sicheren Geräte G übersenden (mittels eines Datenschutz garantierenden Kommunikationssystems) anonym der Bank ihre Listen WL_G und erhalten hierfür eine Quittung.

[1.2] Alle sicheren Geräte, die in [1.1] eine Quittung erhalten haben, melden sich nach Ablauf einer zufälligen Zeitverzögerung bei der Bank als nicht verloren.
Das Gerät G gibt dabei als Identität das Bild $f(s_G)$ von s_G unter einer Einwegfunktion f an. Sodann wird G neu initialisiert, es sei denn, die Bank stellt durch Vergleich mit den in Schritt [2] früher erhaltenen Schlüsseln rückgesetzter Geräte fest, daß G bereits auf Wunsch von B_G rückgesetzt wurde.
Alle anderen Geräte werden unbrauchbar.

[2] Um ein verlorenes sicheres Gerät G1 rücksetzen zu können, übergibt B_{G1} spätestens zum Zeitpunkt des Ungültigwerdens von G1 der Bank den Schlüssel s_{G1}. Diese bildet $f(s_{G1})$ und kontrolliert, daß dieses Gerät bisher nicht neu initialisiert wurde.

[3] Sodann wartet die Bank das Ungültigwerden von G1 ab, dann die Zeit, bis alle Banknoten, die G1 haben könnte, ebenfalls ungültig sind, und zum Schluß, bis auch alle anderen Geräte G2, die diese Banknoten haben könnten, ungültig sind.

[4] Nun werden G1 alle ungültig gewordenen Banknoten N zugeschrieben, für die gilt:

- N ist verloren, d.h. kein Gerät G2 hat N eingelöst, und
- $s_{G1}(r,N,z)$ taucht in einer Liste WL_{G2} auf und für alle weiteren Einträge $s_{G3}(r',N,z')$ für verlorene G3 in Listen WL_{G4} gilt $z' < z$.

Um letzteres zu prüfen, muß die Bank mit dem Schlüssel s_G jedes verlorenen Gerätes G jeden Eintrag jeder WL-Liste einmal entschlüsseln und anhand der Redundanz r prüfen, ob er von G erzeugt wurde.

Protokollskizze 5 Anonyme verteilte Aufzeichnung: Standardwerttransaktionen

Die Korrektheit des Verfahrens wird dadurch, daß in [4] nur noch Einträge für verlorene Geräte G3 betrachtet werden können, offensichtlich nicht beeinträchtigt.

Der Speicherbedarf der einzelnen Geräte ist ebenso hoch wie im nicht anonymen Fall, der der Rücksetzprozedur unterscheidet sich kaum.

Die Rücksetzprozedur wird allerdings etwas zeitaufwendiger: jeder Änderungsvermerk muß mit dem Schlüssel jedes verlorenen Gerätes probeweise entschlüsselt werden, so daß der Zeitaufwand dieses Teils der Prozedur nun auch proportional zur Anzahl der verlorenen Geräte wächst.

Das Problem, nachzuprüfen, ob ein Änderungsvermerk sich auf ein verlorenes Gerät bezieht, kann man jedoch auch lösen, indem jedes Gerät seine Vermerke wieder mit expliziten Kennzeichen versieht, die aber nun pseudozufällig gewählt werden.

Sind der Bank zum Rücksetzen alle möglichen Transaktionskennzeichen aller verlorenen Geräte bekannt, so erfordert das Nachprüfen nun einen Zeitaufwand, der proportional zum Logarithmus der Anzahl all dieser Transaktionskennzeichen wächst (wobei die einzelnen Schritte relativ einfach sind), statt direkt proportional zur Anzahl der verlorenen Geräte (wobei jeder Schritt eine aufwendige Entschlüsselung enthält). Für eine genauere Beschreibung der Erzeugung und Verwendung zusätzlicher Transaktionskennzeichen sei auf [WaPf_87] verwiesen.

Welches von beiden Verfahren das effizientere ist, hängt also von den jeweiligen Systemparametern ab.

Soll zur Erhöhung der Verlusttoleranz ein Änderungsvermerk mehrfach weitergegeben werden, so geschieht dies am einfachsten durch den Zahlungsempfänger G2 (der ja auch ein größeres Interesse daran haben wird als der Zahlende G1): er übergibt nicht nur dem Zahlenden den Änderungvermerk, sondern auch noch n weiteren Geräten, die diesen in ihren WL-Listen abspeichern. Um zu verhindern, daß die Bank auch ohne Kenntnis von s_{G2} aus dem mehrmaligen Auftauchen gleicher Einträge in verschiedenen Listen Schlüsse ziehen kann, muß dabei der Änderungsvermerk für jede Weitergabe verschieden aussehen. Dies wird am einfachsten durch n verschiedene Werte r_i für r erreicht.

Soll statt des Empfängers doch der Zahlende $s_{G2}(r,N,z)$ weitergeben, so muß G2 den Änderungsvermerk in n Versionen $s_{G2}(r_i,N,z), i = 1,...,n$, an G1 übergeben und G1 jeden Vermerk genau einmal weitergeben.

Durch die Erweiterung erhöht sich, wie in 4.1.3, sowohl der Speicherbedarf der Geräte als auch der Zeitaufwand der Rücksetzprozedur um den Faktor n.

Soll schließlich zur Sicherung gegen die Bank jedem Änderungsvermerk noch die Vorgeschichte aller anderen Weitergaben von N hinzugefügt werden (vgl. 4.1.3), so genügt der hier vorgestellte Ansatz zur Anonymisierung nicht. $s_G(r,N,z)$ müßte in allen Weitergabelisten auftauchen, die Weitergaben von (N,z') mit $z' > z$ vermerken. Da dies beliebig viele sein können, kann G nicht bereits wie oben während der Zahlung alle notwendigen Einträge durch verschiedene Werte für r erzeugen.

Ähnliche Schwierigkeiten ergeben sich auch bei der Anonymisierung der in 4.1.2 erwähnten vollständigen Verteilung, da auch hier Änderungsvermerke in beliebig vielen Geräten abgespeichert werden können.

Abhilfe schafft hier wieder die Verwendung von pseudozufälligen expliziten Transaktionskennzeichen zur Zuordnung von T_G zu G und von Einwegfunktionen zur unterschiedlichen Verschlüsselung von (T_G, N, z). Da die resultierenden Verfahren in jedem Fall einen sehr viel höheren

Speicherbedarf der Geräte und Rücksetzaufwand der Bank erfordern als bei Verwendung markierter Standardwerte (evtl. mit n-maliger Weitergabe), sei an dieser Stelle nicht näher darauf eingegangen. Einzelheiten findet man in [WaPf_87].

5 Resümee

Die in den Kapiteln 3 und 4 dargestellten Überlegungen zeigen, daß trotz der Forderungen nach Betrugssicherheit, Anonymität und Autonomie auf elektronische Brieftaschen zur Fehlertoleranz übliche Verfahren ohne übermäßige Erhöhung der Speicher- und Zeitkomplexität der Zahlungsprotokolle angewendet werden können:

Verfahren, die durch Maßnahmen des Gerätes G alleine ein Rücksetzen sofort nach dem Verlust von G erlauben, müssen zwangsläufig die Verfügbarkeit von K_G und die Autonomie von G beschränken, so daß man statt spezieller Fehlertoleranzmaßnahmen genausogut einen vor Verlust zu schützenden Geldbetrag von einem sicheren Gerät auf ein spezielles sichereres (oder ein anonymes Konto) transferieren kann. Die Höhe des möglichen Verlustes ist dabei durch den Besitzer selbst begrenzbar, und Verfahren dieser Art sind mit allen anderen Verfahren zur Verlusttoleranz kombinierbar, sofern garantiert ist, daß der Verlust den Besitz zum Verlustzeitpunkt nie übersteigt.

Zur weiteren Verringerung der erwarteten Verluste ist eine Änderungsaufzeichnung der Transaktionen eines Gerätes nötig, die aufgrund der Forderung nach Autonomie verteilt erfolgen muß, so daß hier spezielle Weitergabeprotokolle notwendig sind. Da alle anderen Verfahren einen relativ hohen Speicherbedarf für die Geräte und einen hohen Rücksetzaufwand für die Bank verursachen, beschränkte sich die Diskussion auf das Verfahren der markierten Standardwerttransaktionen (4.1.3 und 4.2).

Die Verlusttoleranz des Verfahrens dürfte insbesondere bei mehrfacher Weitergabe von Änderungsvermerken recht hoch sein. Ein verlorenes Gerät kann jedoch erst nach einer gewissen Wartezeit rückgesetzt werden. Hinsichtlich Betrugssicherheit, Anonymität und Einsatzmöglichkeit von Rücksetzpunkterstellung zur Sicherung von Änderungsaufzeichnungen ist das Verfahren als sehr zufriedenstellend zu bewerten.

Noch wichtiger als die Verlusttoleranz ist aber das Problem, ob und wie Geräte so gebaut werden können, daß sie die Bezeichnung „sicheres Gerät" verdienen. Die heutigen Chipkarten sind in diesem Sinne vermutlich nicht sicher und stellen für die hier behandelte Anwendung auch keinen vernünftigen Ersatz für sichere Geräte dar.

Solange dieses Problem nicht gelöst ist, ist von einem digitalen Zahlungssystem mit der Fähigkeit zu autonomen Zahlungen, ob mit oder ohne Verlusttoleranz, aus Sicherheitsgründen abzuraten.

Für ihre Kritik und Diskussionsbereitschaft danken wir Birgit Baum, Dr. Klaus Echtle, Prof. Winfried Görke, Andreas Pfitzmann und Dr. Karl Rihaczek. Der Deutschen Forschungsgemeinschaft (DFG) danken wir für ihre freundliche Unterstützung, die diese Arbeit erst möglich gemacht hat.

Stichwörter: Anonymität, Betrugssicherheit, Chipkarte, digitales Zahlungssystem, elektronische Brieftasche, Fehlertoleranz, markierte Standardwerte, Rücksetzen, sichere Geräte, Verlusttoleranz, verteilte Änderungsaufzeichnung

Literatur

Akl_83 S.G. Akl: Digital Signatures: A Tutorial Survey; Computer 16/2 (1983) 15–24

AnLe_81 T. Anderson, P. A. Lee: Fault Tolerance, Principles and Practice; Prentice-Hall International, London 1981

BüPf_86 H. Bürk, A. Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Proc. 4th Intern. Conf. on Computer Security, Monte Carlo, Dez. 1986, erscheint bei North-Holland, 1987

Chau_85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; CACM 28/10 (1985) 1030–1044

Denn_82 D. E. Denning: Cryptography and Data Security; Addison-Wesley, Reading 1982

EvGY_84 S. Even, O. Goldreich, Y. Yacobi: Electronic Wallet; Proc. 1984 Intern. Zurich Seminar on Digital Communications, March 1984, Zurich, Swiss Federal Inst. of Technology, IEEE, 199–201

GoMR_84 S. Goldwasser, S. Micali, R. L. Rivest: A „Paradoxical" Solution to the Signature Problem; 25th FOCS, Oct. 1984, IEEE Computer Society, 441–448

Hors_85 P. Horster: Kryptologie; Reihe Informatik/47, Bibliogr. Institut, Mannheim 1985

Levi_85 L. A. Levin: One-way functions and pseudorandom generators; 17th STOC, ACM, New York 1985, 363–365

LuRa_86 M. Luby, C. Rackoff: Pseudo random permutation generators and cryptographic composition; 18th STOC, ACM, New York 1986, 356–363

PfPW_86 A. Pfitzmann, B. Pfitzmann, M. Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen – Warum und wie?; DuD Heft 3 (1986) 178–191

PlLe_86 G. M. J. Pluimakers, J. van Leeuwen: Authentication: A Concise Survey; Computers & Security, North-Holland, 5/3 (1986) 243–250

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, LNCS 60, Springer-Verlag 1978; nachgedruckt als Springer Study Edition, Springer-Verlag, Heidelberg 1979, 209–227

PWP_87 B. Pfitzmann, M. Waidner, A. Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, erscheint in Computer und Recht (CR) 10, 11, 12 (1987)

Riha_85 K. Rihaczek: Der Stand von OSIS; DuD Heft 4 (1985) 213–217

Schn_83 F. B. Schneider: Fail-Stop Processors; IEEE Digest of Papers from Spring CompCon '83, San Francisco, March 1983, 66–70

Schr_86 H. Schrenk: Neuartiges Chipkartenkonzept mit dem „Intelligenten" Speicher SLE 4401 K; Siemens telcom report, 9/1 (1986) 88–91

Tane_81 A. S. Tanenbaum: Computer Networks; Prentice-Hall, Englewood Cliffs 1981

TuCh_85 M. Turoff, S. Chinai: An Electronic Information Marketplace; Computer Networks and ISDN Systems 9/2 (1985) 79–90

WaPf_87 M. Waidner, B. Pfitzmann: Anonyme und verlusttolerante elektronische Brieftaschen; Interner Bericht 1/87 der Fakultät für Informatik, Univ. Karlsruhe 1987

Wein_84 S. B. Weinstein: Smart credit cards: the answer to cashless shopping; IEEE Spectrum Feb. (1984) 43–49