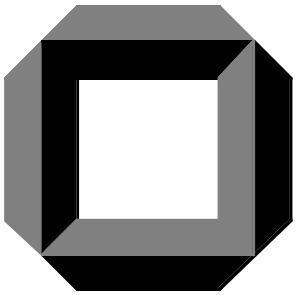


UNIVERSITÄT KARLSRUHE

FAKULTÄT FÜR INFORMATIK

Postfach 6980, D 7500 Karlsruhe

Anonyme und verlusttolerante elektronische Brieftaschen

Michael Waidner, Birgit Pfitzmann
Institut für Rechnerentwurf und Fehlertoleranz
(früher Institut für Informatik IV)

Interner Bericht 1/87

Zusammenfassung

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 korrekte Abwicklung digitaler Zahlungen garantieren, angewiesen. Aus Sicherheitsgründen müssen diese Geräte über eine eingebaute Tastatur und eine eingebaute Anzeige direkt mit ihrem Benutzer kommunizieren können. (Heutige Chipkarten sind daher, ihre zweifelhafte Ausforschungssicherheit und starke Beschränktheit im Funktionsumfang unbeachtet, als elektronische Brieftaschen untauglich.)

Neben der Verläßlichkeit der physischen Sicherheitstechnik ist vor allem die Tolerierung von Verlusten oder vollständigen Ausfällen, mit denen ohne Fehlertoleranzmaßnahmen ein Geldverlust verbunden wäre, ein Problem. Wir untersuchen unter der Annahme der Existenz idealer sicherer Geräte die prinzipiellen Möglichkeiten für *Verlusttoleranzmaßnahmen*, wobei sowohl die Erhaltung der Sicherheit des Zahlungssystems als auch des Datenschutzes der Teilnehmer (Unbeobachtbarkeit von Zahlungen) berücksichtigt werden muß.

Es ergibt sich dabei in natürlicher Weise eine Klasse sicherer Verfahren zur verteilten Änderungsaufzeichnung, die *Weitergabeverfahren*, die jedoch aufgrund ihres sehr hohen Speicherbedarfes unpraktikabel erscheinen. Aus ihnen läßt sich jedoch eine weitere Klasse ableiten, die der *markierten Standardwerttransaktionen*, welche die sonstigen Eigenschaften elektronischer Brieftaschen kaum beeinträchtigen und damit zur Konstruktion verläßlicher Verlusttoleranzverfahren geeignet sind.

Schlagwörter

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

Abstract

If a payment system is to be used for payments over a communication network as well as for off-line payments, "electronic wallets" are needed, i.e. tamper-resistant devices guaranteeing the correctness of digital payments. For reasons of security, these devices have to communicate with their users by built-in keyboards and displays. (Therefore, and because of their doubtful tamper-resistance and restricted functionality, chipcards as manufactured today are unsuitable for electronic wallets.)

Besides the trustworthiness of the physical security techniques, the main problem with such devices is how to tolerate complete failures or losses, which would imply a loss of money, if no fault tolerance measures were taken. On the assumption that ideally tamper-resistant devices exist we discuss the possibilities for such *loss tolerance* measures, taking into account both the preservation of security of the payment system and the preservation of the users' privacy.

In a natural way we get a class of secure procedures for distributed auditing, the *passing-on procedures*. Because of their high memory-requirements they seem to be unsuitable. But from these we can derive the class of *marked standard value transactions*, which can be used to construct efficient mechanisms providing high fault tolerance and leaving security, privacy, and the ability for off-line payments of electronic wallets nearly unchanged.

Keywords

Anonymity, security against fraud, chipcard, digital payment system, electronic wallet, fault tolerance, marked standard value transactions, backward error recovery, tamper-resistant device, loss tolerance, distributed audit trail, passing-on procedure.

Gliederung

1 Motivation 1

2 Zahlungen mit elektronischen Brieftaschen 4

3 Prinzipielle Möglichkeiten zur Verlusttoleranz 8

3.1 Rücksetzbares Objekt 9
3.2 Abschätzung der Rücksetzabweichung 10
3.2.1 Rücksetzen ohne Wartefristen 10
3.2.2 Änderungsaufzeichnung 11

4 Verteilte Änderungsaufzeichnung 13

4.1 Unsicherheit der einfachen Aufzeichnung 14
4.2 Sicherheit durch Weitergabe 16
4.2.1 Maximale Weitergabe 16
4.2.1.1 Protokoll, Sicherheit und Verlusttoleranz 16
4.2.1.2 Notwendigkeit der Systemterminierung 19
4.2.1.3 Aufwand 20
4.2.1.4 Verteilte Kontostände 23
4.2.2 Überdeckungsverfahren 24
4.2.2.1 Protokoll, Sicherheit und Verlusttoleranz 24
4.2.2.2 Aufwand 29
4.2.3 Minimale Überdeckungen durch Standardwerte 32
4.2.4 Grenzen allgemeiner Weitergabeverfahren 34
4.3 Markierte Standardwerte 37
4.3.1 Protokoll, Sicherheit und Verlusttoleranz 37
4.3.1.1 Grundprinzip 37
4.3.1.2 Rücksetzzeitpunkte 38
4.3.1.3 Umgang mit Zeitabweichungen 40
4.3.1.4 Protokoll 41
4.3.1.5 Sicherheit und Verlusttoleranz 42
4.3.2 Aufwand 43
4.3.2.1 Aufwand der sicheren Geräte 43
4.3.2.2 Aufwand zum Rücksetzen 45
4.3.2.2.1 Minimaler Aufwand bei gleichzeitiger Systemterminierung 46
4.3.2.2.2 Rücksetzen ohne gleichzeitige Systemterminierung 49
4.3.2.2.2.1 Parameter 49
4.3.2.2.2.2 Bearbeiten der WL-Listen 50

4.3.2.2.2.3 Verfahren 1: Vorsortieren der WL-Listenreste 52
4.3.2.2.2.4 Verfahren 2: Vorsortieren von BL_B 55
4.3.2.2.2.5 Abschließende Bemerkungen 57

5 Anonymisierung 59
5.1 Angreifermodelle 59
5.2 Schutzmechanismen 64
5.2.1 Verbergung des Inhalts der Vermerke nicht verlorener Geräte 64
5.2.1.1 Verbergung des Inhalts im Modell A1 64
5.2.1.2 Verbergung des Inhalts im Modell A3 65
5.2.1.2.1 Verschlüsselung zum Schutz des Inhalts 65
5.2.1.2.2 Anonyme Kennzeichnung 65
5.2.1.2.2.1 Verschlüsselung mit Redundanz 65
5.2.1.2.2.2 Pseudozufällige Kennzeichen 65
5.2.2 Verbergung des aufzeichnenden Gerätes 67
5.2.3 Verhinderung statistischer Auswertungen in A2 und A3 68
5.2.3.1 Verbergung der Gleichheit zweier Vermerke in Modell A2 70
5.2.3.1.1 Unterschiedliche Verschlüsselung mit Redundanz 70
5.2.3.1.2 Pseudozufällige Kennzeichen 71
5.2.3.1.2.1 A priori festgelegte Kennzeichen 71
5.2.3.1.2.2 Dynamisch bestimmte Kennzeichen 72
5.2.3.2 Verbergung der Gleichheit zweier Vermerke in Modell A3 73
5.3 Protokolle, Aufwand 75
5.3.1 Weitergabeverfahren 76
5.3.1.1 Protokolle 76
5.3.1.2 Aufwand 77
5.3.1.2.1 Verschlüsselung mit Redundanz 77
5.3.1.2.2 Pseudozufällige Kennzeichen 78
5.3.1.2.3 Vergleich der Kennzeichnungsverfahren 78
5.3.2 Markierte Standardwerte 79
5.3.2.1 Protokolle 79
5.3.2.2 Aufwand 80
5.3.2.2.1 Verschlüsselung mit Redundanz 81
5.3.2.2.2 Pseudozufällige Kennzeichen 81
5.3.2.2.3 Vergleich der beiden Kennzeichnungsverfahren 82
5.3.2.2.4 Eingeschränkte Anonymität 82
5.3.3 Zusammenfassung 83

6 Resümee 85

7 Anhang 87
7.1 Literatur 87
7.2 Mathematische Symbole 88

Protokollskizzen

Protokollskizze 1 Grundschema für ein Zahlungssystem mit elektronischen Brieftaschen.....5
Protokollskizze 2 Grundschema für das Rücksetzen eines Gerätes G auf G'.....9
Protokollskizze 3 Grundschema für die verteilte Änderungsaufzeichnung..... 14
Protokollskizze 4 Verteilte Aufzeichnung: maximale Weitergabe..... 16
Protokollskizze 5 Verteilte Aufzeichnung: Klasse der Überdeckungsverfahren zur Überdeckung μ..... 26
Protokollskizze 6 Verteilte Aufzeichnung: Standardwerttransaktionen..... 41
Protokollskizze 7 Beginn der Rücksetzprozedur zu einem Zeitpunkt $b+\Delta_1+\Delta_2$..... 51
Protokollskizze 8 Fortsetzung 1 der Rücksetzprozedur zu einem Zeitpunkt $b+\Delta_1+\Delta_2$..... 53
Protokollskizze 9 Fortsetzung 2 der Rücksetzprozedur zu einem Zeitpunkt $b+\Delta_1+\Delta_2$..... 56

Bilder

Bild 1 Eliminierung der Rücksetzabweichung durch Änderungsaufzeichnung..... 12
Bild 2 Übersicht zu Kapitel 4..... 13
Bild 3 Verlust zweier aufeinanderfolgender Geräte..... 15
Bild 4 Zwei für die Bank zum Rücksetzzeitpunkt ununterscheidbare Situationen 20
Bild 5 Konstruktion einer feinsten linearisierbaren Überdeckung 26
Bild 6 Beispiel eines Überdeckungswechsels..... 35
Bild 7 WL- und BL-Listen nach Weitergabe eines Standardwertes N..... 38
Bild 8 Dauer des „kleinen" Zahlungssystems zum Standardwert N..... 39
Bild 9 Für das Rücksetzen von G zu berücksichtigende andere Geräte..... 40
Bild 10 Weitergabebaum 44
Bild 11 Für das Bearbeiten einer Liste WL_G zu berücksichtigende verlorene Geräte..... 51
Bild 12 Beim Bearbeiten eines Teils von BL_B zu berücksichtigende Teile der VL-Listen..... 53
Bild 13 Für das Bearbeiten einer Liste VL_G zu berücksichtigende Standardwerte 56
Bild 14 Informationsquellen des Angreifers 60
Bild 15 Angreifermodelle..... 63
Bild 16 Erzeugung pseudozufälliger Gerätekennzeichen..... 66
Bild 17 Verschlüsselungen des Vermerkes V unter Annahme des Angreifermodelles A2..... 70
Bild 18 Verschlüsselungen und pseudozufällige Kennzeichnungen des Vermerkes V unter Annahme des Angreifermodelles A2 72
Bild 19 Verschlüsselungen des Vermerkes V unter Annahme des Angreifermodelles A3..... 74
Bild 20 Verschlüsselungen des Vermerkes V unter Annahme des abgeschwächten Angreifermodelles A3 74
Bild 21 Rücksetzaufwand..... 83
Bild 22 Speicherbedarf der sicheren Geräte..... 84
Bild 23 Vergleich der Verfahren..... 86

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 (d.h. die Anonymität der Teilnehmer ermöglichenden) 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, Chau_87, 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.

Ein sicheres Gerät muß sich (seiner Einsatzweise entsprechend) im Besitz seines Benutzers befinden, so daß dieser die physische 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, GoMR_88, 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 die Ausforschungssicherheit nur dann hilft, wenn keine vertraulichen Daten außerhalb des sicheren Gerätes verarbeitet werden müssen. Zur Erfüllung aller Aufgaben des Zahlungssystems muß es daher im Gegensatz zu heutigen Chipkarten zumindest etwa dieselben Verarbeitungs- und Speicherfähigkeiten besitzen wie heutige PCs. 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 Geldverlust 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 ($b \geq 0$) genau dann, wenn B_G den Auftrag zu dieser Zahlung erteilt hat, wenn $b \leq K_G$ und wenn es sicher ist, daß ein anderes sicheres Gerät seinen Kontostand entsprechend um b erhöht.

Umgekehrt erhöht es K_G um b ($b \geq 0$) 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 $K_G \geq 0$ 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 passiv 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 können.

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_87], 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 [Yao_82] 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 (oder 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 ($b \geq 0$) 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 auf der folgenden Seite 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.

Dazu müssen sich die Blockierungszustände der Geräte G1 und G2 nach außen hin nicht unbedingt unterscheiden, sondern es genügt, daß die Bank dem Gerät mitteilt, ob das Partnergerät verloren ist oder nicht. Im zweiten Fall kann das Gerät selbständig entscheiden, ob es die letzte oder die vorletzte Nachricht erwartete, und entsprechend die Transaktion für gültig bzw. ungültig erklären.

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 des Verlustes durch Fehler des Gerätes sicher sinnvoll. Das Verlegen eines Gerätes kann man damit allerdings selten tolerieren, da die 2-von-3-Systemen eigene Annahme, daß Fehler unabhängig voneinander auftreten und Doppelfehler damit unwahrscheinlich sind, gerade hier nicht zutrifft. Verlegt 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 verlegen. 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, z.B. nach größeren Einnahmen, ändern lassen und somit den möglichen Verlust selbst begrenzen.

Damit ergibt sich, daß für elektronische Brieftaschen das Erstellen von „Rücksetzpunkten" einfach dem Vorgehen entspricht, Geld, das man nicht verlieren möchte, nicht mit sich herumzutragen.

Um dabei die 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 man einen Transfer zwischen sicheren Geräten und einem anderen, nicht auf sicheren Geräten basierenden Zahlungssystem ermöglicht, wobei sinnvollerweise die Bank als Mittler verwendet wird, der in beiden Zahlungssystemen als Teilnehmer auftreten kann [PWP_87].

Möchte man jedoch vermeiden, daß die Bank die Höhe von $K_{G'}$ erfährt, aber dennoch auf ein zweites sicheres Gerät G^* verzichten, so muß B_G bei der Bank einen passiven, für die Bank im Normalfall unlesbaren Rücksetzpunkt hinterlegen.

Um beim Rücksetzen entscheiden zu können, welcher Rücksetzpunkt aktuell ist, werden diese von G fortlaufend durchnumeriert und unterschrieben [Denn_82, GoMR_88, PlLe_86]. Dabei muß der Signierschlüssel von G eigens hierfür gewählt sein, der zugehörige Testschlüssel schon bei der Initialisierung von G dem Besitzer B_G und der Bank mitgeteilt werden (durch G, damit klar ist, daß die Mitteilung korrekt ist) und die Bank muß B_G unterschreiben, daß alle so unterschriebenen Rücksetzpunkte B_G zugerechnet werden.

Um die gewünschte Anonymität zu erzielen, werden die eigentlichen Rücksetzdaten (also der Wert $K_{G'}$) mit einem ebenfalls eigens zu diesem Zweck von G oder B_G gewählten und nur diesen bekannten Schlüssel s_R eines symmetrischen Kryptosystems verschlüsselt. Um später den korrekten Schlüssel erkennen zu können, unterschreibt G für B_G diesen Schlüssel mit dem oben gewählten Signierschlüssel.

Möchte B_G auf G wieder über $K_{G'}$ verfügen, so muß G einen neuen Rücksetzpunkt erstellen und vertraulich an die Bank senden. Der erhaltene Rücksetzpunkt wird von der Bank sofort als der aktuell gültige registriert und eine entsprechende Quittung an G zurückgeschickt. G bleibt solange blockiert, bis es die Quittung der Bank erhält; im Notfall muß G der Bank vorgelegt und die Quittung nachgereicht werden. (Dies ist in stark vereinfachter Form dasselbe Quittungsprotokoll, wie es in Anschluß an Protokollskizze 1 geschildert wurde.)

Nach Erhalt der Quittung gibt G den Rücksetzpunkt nochmals, nun aber an den Besitzer B_G, aus. Sowohl die Bank als auch B_G selbst speichern jeweils den aktuellen Rücksetzpunkt.

Geht G verloren, so meldet B_G dies unterschrieben der Bank, die ab diesem Zeitpunkt keinen neuen Rücksetzpunkt von G mehr akzeptiert. Sodann bestimmt B_G ein Ersatzgerät G', dem er und die Bank jeweils den aus ihrer Sicht aktuellen Rücksetzpunkt übergeben, und das von B_G zusätzlich noch s_R und den zu G gehörenden Testschlüssel erhält. G' prüft die Authentikation des Schlüssels s_R und der beiden erhaltenen Rücksetzpunkte, entschlüsselt ggf. den neuesten (wobei im korrekten Fall beide identisch sein müssen) und übernimmt $K_{G'}$ als seinen Kontostand.

Eine Verbergung der Identität des Gerätes G beim Rücksetzpunkterstellen ist mit dem geschilderten Ansatz nicht möglich, da die Bank jeden Versuch eines rückgesetzten, aber möglicherweise noch existierenden Gerätes, einen weiteren Rücksetzpunkt zu erstellen, zurückweisen können muß. Auf die Abspeicherung der Rücksetzpunkte von G durch B_G kann allerdings verzichtet werden, wenn man der Bank entsprechend vertraut.

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 erzwingen, daß 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.

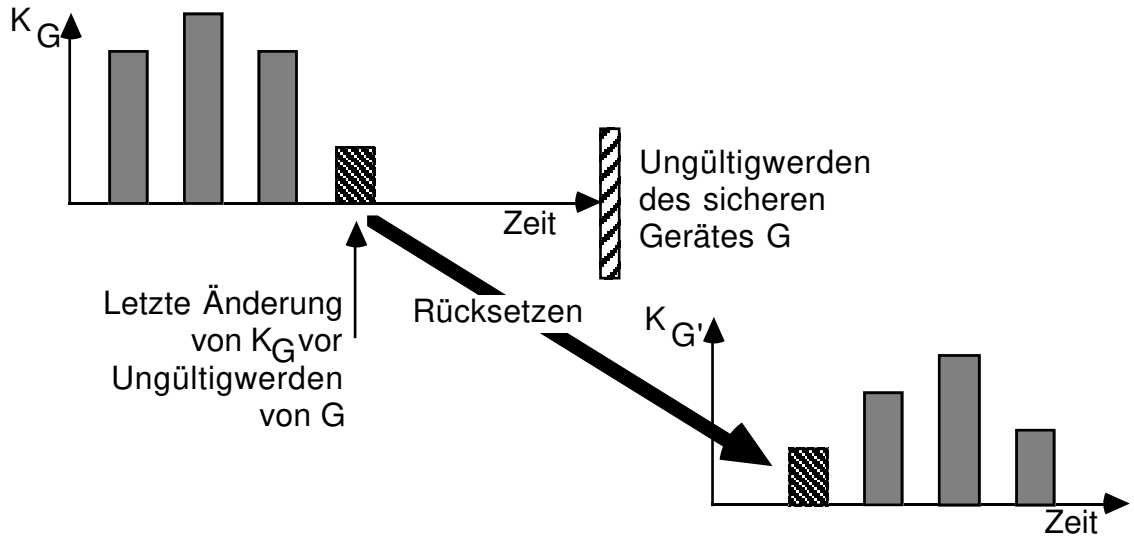


Bild 1 Eliminierung der Rücksetzabweichung durch Änderungsaufzeichnung

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.

Dies bedeutet jedoch auch, daß eine vollständige Eliminierung der Rücksetzabweichung für manche Verlustsituationen prinzipiell unmöglich ist: Soll keine Transaktion zum Rücksetzen unberücksichtigt bleiben, so muß zwangsläufig jedes sichere Gerät die vollständige Änderungsaufzeichnung enthalten.

Diese Forderung ist jedoch nicht erfüllbar: zerfällt z.B. 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 berücksichtigt werden.

Ist ein Gerät G nicht verloren, so könnte sich B_G daher einen Vorteil davon versprechen, sein Gerät nach dessen Ungültigwerden absichtlich zu verlieren: B_G verliert nichts, wenn er vorher sein Gerät leert, G könnte aber durch Rücksetzen zufällig noch früher besessenes Geld zurück erhalten. 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 seine Rücksetzinformationen an die Bank sendet und dafür eine Quittung erhält.

Die Untersuchung der Möglichkeiten für eine verteilte Änderungsaufzeichnung stellen den Schwerpunkt dieser Arbeit dar. Sie sollen daher in den folgenden beiden Kapiteln behandelt werden. In Kapitel 4 werden die prinzipiellen Verfahren und deren Sicherheit diskutiert. Die aus Anonymitätsgründen notwendigen Änderungen dieser Verfahren werden in Kapitel 5 dargestellt.

4 Verteilte Änderungsaufzeichnung

Um die Übersicht über dieses Kapitel zu erleichtern, sind vorweg in Bild 2 die darin behandelten Verfahren dargestellt.

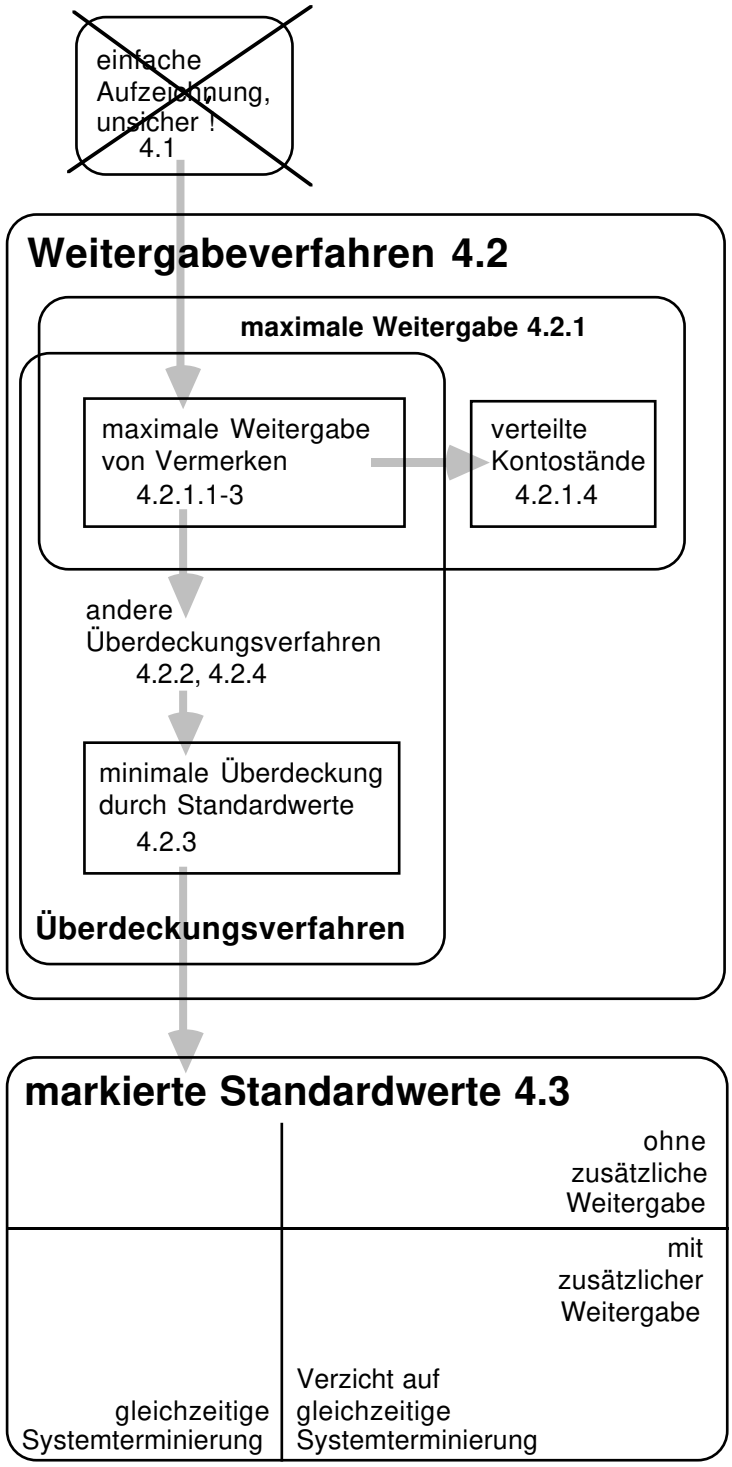


Bild 2 Übersicht zu Kapitel 4. Die abgerundeten Rahmen geben die Einteilung der Verfahren in Klassen an, die eckigen Rahmen bezeichnen die wesentlichen Verfahren, die Pfeile zeigen, welche Verfahren aus welchen hergeleitet werden.

Im folgenden bezeichne T(t,G1,G2,b) eine Zahlung zum Zeitpunkt t von G1 an G2 mit dem Betrag b ($b \geq 0$). Um die Transaktion dokumentieren zu können, müssen sie beide Geräte jeweils so kennzeichnen, daß der Änderungsaufzeichnung 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.

Als T_G kann dabei beispielsweise die Zufallszahl dienen, die G zum Zwecke der Authentikation (vgl. Kapitel 2, Schritt [2] der Zahlung in Protokollskizze 1) sowieso für diese Zahlung eindeutig wählen mußte. Etwas kürzer wird die Aufzeichnung, wenn jedes Gerät einfach seine Transaktionen durchnumeriert. Daß die Geräte sich statt der Verwendung zweier T_G auf ein gemeinsames Transaktionskennzeichen einigen, bringt keine Vorteile.

4.1 Unsicherheit der einfachen Aufzeichnung

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 für es eindeutig kennzeichnet.

[4.2] Wie Schritt [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 erhaltenen Änderungsaufzeichnungen werden nach Einträgen (G,b,T) untersucht. Die darin verzeichneten 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 3):

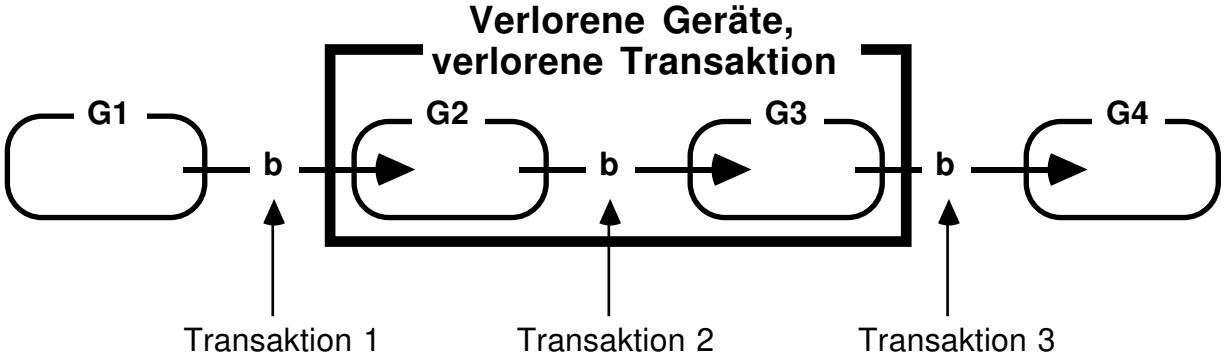


Bild 3 Verlust zweier aufeinanderfolgender Geräte

- 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 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.

4.2 Sicherheit durch Weitergabe

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

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

4.2.1 Maximale Weitergabe

Wie in 3.2.2 begründet, müßte für eine vollständige Eliminierung jeder Rücksetzabweichung jedes Gerät die gesamte Änderungsaufzeichung enthalten, was jedoch unter Wahrung der Autonomie nicht erzwungen werden kann.

Die maximal erreichbare Verlusttoleranz erhält man daher, wenn jedes Gerät alle ohne Kommunikation mit der Bank, d.h. von anderen Geräten während einer Transaktion erreichbare Rücksetzinformationen aufzeichnet.

4.2.1.1 Protokoll, Sicherheit und Verlusttoleranz

Um dies zu erreichen, müssen die Geräte die Aufzeichnungen über Transaktionen durch Fluten (flooding, [Tane_81]) möglichst vollständig verteilen:

Jedes sichere Gerät G1 führt eine Liste L_{G1}, die alle G1 bekannten Änderungen verzeichnet. Zur Initialisierung ist L_{G1} leer. Bei jeder Transaktion, an der G1 beteiligt ist, fügt G1 zunächst seine eigene Information über die laufende Transaktion in L_{G1} ein, gibt diese an seinen Partner G2 und erhält umgekehrt von seinem Partner dessen Liste L_{G2}, die G1 in seine eigene unter Beseitigung von Duplikaten einfügt.

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 für es eindeutig kennzeichnet.
- [4.2] G1 (bzw. G2) fügt den Änderungsvermerk (G1,-b,T_{G1}) (bzw. (G2,b,T_{G2})) in die Liste L_{G1} (bzw. L_{G2}) ein. G1 und G2 tauschen ihre Listen L_{G1} bzw. L_{G2} aus.
- [4.3] Zur Sicherung der Unteilbarkeit der Zahlung sendet eines der beiden Geräte eine Quittung (vgl. Schritt [4] in Protokollskizze 1).
- [4.4] G1 (bzw. G2) fügt die Liste L_{G2} (bzw. L_{G1}) in seine eigene ein.

Ungültigwerden und Rücksetzen der sicheren Geräte

[1] Zu einem von der Bank festgelegten und allgemein bekannten Zeitpunkt werden alle Geräte ungültig. Alle nicht verlorenen Geräte transferieren ihr Guthaben in ein

anderes Zahlungssystem oder auf ihr Nachfolgegerät und teilen zugleich der Bank ihre Änderungsaufzeichnungen mit.

[2] Jedes sichere Gerät G, das in [1] seine Änderungsaufzeichnung der Bank nicht mitgeteilt hat, wird rückgesetzt.
Hierzu werden die von allen sicheren Geräten erhaltenen Änderungsaufzeichnungen nach Einträgen (G,b,T) untersucht. Die gefundenen Änderungen werden ausgehend von der Initialisierung von K_G nachvollzogen und so K_G rekonstruiert.

Protokollskizze 4 Verteilte Aufzeichnung: maximale Weitergabe

Zu einer bestimmten Transaktion T=T(t,G1,G2,b) und einem Zeitpunkt t' sei die Menge der sicheren Geräte, die die Transaktion zum Zeitpunkt t' aufgezeichnet haben, mit $M_T(t')$ bezeichnet. Sie ist gegeben durch:

- Für alle t'<t ist $M_T(t') = \emptyset$
- $M_T(t) = \{G1, G2\}$.
- Ist $G3 \in M_T(t')$ und nimmt G3 zum Zeitpunkt t' eine Transaktion mit G4 vor, so gilt für alle t">t': $G3, G4 \in M_T(t")$.

Sei t_R der Zeitpunkt, an dem die Bank alle Änderungsaufzeichnungen zum Rücksetzen besitzt und $M_T = M_T(t_R)$.

Das Verfahren garantiert:

- Eine Transaktion T taucht in der Änderungsaufzeichnung der Bank genau dann auf, wenn wenigstens ein Gerät aus M_T zum Zeitpunkt des Rücksetzens nicht verloren ist.
- Durch Rücksetzen wird kein Kontostand K_G auf einen negativen Wert gesetzt.
  Grund hierfür ist, daß, falls die Bank eine K_G belastende Transaktion T nachvollzieht, sie auch alle zuvor stattgefundenen Transaktionen von G nachvollziehen kann, da diese in den Geräten aus M_T ebenfalls vermerkt sein müssen. Da angenommen wird, daß das Grundprotokoll die Anforderungen aus Kapitel 2 erfüllte, folgt die Behauptung.
- Durch Rücksetzen ändert sich die Summe aller Kontostände nicht.
  Man betrachte hierzu eine Transaktion T(t,G1,G2,b). Sind beide Geräte verloren, so vollzieht die Bank, da $(G1,-b,T_{G1})$ und $(G2,b,T_{G2})$ stets gemeinsam weitergegeben werden, die Transaktion entweder für keines oder für beide Geräte nach. Ist nur ein Gerät verloren und wurde sie daher beim nicht verlorenen Partner dank der Sicherheit der Geräte korrekt verbucht, so wird sie dank dessen Änderungsaufzeichnung auch für den verlorenen Partner nachvollzogen.
  Diese Eigenschaft war, bei Zulassung negativer Kontostände, natürlich auch im Verfahren aus Protokollskizze 3 gegeben.

Im allgemeinen wird die Rücksetzabweichung sehr gering sein, da zumindest beinahe jede Transaktion T, die weit vor dem Verlustzeitpunkt eines der beteiligten Geräte liegt, aufgefunden wird, da M_T für solche Transaktionen meist sehr groß ist. Das Verfahren garantiert jedoch, wie alle auf verteilten Änderungsaufzeichnungen beruhenden Verfahren, keine feste obere Schranke für die Rücksetzabweichung, so daß diese Forderung der Verlusttoleranz nicht erfüllt ist.

Da aber alle Kontostände stets größer Null bleiben, ist zumindest garantiert, daß B_G nicht mehr verlieren kann, als er zum Zeitpunkt des Verlustes von G besaß, so daß jetzt das gelegentliche Erstellen von Rücksetzpunkten durch Überweisen eines Betrages im Sinne von 3.2.1 sinnvoll

erscheint. Wird dazu ein anderes sicheres Gerät G^* von B_G verwendet, so braucht der Betrag aber nicht auf G^* „gesperrt" zu werden, sondern kann sofort wieder zurücküberwiesen werden: durch die Übergabe von L_G an G^* ist die gesamte Vorgeschichte von G in G^* dokumentiert.

Die Bank kann bei diesem Verfahren Teilnehmer, deren Geräte nicht verloren sind, natürlich genausowenig betrügen wie beim zugrundeliegenden Zahlungssystem ohne Verlusttoleranz. Ist G jedoch verloren und wird das Rücksetzen von der Bank nicht durch sichere Geräte durchgeführt, so könnte die Bank versuchen, B_G auf zwei Arten zu betrügen: Zum einen könnte die Bank zusätzliche Vermerke über Ausgaben erzeugen, allerdings nur so weit, daß der Kontostand von G nicht negativ wird; zum anderen könnte sie gefundene Vermerke über Einnahmen von G unterschlagen.

Die erste Betrugsart kann man verhindern, indem jedes Gerät G die es betreffenden Vermerke bei der Erzeugung unterschreibt [Denn_82, GoMR_88, PlLe_86]. Dabei muß der Signierschlüssel vom Gerät selbst gewählt sein, der zugehörige Testschlüssel schon bei der Initialisierung von G dem Besitzer B_G und der Bank mitgeteilt werden (durch G, damit klar ist, daß die Mitteilung korrekt ist) und die Bank muß B_G unterschreiben, daß genau die so unterschriebenen Vermerke G zugerechnet werden.

Um die zweite Betrugsart zu verhindern, muß zusätzlich dafür gesorgt werden, daß ein Benutzer B_G eines verlorenen Gerätes G kontrollieren kann, welche sein Gerät betreffenden Vermerke der Bank übergeben wurden. Dann kann B_G zumindest im Prinzip das Ergebnis des Rücksetzens von G „nachrechnen" und so der Bank eine mögliche Unterschlagung nachweisen.

Näherungsweise läßt sich dieses Ziel sehr leicht mit Hilfe des oben zur Erhöhung der Verlusttoleranz genannten Erstellens von „Rücksetzpunkten" auf einem zweiten sicheren Gerät G* erreichen. Hierzu müssen die sicheren Geräte ihre Aufzeichnungen zunächst vertraulich an die Bank überspielen, nach Erhalt einer Quittung aber auch ihrem Besitzer mitteilen. Übergibt nun die Bank B_G die aus ihrer Sicht vollständige Änderungsaufzeichnung über G und fehlt in dieser ein Vermerk, den G* verzeichnete, so ist die Unterschlagung nachgewiesen. Daher stellt zumindest die Unterschlagung älterer Vermerke für die Bank ein zu hohes, zumindest aber unkalkulierbares Risiko dar. Die Nachrechnung des Rücksetzergebnisses geschieht dann anhand der von der Bank erhaltenen Änderungsaufzeichnung für G.

Vollständig läßt sich das Ziel dadurch erreichen, daß jedes Gerät seine Vermerke nicht einfach nur der Bank übergibt, sondern sie veröffentlicht, d.h. an ein „Schwarzes Brett" hängt [PWP_87]. Damit hat B_G bezüglich seines Gerätes G dieselben Voraussetzungen wie die Bank, d.h. es kann das Rücksetzprotokoll für G ausführen und damit das Ergebnis der Bank nachprüfen. Aus Aufwandsgründen (vgl. 4.2.1.3) erscheint diese Möglichkeit jedoch für den allgemeinen Gebrauch als wenig praktikabel. Statt dessen könnte man die Zuverlässigkeit der Bank dadurch erhöhen, daß das Rücksetzprotokoll auf den veröffentlichten Vermerken neben der eigentlichen Bank noch von einer weiteren „Kontrollbank" (oder auch mehreren) ausgeführt wird, so daß beide (alle) Banken gleichermaßen betrügen müßten, um eine Unterschlagung zu verbergen.

4.2.1.2 Notwendigkeit der Systemterminierung

Im Verfahren der maximalen Weitergabe wurde davon ausgegangen, daß mit einem Gerät G auch zugleich alle Geräte, die demselben System wie G angehören, ungültig werden.

Man könnte nun versuchen, den Austausch der ungültig gewordenen Geräte wie in Protokollskizze 3 zu beliebigen Zeiten vorzunehmen, so daß dasselbe System länger als die einzelnen Geräte, möglichst gar beliebig lang, andauern könnte. Dabei sollten natürlich verlorene Geräte vor

dem Systemende rückgesetzt werden können, denn sonst könnte man auch die Gültigkeit der Geräte bis zum Systemende ausdehnen. Im folgenden wird gezeigt, daß dies leider nicht möglich ist.

Definition

Das System, zu dem G gehört, sei dadurch definiert, daß es mit jedem dazugehörenden Gerät G1 auch alle weiteren Geräte G2 enthält, die zu mindestens einem Zeitpunkt eine Transaktion mit G1 ausführen können, und sonst keine (d.h. die Relation „G1 gehört zum selben System wie G2" ist die transitive Hülle der Relation „G1 kann zu mindestens einem Zeitpunkt eine Transaktion mit G2 vornehmen"; oder: die Systeme sind die Zusammenhangskomponenten des Graphen mit den Geräten als Ecken und Kanten zwischen genau den Geräten, die zu mindestens einem Zeitpunkt eine Transaktion miteinander ausführen können).

Rücksetzen eines verlorenen Gerätes G zu einem bestimmten Zeitpunkt beinhalte, daß B_G den Betrag, auf den rückgesetzt wird, endgültig erhält, d.h. daß ihm keine künftige Wegnahme desselben mehr droht (was bei einem anonymen Verfahren auch nicht durchführbar wäre). Für den Beweis ist nicht nötig, daß es auch beinhaltet, daß B_G nach diesem (ersten) Rücksetzen keine weiteren Gutschriften für G mehr erhält, wenngleich in allen von uns explizit beschriebenen Verfahren auch in diesem Sinne nur ein einziger Rücksetzzeitpunkt pro Gerät existiert.

Behauptung

Zum beschriebenen Zahlungs- und Aufzeichnungsverfahren gibt es kein Rücksetzverfahren, bei dem

- bei der Ausgabe irgendeines Gerätes G garantiert werden kann, daß dieses im Verlustfalle rückgesetzt werden kann, bevor alle Geräte des Systems von G ungültig geworden sind, und
- zumindest beim Rücksetzen eines Gerätes G, dessen sämtliche Transaktionspartner nicht verloren sind, alle Transaktionen von G richtig nachvollzogen werden.

Beweis

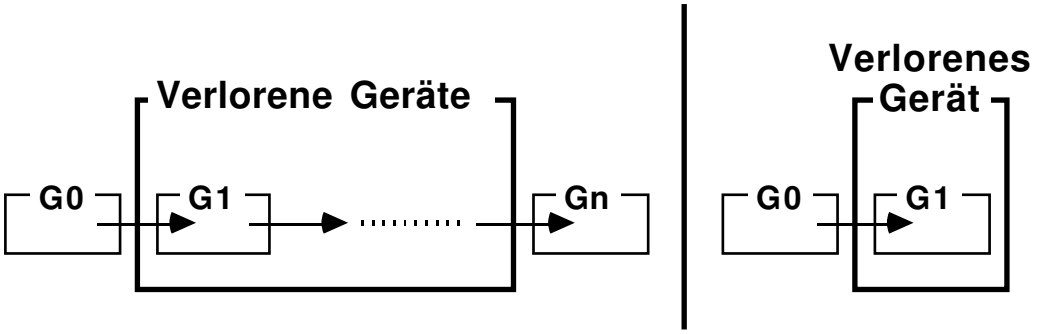
Wir nehmen an, es gäbe ein solches Verfahren und G1 wäre ein Gerät, für das ein Rücksetzzeitpunkt R vor dem Systemende garantiert würde.

G1 kann nun zunächst einen Betrag b von einem Gerät G0 einnehmen, das nicht verloren geht und seine Änderungsaufzeichnung der Bank übermittelt.

Gemäß der Definition eines Systems kann damit eine bis zum Systemende andauernde Folge von Geräten $(Gi)_{i=0,...,n}$ beginnen (vgl. Bild 4), von denen Gi für i=1,...,n-1 nur den Betrag b von G(i-1) einnimmt, an G(i+1) wieder ausgibt und dann verloren geht.

Auch Gn führe keine weitere Transaktion durch, gehe jedoch nicht verloren, sondern übermittle zum Systemende, also insbesondere nach R, seine Aufzeichnung der Bank.

Alle weiteren Geräte seien nicht verloren.



Gi (i=1,...,n-1) nimmt den Betrag b von G(i-1) ein, gibt ihn an G(i+1) wieder aus und geht dann verloren. Gn geht nicht verloren und meldet sich nach dem Rücksetzzeitpunkt von G1 bei der Bank.

G1 nimmt den Betrag ein und geht sofort verloren.

Bild 4 Zwei für die Bank zum Rücksetzzeitpunkt ununterscheidbare Situationen

Um zu bestimmen, wie G1 in dieser Situation rückgesetzt wird, wird zunächst eine zweite Situation konstruiert, die für die Bank bis zum Rücksetzzeitpunkt R einschließlich von der eigentlich vorliegenden nicht zu unterscheiden ist:

Dabei führt G1 zwar die Transaktion mit G0 durch und die Geräte G1 bis G(n-1) gehen verloren, alle weiteren oben genannten Transaktionen finden jedoch nicht statt. Alle Geräte außer G1,...,Gn verhalten sich wie oben. Letzteres ist möglich, da bereits diese anderen Geräte die beiden Situationen nicht unterscheiden können. Insbesondere ist also der Zeitpunkt, zu dem G0 seine Änderungsaufzeichnung der Bank übermittelt, in beiden Situationen gleich.

In dieser zweiten Situation ist kein Transaktionspartner von G1 verloren, so daß die Transaktionen von G1 nachvollzogen werden müssen und G1 der Betrag b gutgeschrieben werden muß (insbesondere muß also das Ungültigwerden von G0 vor R liegen, damit der Vermerk (G1,b,T) bei G0 gefunden wird).

Folglich wird auch in der wirklich vorliegenden Situation G1 der Betrag b gutgeschrieben.

Da Gn nicht verloren ist, kann ihm jedoch derselbe Betrag b am Systemende nicht aberkannt werden, im Widerspruch zur Annahme, daß sich die Geldmenge im System nicht erhöhte.

(Auch das Auffinden der Vermerke über alle dazwischenliegenden Transaktionen bei Gn hilft nichts, unabhängig davon, ob die anderen Gi schon rückgesetzt sind, da bei ihnen, wenn man b abziehen würde, negative Kontostände entstünden.)

4.2.1.3 Aufwand

Da noch mehrere Aufwandsabschätzungen folgen und deren Ergebnisse vergleichbar sein sollen, werden einige Systemparameter bereits allgemeiner als für dieses Verfahren notwendig eingeführt. Da diese Abschätzungen andererseits nicht eine endgültige Festlegung der Leistungsparameter der sicheren Geräte und der Rechner der Bank erlauben, sondern nur zeigen sollen, bei welchen Größenordnungen von Systemen welche Verfahren praktisch einsetzbar sind, beschränken wir uns auf eine stark vergröberte Beschreibung des Benutzerverhaltens:

g sei stets die mittlere Anzahl der Geräte, die sich gleichzeitig im System (s.o.) befinden, einschließlich der verlorenen.

Dies dürfte eine vom verwendeten Verfahren zur verteilten Änderungsaufzeichnung unabhängige Größe sein (wenn sie natürlich auch von der Verwendung weiterer Verlusttoleranzverfahren, etwa zweiter sicherer Geräte zur Erstellung von Rücksetzpunkten, abhängen kann). Wenn jeder Teilnehmer nur ein Gerät gleichzeitig verwendet, so ist es gerade die Teilnehmerzahl.

Speziell hier beim Verfahren der maximalen Weitergabe, bei dem alle Geräte gleichzeitig ungültig werden, ist g zugleich die Gesamtzahl der Geräte eines Systems.

z sei die mittlere Zahlungsrate der Geräte, d.h. die im Mittel mit einem Gerät vorgenommenen Zahlungen pro Zeiteinheit.

Auch z dürfte nicht vom verwendeten Verfahren zur verteilten Änderungsaufzeichnung abhängig sein.

Speziell hier ist es zugleich die Transaktionsrate. (Bei anderen Verfahren werden manche Zahlungen in mehrere Transaktionen aufgespalten.)

p sei die Periodendauer, d.h. die Gültigkeitsdauer der Geräte. Daß manche Geräte kürzer gültig sind, z.B. weil alle Geräte gleichzeitig ungültig werden, der Besitzer sich aber erst mitten im System zur Teilnahme entschließt, wird vernachlässigt.

Speziell hier ist p zugleich die Dauer eines Systems.

v sei die Verlustrate, d.h. die Anzahl der Geräte, die im Mittel pro Zeiteinheit verloren wird, dividiert durch die Gesamtzahl der gerade vorhandenen, nicht verlorenen Geräte. Auch v sollte nicht vom verwendeten Verfahren zur verteilten Änderungsaufzeichnung abhängig sein.

Wir werden im folgenden vernachlässigen, daß die gerade vorhandenen Geräte wegen der bisherigen Verluste meist etwas weniger als g sind und somit einen gleichmäßigen Verlust von g•v Geräten pro Zeiteinheit annehmen (was speziell hier der Approximation 1. Ordnung an die eigentlich exponentielle Abnahme der Geräte ist).

v ist nicht gleich dem Anteil der Geräte, die verloren gehen, da jener von der Gültigkeitsdauer der Geräte abhängt und sich, gemäß der gerade gemachten Annahme, als p•v berechnet.

(Die obige Annahme kann man sich erlauben, da zum einen die Periodendauer nie so gewählt werden sollte, daß ein großer Teil der Geräte verlorengeht, und zum anderen die dadurch eingeführten Ungenauigkeiten nicht größer sind als die wegen der ungenauen Modellierung des Benutzerverhaltens ohnehin vermutlich vorhandenen. Beispielsweise wäre in dem Fall, daß manche Leute jedes Gerät in kürzester Zeit verlieren, während den übrigen, ordentlichen dies nie passiert, der Anteil der Geräte, die verloren gehen, i.allg. doch gleich v.)

Gravierendster Nachteil des Verfahrens ist der sehr hohe Speicherbedarf der Listen L_G.

Die Länge von L_G wächst anfangs exponentiell mit der Anzahl der Transaktionen, die G durchführt, da sie bei jeder Transaktion durch die Liste des Partnergerätes etwa verdoppelt wird. (Dies bedeutet auch, daß für im Vergleich zu g sehr kleines p•z und gleichverteiltes Zahlungsverhalten der maximale Speicheraufwand jedes Gerätes exponentiell in p•z ist.)

Mit zunehmender Dauer wird allerdings die Anzahl der Vermerke zunehmen, die bereits in beiden Listen vorhanden sind und folglich nicht mehr verdoppelt werden müssen.

Die endgültige Speicherkomplexität von L_G ist auch „nur" linear in g•z•p, da im schlimmsten (und für die Verlusttoleranz zugleich besten) Fall ein Gerät Vermerke von sämtlichen stattgefundenen Transaktionen enthält. Dabei wurden, wie auch im folgenden, noch logarithmische Faktoren, die sich durch die Abhängigkeit der Länge der einzelnen Vermerke von der Gesamtzahl der Geräte oder Transaktionen ergeben, vernachlässigt. Die Länge einer einzelnen Aufzeichnung wird dabei zumindest $\log_2(g•z•p)$ sein, da jede ausgeführte Transaktion eindeutig gekennzeichnet sein muß.

Leider sagt die Speicherkomplexität recht wenig aus, da für praktische Belange das asymptotische Verhalten uninteressant ist. Bei g=80000 Teilnehmern mit je einem Gerät, einer Periode p=1 Monat, z=100 Transaktionen/Monat je Teilnehmer und nur 4 byte zu speichernder Information je Vermerk benötigt jedes Gerät für den äußersten Fall bereits einen Speicher von fast 32 Mbyte.

Zur Reduzierung des Speicherbedarfs der einzelnen sicheren Geräte könnte man sicheren Geräten erlauben, einen „erschöpften" Speicher durch anonyme Übergabe der darin befindlichen Änderungsvermerke an die Bank zu leeren. Erschöpft ist ein Speicher dann, wenn er mehr als halbvoll ist, da bei Zulassung mehr als halbvoller Speicher die Gefahr bestünde, daß bei einer Transaktion die Vereinigung der L_G-Listen keinen Platz mehr hat.

Dieses Verfahren ist allerdings bei sehr kleinen Speicherkapazitäten, bei denen beinahe alle Geräte lange vor dem Systemende ihren Speicher erstmals erschöpft haben, wenig sinnvoll: Im Extremfall ist der Speicher eines Gerätes bereits nach zwei Transaktionen wieder erschöpft, wenn es von beiden Transaktionspartnern eine Liste erhält, die ebenfalls bereits fast die Hälfte des Speichers beansprucht. Auch im Mittel würden bei einem absolut gleichmäßigen Transaktionsverhalten die Geräte nur vier Transaktionen zwischen zwei Kommunikationen mit der Bank durchführen können, da stets etwa die Hälfte der Geräte einen gerade geleerten und die andere Hälfte einen durch eine Transaktion mit einem nicht geleerten Gerät wieder fast zur Hälfte gefüllten Speicher hätten.

Zur Vermeidung von Duplikaten in L_G und zur Erleichterung der Rücksetzprozedur der Bank (s.u.) sollte die Liste L_G sortiert sein. Geschieht die Vereinigung zweier Listen L_{G1} und L_{G2} durch Mischen, so erfordert dies einen Zeitaufwand in der Größenordnung g•z•p. Zusätzlicher Speicheraufwand entsteht durch das Mischen nicht, wenn beide Geräte die jeweils vom Partner erhaltenen Vermerke sofort einsortieren und eine sequentielle ringförmige Speicherung verwenden.

Das Rücksetzen selbst wird nach der Terminierung des Systems unter der Annahme eines sequentiellen Ablaufs so durchgeführt, daß die vergleichsweise kurze Liste der Gerätekennzeichen der verlorenen Geräte (Länge p•v•g) vorsortiert wird. Zu jedem davon wird eine Liste der bereits aufgefundenen Aufzeichnungen über dieses Gerät angelegt, in die Duplikate nicht aufgenommen werden, so daß die Länge im Mittel z•p betragen wird. Nun werden die aufgefundenen Aufzeichnungen der Reihe nach mit der Liste der Gerätekennzeichen verglichen und ggf. in die passende Liste gefundener Aufzeichnungen aufgenommen. Letzteres dürfte etwa für einen Anteil p•v/2 der Aufzeichnungen zutreffen, wenn verlorene Geräte etwa halb soviele Transaktionen durchführten wie die anderen. Die Zeitkomplexität ist damit proportional zu

Vorsortieren der verlorenen Geräte		p•v•g • log(p•v•g)
Vergleich der Aufzeichnungen der nicht verlorenen Geräte	+	g•(1-p•v) • g•z•p
… mit der Liste der verlorenen Gerät	•	(log(p•v•g)
… und ggf., mit der Häufigkeit		+ p•v/2
Einfügen in die bereits aufgefundenen Aufzeichnungen über ein verlorenes Gerät		• log(z•p))

d.h. in der Größenordnung

$$\Theta(\ g\bullet(1-p\bullet v)\ \bullet\ g\bullet z\bullet p\ \bullet\ (\log(p\bullet v\bullet g) + p\bullet v/2 \bullet \log(z\bullet p))\ )$$

wobei 1-p•v nahe 1 ist, wenn man annimmt, daß der größere Teil der Geräte nicht verloren ist.

Allerdings kann man hier einiges parallelisieren, insbesondere, wenn die Geräte selbst so konstruiert sind, daß sie den Beginn der Prozedur unterstützen. Beispielsweise könnten sie der Bank gestatten, jeweils zwei zusammenzuschalten, um ihre Listen zu vereinigen, was sie ja auch im

normalen Betrieb können. Dadurch können in log(g) vielen Schritten der Zeitkomplexität $\Theta(g \bullet z \bullet p)$ die Aufzeichnungen zu einer einzigen Liste L, die auch nur die maximale Länge $g \bullet z \bullet p$ haben kann, zusammengefaßt werden. Hiermit ist auch klar, daß, wenn geeignete sichere Geräte für dieses Verfahren gebaut werden können, die Rücksetzprozedur sicherlich auch praktisch durchführbar ist.

4.2.1.4 Verteilte Kontostände

Beachtet man, daß in einer Liste L_{G1} zu jedem Änderungsvermerk über ein Gerät G2 auch alle älteren desselben Gerätes G2 enthalten sind, d.h. L_{G1} sämtliche Transaktionen von G2 bis zu einem bestimmten Zeitpunkt verzeichnet, liegt ein einfacher Weg nahe, die Speicherkomplexität erheblich zu senken: Statt der einzelnen Kontostandsänderungen sollte L_{G1} nur den sich daraus ergebenden Kontostand K_{G2} enthalten.

Beim Zusammenfügen zweier Listen muß erkennbar sein, welcher von zwei Kontoständen für ein Gerät der aktuellere ist. Dazu wird jedem Kontostand K_{G2} ein Zähler beigefügt, der als Transaktionskennzeichen der letzten darin aufgenommenen Transaktion von G2 aufgefaßt werden kann, so daß die Einträge die Form $(G2, K_{G2}, T_{G2})$ haben. Rückgesetzt wird ein verlorenes Gerät natürlich auf den neuesten für es gefundenen Kontostand.

Die Sicherheit dieses Verfahrens der verteilten Kontostände ergibt sich unmittelbar aus der Sicherheit des normalen Verfahrens der maximalen Weitergabe: unabhängig davon, welches der beiden Verfahren man wählt, wird ein verlorenes Gerät G2 auf denselben Kontostand rückgesetzt.

Dies ist leicht einzusehen: Ist $(G2,b,T_{G2})$ der neueste Vermerk über eine Transaktion von G2, die beim Verfahren der maximalen Weitergabe gefunden wird, so werden damit in derselben Liste L_{G1} auch alle vorangegangenen Transaktionen von G2 entdeckt, so daß auf denselben Kontostand K_{G2} rückgesetzt wird, den G1 im Verfahren der verteilten Kontostände für G2 verzeichnen würde und der dann auch der neueste über G2 gefundene Kontostand wäre.

Damit folgt auch, daß das Verfahren der verteilten Kontostände wie das der maximalen Weitergabe die maximal mögliche Verlusttoleranz realisiert.

Für die Sicherheit der Teilnehmer vor Betrugsversuchen der Bank gilt dasselbe wie für die maximale Weitergabe. Die Bank kann Teilnehmer, deren Geräte nicht verloren sind, nicht betrügen. Ist G jedoch verloren und wird das Rücksetzen von der Bank nicht durch sichere Geräte durchgeführt, so könnte die Bank versuchen, B_G auf zwei Arten zu betrügen: Zum einen könnte die Bank einen „neuesten" Kontostand für G erfinden, zum anderen könnte sie einen beliebigen gefundenen Kontostand als den neuesten ausgeben.

Die Verhinderung bzw. Begrenzung beider Betrugsarten erfolgt genau wie in 4.2.1.1 für die maximale Weitergabe beschrieben.

Wie schon im Verfahren der maximalen Weitergabe, so muß auch hier das gesamte Zahlungssystem terminieren, bevor ein verlorenes Gerät zurückgesetzt werden kann. Der Beweis dieser Behauptung erfolgt wie in 4.2.1.2.

Die Speicherkomplexität des Verfahrens ist linear in g. Für das Beispiel in 4.2.1.3 reduziert sich der Speicherbedarf von 32 MByte auf 320 KByte je Gerät.

Die Rücksetzprozedur selbst wird natürlich ebenfalls einfacher, da weniger Vermerke zu betrachten sind und zu jedem verlorenen Gerät auch nur der neueste aufgefundene Kontostand gespeichert werden muß. Ihre Zeitkomplexität beträgt, wenn man wieder annimmt, daß der größere Teil der Geräte nicht verloren ist, nur noch

$$\Theta(g \bullet g \bullet \log(p \bullet v \bullet g)),$$

Wenn man, wie oben, die Geräte ihre Listen selbst mischen läßt, so reduziert sich die Zeitkomplexität auf

$$\Theta(\log(g) \bullet g + g \bullet \log(p \bullet v \bullet g))$$

und es ist wieder klar, daß der Engpaß nicht bei der Rücksetzprozedur liegen kann.

4.2.2 Überdeckungsverfahren

Der Hauptnachteil des in 4.2.1.1 beschriebenen Verfahrens der maximalen Weitergabe war dessen enormer Speicherbedarf für jedes einzelne Gerät. Mit den verteilten Kontoständen (vgl. 4.2.1.4) wurde ein Verfahren vorgestellt, das unter Beibehaltung der maximalen Verlusttoleranz diesen Nachteil stark reduzierte.

Im Rest dieses Kapitels 4.2 soll nun versucht werden, unter Beibehaltung des Prinzips, Transaktionen wie beim ursprünglichen Verfahren der maximalen Weitergabe in der Form (G,b,T_G) aufzuzeichnen und weiterzugeben, den Speicherbedarf zu verringern (falls möglich, noch unter den der verteilten Kontostände und in die Größenordnung dessen der unsicheren einfachen Aufzeichnung).

Hierzu muß die Verteilung der Vermerke über Transaktionen eingeschränkt werden, so daß sich in jedem Fall auch die Menge der ohne Rücksetzabweichung tolerierbaren Verluste verringern wird. Dies ist jedoch akzeptabel, solange unter allen Umständen die Geldmenge im System nicht zunimmt und keine negativen Kontostände auftreten. Zudem wird man verlangen, daß zumindest weiterhin all diejenigen Verluste toleriert werden können, die das (unsichere) Verfahren der einfachen Aufzeichnung (vgl. 4.1) toleriert, d.h. überlebt genau ein Partner einer Transaktion, so soll diese auch für den verlorenen Partner nachvollzogen werden können.

Eine Lösung dieser Aufgabe erhält man in natürlicher Weise, wenn man betrachtet, wie beim Verfahren der maximalen Weitergabe die Sicherheit garantiert wurde, und die Weitergabe nur derjenigen Änderungsvermerke vorschreibt, die zu diesem Zweck benötigt wurden.

4.2.2.1 Protokoll, Sicherheit und Verlusttoleranz

Zahlt ein Gerät G einen Betrag b, so muß dieser Betrag durch eine frühere Einnahme „gedeckt" sein. Geht nun G irgendwann verloren und wird der Änderungsvermerk über diese Zahlung, etwa (G,b,T_G) mit $b<0$, gefunden, so muß zur Wahrung der Sicherheit des Zahlungssystems die Deckung der Zahlung den gesamten über G gefundenen Vermerken zu entnehmen sein.

Um diese Eigenschaft bei eingeschränkter Weitergabe zu garantieren, ist es naheliegend, zu jeder Zahlung (G,b,T_G) von G zugleich auch soviele Vermerke über frühere Einnahmen von G an den Partner weiterzugeben, daß die Zahlung durch diese gedeckt wird. Dabei darf dieselbe Einnahme natürlich höchstens zum Überdecken sovieler Ausgaben verwendet werden, wie es ihrem Wert entspricht. Die Zuordnung von Einnahmen zu durch sie zu deckenden Ausgaben soll im folgenden Überdeckung genannt werden. Etwas konkreter sei definiert:

Definition

Eine Funktion μ, die

- jedem Vermerk (G,b,T_G) über eine Ausgabe eines Gerätes G (also $b<0$) eine Menge $\mu(G,b,T_G)$ von Änderungsvermerken früherer Einnahmen von G zuordnet, und

- jedem Vermerk über eine Einnahme die leere Menge zuordnet,

werde Überdeckung genannt, falls für jede Menge von Vermerken über Transaktionen von G, die mit (G,b',T'_G) auch $\mu(G,b',T'_G)$ enthält (d.h. die gegen μ abgeschlossen ist), die Summe der Beträge b aller Vermerke größer oder gleich Null ist.

Insbesondere folgt dann, daß für jede Ausgabe die Menge $\{ (G,b,T_G) \} \cup \mu(G,b,T_G)$ eine nichtnegative Summe ergibt, d.h. daß durch die Einnahmen in $\mu(G,b,T_G)$ die Ausgabe (G,b,T_G) gedeckt wird.

Eine besonders einfache Überdeckung erhält man, indem jeder Ausgabe von G die Menge aller bisherigen Einnahmen von G zugeordnet wird. Die Überdeckungseigenschaft ist trivialerweise erfüllt: jede gegen diese Überdeckung abgeschlossene Menge M von Vermerken über G ergibt als Summe einen Wert größer oder gleich dem Kontostand von G zum Zeitpunkt nach der Ausführung der aktuellsten in M vermerkten Ausgabe.

Dies ist die gröbste mögliche Überdeckung, denn offensichtlich enthält die Überdeckung von (G,b,T_G) zugleich alle anderen für (G,b,T_G) möglichen Überdeckungen.

In diesem Sinne feinste Überdeckungen (also solche, in denen man keinen Vermerk aus $\mu(G,b,T_G)$ entfernen könnte, ohne die Überdeckungseigenschaft zu verlieren), erhält man wie folgt (vgl. Bild 5):

> Zu jeder Einnahme merkt sich G, ob diese schon „verbraucht" ist.
>
> Jede Ausgabe der Höhe b' wird durch noch unverbrauchte Einnahmen gedeckt, wobei im allgemeinen am Ende ein Teilbetrag von b' übrigbleiben wird, der kleiner ist als jede noch unverbrauchte Einnahme. Um diesen zu überdecken, wählt sich G eine weitere, zu große Einnahme, die, soweit zur Überdeckung nötig, teilweise verbraucht wird.
>
> Dabei muß sich G stets nur eine einzige Einnahme als teilweise verbraucht merken (was sich für den zusätzlichen Speicherbedarf positiv bemerkbar machen wird), wenn eine teilweise verbrauchte Einnahme stets zu Ende verbraucht wird, bevor eine neue geteilt wird.

Daß auf diese Weise eine Überdeckung konstruiert wird, ist offensichtlich; ebenso, daß keine Einnahme aus der Überdeckung einer Ausgabe gestrichen werden kann (denn sonst würde ja bereits die Ausgabe vereinigt mit ihrer Überdeckung die Überdeckungseigenschaft verletzen).

Auf diese Weise erhält man natürlich nicht alle feinsten Überdeckungen, sondern nur eine Klasse von besonders leicht schrittweise konstruier- und linear darstellbaren.

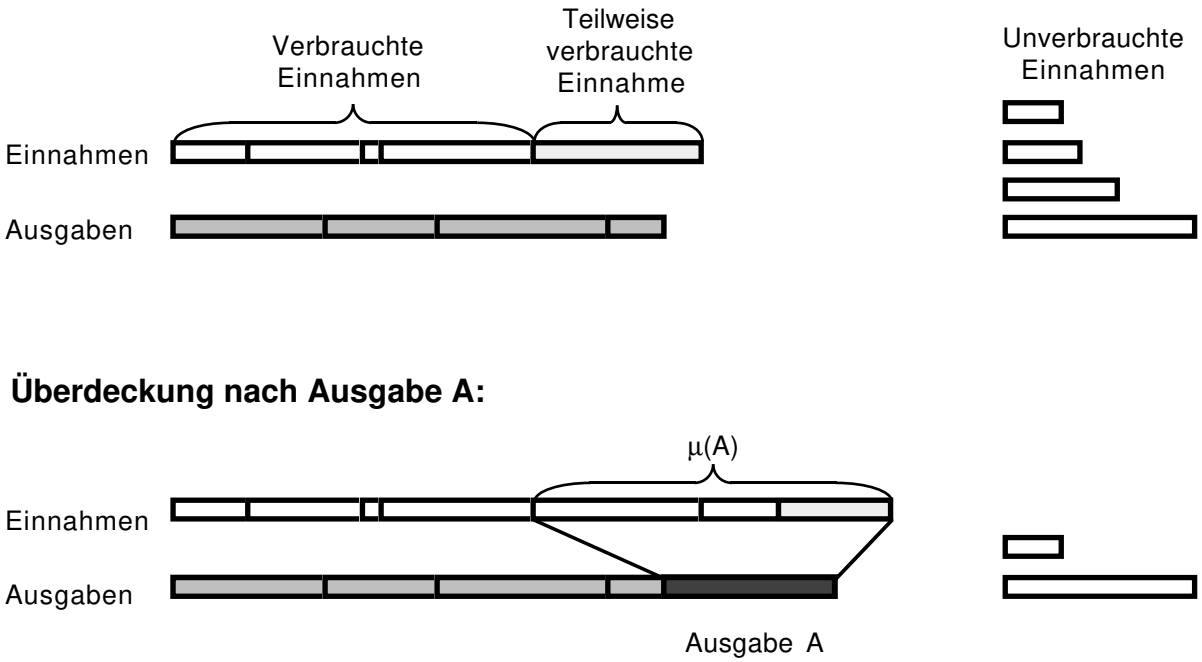


Bild 5 Konstruktion einer feinsten linearisierbaren Überdeckung

Die durch die folgende Protokollskizze 5 definierten Überdeckungsverfahren sind nun dadurch gekennzeichnet, daß jedes Gerät selbst eine feste Überdeckung μ wählt (wobei das Wählen schrittweise für jede neue Ausgabe erfolgt) und alle übrigen Geräte mit jedem Änderungsvermerk auch dessen Überdeckung und den Änderungsvermerk des Partnergerätes über dieselbe Transaktion weitergeben. Diese Zusammenhänge zwischen verschiedenen Änderungsvermerken bestimmen sie dabei nicht bei jeder Weitergabe selbst, sondern sie lassen (in Schritt [4.2]) einfach Mengen von Änderungsvermerken, die sie (in Schritt [4.4]) zusammen erhalten haben, beieinander.

Die Schritte [4.5] und [4.6] dienen lediglich der Verbesserung der Verlusttoleranz; für speicherplatzoptimierte Verfahren können sie entfallen (bzw. V_G und damit O_G als leere Menge gewählt werden).

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 für es eindeutig kennzeichnet.

[4.2] Zusätzlich bestimmt G1 die Überdeckung $\mu(G1,b,T_{G1})$ und damit die Menge M_{G1} der an G2 zu übergebenden Änderungsvermerke als kleinste Menge, für die gilt:

- $M_{G1} \supseteq \{ (G1,b,T_{G1}) \} \cup \mu(G1,b,T_{G1})$
- Ist $(G1,b',T'_{G1}) \in \mu(G1,b,T_{G1})$ und ist M^* die Menge der Vermerke, die G1 während der Ausführung der so bezeichneten Transaktion in Schritt [4.4] erhielt, so gilt $M_{G1} \supseteq M^*$.

Entsprechend verfährt G2 und bestimmt die Menge M_{G2}. Beide tauschen die soeben bestimmten Mengen aus.

[4.3] Zur Sicherung der Unteilbarkeit der Zahlung sendet eines der beiden Geräte eine Quittung (vgl. Schritt [4] in Protokollskizze 1).

[4.4] G1 fügt die Menge M_{G2} in seine Liste L_{G1} unter Wahrung einer Standardreihenfolge ein und merkt sich die Zuordnung von $(G1,b,T_{G1})$ zu M_{G2}.
Entsprechend verfährt G2 mit M_{G1}.

[4.5] G1 wählt sich eine beliebige (evtl. auch leere) Teilmenge V_{G1} von Vermerken über seine früheren Transaktionen und bildet daraus die Menge N_{G1} als kleinste Menge, für die gilt:
- $N_{G1} \supseteq V_{G1}$
- Ist $(G1,b',T'_{G1}) \in N_{G1}$ ein von $(G1,b,T_{G1})$ verschiedener Vermerk und ist M^* die Vereinigungsmenge der Vermerke, die G1 während der Ausführung der so bezeichneten Transaktion in Schritt [4.4] erhielt oder weitergab, so gilt $N_{G1} \supseteq M^*$.

G_1 wählt sich sodann eine Menge O_{G1} als Vereinigung von N_{G1} und beliebigen in einem früheren Schritt [4.5] erhaltenen O_G-Mengen.
Entsprechend verfährt G2 und wählt eine Menge O_{G2}. Beide tauschen die soeben bestimmten Mengen aus.

[4.6] G1 (bzw. G2) fügt die Menge O_{G2} (bzw. O_{G1}) in seine Liste L_{G1} (bzw. L_{G2}) unter Wahrung einer Standardreihenfolge ein.

Ungültigwerden und Rücksetzen der sicheren Geräte

Wie in Protokollskizze 4.

Protokollskizze 5 Verteilte Aufzeichnung: Klasse der Überdeckungsverfahren zur Überdeckung μ

Jedes Überdeckungsverfahren zur Überdeckung μ ist sicher, d.h.:

- Durch Rücksetzen wird kein Kontostand K_G auf einen negativen Wert gesetzt.

  Grund hierfür ist, daß die Menge der gefundenen Änderungsvermerke für jedes verlorene Gerät gegen μ abgeschlossen ist und damit nach Definition der Überdeckung zu einem nicht-negativen Kontostand führt.

  Die Abgeschlossenheit gegenüber μ ergibt sich wie folgt:

  a) Die Vereinigung von gegen μ abgeschlossenen Mengen ist trivialerweise wieder gegen μ abgeschlossen.

  b) Gemäß Schritt [4.2] ist M_{G1} gegen μ abgeschlossen:

     Für $(G1,b,T_{G1})$ ist dies in [4.2] explizit gefordert. Für die erste Transaktion jedes Gerätes ist damit alles gezeigt.

     Sei nun $(G3,b',T'_{G3})$ ein von $(G1,b,T_{G1})$ verschiedener Vermerk aus M_{G1}. Dann muß es einen Vermerk $(G1,b'',T''_{G1})$ in L_{G1} geben, so daß in Schritt [4.2] M^* aufgrund von $(G1,b'',T''_{G1})$ konstruiert wurde und $(G3,b',T'_{G3})$ enthielt. Da M^* gerade von der Art M_G ist, folgt induktiv die Behauptung.

  c) Gemäß Schritt [4.5] sind N_G und O_G gegen μ abgeschlossen:

Dies folgt aus a) und b), da jedes N_G die Vereinigung von Mengen der Art M_G und jedes O_G die Vereinigung einer Menge N_G und früherer O_G ist.

d) Jede Liste L_G von Änderungsvermerken, die ein Gerät G enthält, ist gegen μ abgeschlossen und damit auch jede Menge von Änderungsvermerken, die die Bank zum Rücksetzen erhält:

Grund hierfür ist, daß sich L_G durch Vereinigung von Mengen der Art M_G und O_G ergibt, die nach b) und c) gegen μ angeschlossen sind, so daß gemäß a) auch L_G gegen μ abgeschlossen ist. Da die Bank wiederum eine Vereinigung von Mengen L_G erhält, folgt die letzte Behauptung.

- Durch Rücksetzen ändert sich die Summe aller Kontostände nicht:

Grund hierfür ist, daß die Menge der gefundenen Änderungsvermerke für jedes verlorene Gerät mit jedem Änderungsvermerk auch den entsprechenden Vermerk des Partners enthält, so daß sich alle Änderungen wie im Verfahren der maximalen Weitergabe gegenseitig aufheben.

Die behauptete Eigenschaft ergibt sich wie folgt:

a) Gemäß Schritt [4] besitzt die Menge $M_{G1} \cup \{ (G2,–b,T_{G2}) \}$ die Eigenschaft:

Dies gilt sicher für das Paar $(G1,b,T_{G1})$ und $(G2,–b,T_{G2})$. Für die erste Transaktion jedes Gerätes ist damit alles gezeigt. Für die übrigen folgt es induktiv:

$M_{G1} \cup \{ (G2,–b,T_{G2}) \}$ ist die Vereinigung von $\{ (G1,b,T_{G1}),(G2,–b,T_{G2}) \}$ und Mengen der Art $M^* \cup \{ (G1,b",T"_{G1}) \}$, die allesamt die Eigenschaft besitzen.

b) Damit besitzt bei jeder Transaktion die Menge $M_{G1} \cup M_{G2}$ die Eigenschaft, denn

$$M_{G1} \cup M_{G2} = M_{G1} \cup \{ (G2,–b,T_{G2}) \} \cup M_{G2} \cup \{ (G1,b,T_{G1}) \}$$

c) Gemäß Schritt [4.4] besitzt jede Menge N_{G1} und O_{G1} die Eigenschaft, denn jede Menge N_{G1} ist gerade die Vereinigung von Mengen der Art $M_{G1} \cup M_{G2}$, für die nach b) die Eigenschaft gilt, und jede Menge O_{G1} die Vereinigung von N_{G1} mit früher erhaltenen O_G-Mengen.

d) Jede Liste L_G von Änderungsvermerken, die ein Gerät G enthält, und damit auch jede Menge von Änderungsvermerken, die die Bank zum Rücksetzen erhält, besitzt die Eigenschaft.

Jedes Überdeckungsverfahren garantiert zumindest die Verlusttoleranz der einfachen (unsicheren) Aufzeichnung: eine Transaktion kann nachvollzogen werden, wenn einer der daran beteiligten Partner nicht verloren ist. Eine obere Schranke für die Rücksetzabweichung kann genausowenig wie bei der maximalen Weitergabe garantiert werden, aber wie dort kann sich ein Benutzer durch das gelegentliche Erstellen von „Rücksetzpunkten" in Form von Überweisungen an ein anderes eigenes Gerät schützen, wobei wieder der Betrag sofort zurücküberwiesen werden kann. Allerdings muß diesmal, um die gesamte Vorgeschichte zu dokumentieren, i.allg. das gesamte derzeitige Guthaben des Gerätes hin und zurück überwiesen werden.

Darüber hinausgehende Verlusttoleranzeigenschaften hängen sehr stark von der gewählten Überdeckung und der Verwendung der O_G–Mengen ab:

- Für maximale O_G–Mengen (d.h. man wählt für V_G jeweils die Menge aller Vermerke über bisherige Transaktionen von G und fügt alle früher erhaltenen O_G–Mengen hinzu) und beliebige Überdeckungen erhält man das Verfahren der maximalen Weitergabe und damit zugleich die maximale Verlusttoleranz.
- Für leere O_G–Mengen und minimale Überdeckungen durch Standardwerte (vgl. Abschnitt 4.2.3) erreicht man gerade soviel Verlusttoleranz, daß das Verfahren die einfache Aufzeichnung enthält, aber im Gegensatz zu dieser sicher ist.

Betrugsversuche der Bank an Besitzern verlorener Geräte sind in gleicher Weise zu behandeln wie in 4.2.1.1.

Auch hinsichtlich der Systemterminierung gilt für Überdeckungsverfahren das bereits in 4.2.1.2 für das Verfahren der maximalen Weitergabe Gesagte; sie ist für „vernünftige" Rücksetzprozeduren unabdingbar. Der Beweis dieser Behauptung erfolgt wörtlich wie in 4.2.1.2, da sich in dem dort konstruierten Beispiel alle Überdeckungsverfahren im wesentlichen gleich verhalten.

4.2.2.2 Aufwand

Der Aufwand der Überdeckungsverfahren hängt von der gewählten Überdeckung und, vor allem bei den einfachen, linearisierbaren Überdeckungen, stark vom Benutzerverhalten ab. Folglich sind viele der im folgenden gemachten Aussagen entweder Betrachtungen des besten oder schlimmsten Falles, die das zu erwartende Systemverhalten nicht sehr eng eingrenzen, oder mit einer gewissen Vorsicht zu behandelnde Plausibilitätsbetrachtungen.

Kennzeichnend für die Ineffizienz des Verfahrens der maximalen Weitergabe war das anfänglich exponentielle Wachstum der von den Geräten ausgetauschten Mengen (vgl. 4.2.1.3). Analog zu den dortigen Überlegungen läßt sich auch das anfängliche Wachstum für Überdeckungsverfahren bestimmen.

Hierzu stelle man sich vor, eine Ausgabe werde durch ü Einnahmen überdeckt, deren zugehörende M_G–Mengen die durchschnittliche Größe m haben. Wieder unter Vernachlässigung von Duplikaten hat die neue M_G–Menge eine Größe von $(ü \bullet m + 1)$. Ist stets $ü > 1$, so liegt also auch hier anfänglich exponentielles Wachstum der M_G–Mengen und damit des gesamten Speicherbedarfs vor, allerdings nicht direkt mit der Anzahl der bisherigen Zahlungen als Exponenten, sondern mit der Anzahl der Weitergaben eines Vermerkes.

Auf die genaue Geschwindigkeit dieses exponentiellen Wachstums hat man durch die Wahl der Überdeckung einen gewissen Einfluß, wobei eine Verkleinerung von ü nicht nur die Basis, sondern auch den Exponenten verkleinert, da bei kleineren Überdeckungen die einzelnen Vermerke seltener weitergegeben werden. Der Wert von ü für eine Ausgabe ist für die maximale Überdeckung stets die Anzahl der bis dahin erhaltenen Einnahmen. Durch geschicktere Wahl von μ kann dieser Wert deutlich verkleinert werden; haben alle Einnahmen und Ausgaben in etwa dieselbe Größe, so ist ü im Durchschnitt zwischen 1 und 2.

Für linearisierbare Überdeckungen läßt sich dies leicht zeigen (wobei $ü \geq 1$ sowieso klar ist): Man denke sich, wie in Bild 5, alle e_G Einnahmen und a_G Ausgaben eines Gerätes G auf zwei Werteachsen so eingetragen, daß die Überdeckung einer bestimmten Ausgabe gerade von den an mehr als einem Punkt über ihr liegenden Einnahmen gebildet wird. Dann beginnt genau an jedem Anfangspunkt einer Einnahme oder Ausgabe ein neues Paar (E,A) von einer Einnahme E und einer Ausgabe A mit $E \in \mu(A)$. Insgesamt gibt es also $a_G+e_G-x_G$ solcher Paare, wobei x_G die Anzahl derjenigen Anfangspunkte ist, die (bei diesem μ) einer Einnahme und einer Ausgabe gemeinsam sind. Dabei ist $x_G \geq 1$ wegen des Nullpunktes und $x_G \leq \min\{a_G,e_G\}$. $a_G+e_G-x_G$ ist also die Summe der ü für dieses Gerät. Der Durchschnitt aller ü ist daher $\sum(a_G+e_G-x_G) / \sum a_G$. Da es insgesamt gleich viele Einnahmen und Ausgaben gibt, folgt die Behauptung.

Eine Betrachtung der O_G–Mengen ist zur Abschätzung des Speicheraufwandes nicht notwendig, da ein Gerät erhaltene O_G–Mengen jederzeit ohne Sicherheitseinbußen löschen kann. Man kann eine O_G–Menge als sinnvollen Inhalt eines zur Zeit ungebrauchten Speicherbereiches betrachten.

Hat man also ein geringeres Wachstum der M_G–Mengen und damit des gesamten Speicheraufwandes erreicht, so ist hier die für die maximale Weitergabe unpraktikable Methode, einem Gerät das gelegentliche Leeren seines Speichers bei der Bank zu erlauben, sinnvoll einsetzbar.

Über diese eher qualitativen Aussagen hinaus lassen sich für den allgemeinen Fall nur noch untere und obere Grenzen für den Aufwand zur Speicherung von Vermerken angeben: Da die Klasse der Überdeckungsverfahren das Verfahren der maximalen Weitergabe enthält, das die maximal mögliche Anzahl von Vermerken aufzeichnet, bildet dessen Speicherbedarf von g•z•p Vermerken zugleich eine allgemeine, obere Grenze für die Anzahl der in einem Gerät zu speichernden Vermerke.

Diese Grenze ist scharf, wie man an folgendem Beispiel sieht: Man fasse das gesamte im System umlaufende Geld zu einem Betrag b zusammen, der p•z mal vom ersten Gerät ausgehend alle Geräte einmal durchläuft und vom letzten wieder an das erste Gerät überwiesen wird. Da der umlaufende Betrag stets nur eine Überdeckung zuläßt, verhalten sich alle Verfahren gleich und sämtliche p•z•g Transaktionen müssen im letzten Gerät gespeichert werden. Dies wird auch nicht wesentlich geändert, wenn man den maximalen Besitz der Geräte beschränkt, z.B. auf das Doppelte des mittleren Besitzes, also 2•b/g. Dann kann man den Betrag b-1 auf g/2 Geräte verteilen und wie im vorigen Beispiel den Betrag 1 die andere Hälfte der Geräte durchwandern lassen. Dadurch müßten im letzten dieser Geräte p•z•g/2 Transaktionen gespeichert werden.

Neben dem Aufwand zur Abspeicherung der Vermerke entsteht bei Überdeckungsverfahren jedoch i.allg. noch der Aufwand zur Speicherung der Zuordnung von Vermerken zu erhaltenen M_G–Mengen und ggf. zu Überdeckungen eigener Zahlungen.

Die Speicherung der Zuordnung von M_G–Mengen zu Einnahmen, also einer zweistelligen Relation zwischen maximal g•z•p und p•z Elementen, läßt sich mit dem maximalen Speicheraufwand $(p•z)^2 • g$ als vollständige Binärmatrix darstellen. Abhängig von der Wahl der Überdeckungen sind auch hier die für dünn belegte Matrizen üblichen Einsparungen anwendbar, wobei allerdings zu beachten ist, daß Zeiger auf Vermerke bzw. Einnahmen bereits einen Aufwand der Größenordnung log(p•z•g) bzw. log(p•z) verursachen.

Dies bedeutet, daß ein Überdeckungsverfahren im schlimmsten Fall mehr Speicheraufwand verursachen kann als das der maximalen Weitergabe.

Der Speicheraufwand zur Herstellung einer Überdeckung ist maximal $\Theta((p•z)^2)$, also gegenüber den anderen Faktoren zu vernachlässigen. Beschränkt man sich auf bestimmte Überdeckungen, so ist er noch geringer, z.B. ist für maximale Überdeckungen überhaupt kein zusätzlicher Speicherplatz notwendig; für linearisierbare Überdeckungen lediglich ein Zeiger auf den Anfang des Stapels der unverbrauchten Einnahmen und einer auf die teilweise verbrauchte Einnahme.

Die Zeitkomplexität einer Transaktion setzt sich für Überdeckungsverfahren im wesentlichen aus drei Teilen zusammen:

- der Berechnung der Überdeckung μ,
- der Berechnung der Menge M_G (und ggf. O_G) und
- dem Einsortieren der vom Partner erhaltenen Mengen in die eigene Änderungsaufzeichnung unter gleichzeitigem Aufbau der notwendigen Verzeigerungen u.ä.

Letzteres ist wiederum linear in p•z•g.

Der Aufwand zur Berechnung der Menge M_G hängt stark von der gewählten Speicherung der Zuordnungsmatrix ab. Wird zu jedem gespeicherten Vermerk eine Bitleiste gespeichert, die jeder eigenen Transaktion ein Bit zuordnet, so ist der Zeitaufwand proportional zur Anzahl aller gespeicherten Vermerke mal der Größe der Überdeckung. Wird die Matrix umgekehrt als Liste von

Paaren (eigene Transaktion, dabei erhaltene M_G–Menge) abgespeichert, so ist der Aufwand zwar nur proportional zur Größe von M_G mal der Größe der Überdeckung, dafür ist aber der Speicheraufwand vermutlich viel höher.

Die Komplexität der Berechnung von μ läßt sich allgemein nicht angeben. Für maximale Überdeckungen ist überhaupt nichts zu tun; für linearisierbare Überdeckungen sind lediglich die unverbrauchten Einnahmen nach passenden Teilen abzusuchen, was bei geeigneter Sortierung der Einnahmen nach Größe des Betrages in $\log(p \bullet z)$ geht. Sollen optimale Überdeckungen erzeugt werden (also solche, die beim erwarteten Systemverhalten minimalen Speicherplatz benötigen), so dürfte das Problem nicht in in $p \bullet z$ polynomialer Zeit zu lösen sein, genauer gilt:

Behauptung

Das Problem, eine Überdeckung μ zu konstruieren, die für die letzte Zahlung unter allen möglichen Überdeckungen diejenige auswählt, die die kleinste M_G–Menge erzeugt und die in dieser Situation damit optimal ist, ist NP-hart.

Damit ist auch das allgemeinere Problem, eine stets optimale Überdeckung zu konstruieren, NP-hart.

Beweis

Das obige Problem läßt sich wie folgt beschreiben: man hat n ($=p \bullet z$) Werte $b_1, \ldots, b_n$, die noch unverbrauchten Teile der Einnahmen des zahlenden Gerätes, mit zugehörigen M_G–Mengen $M_1,...,M_n$ und den zu zahlenden Betrag b mit $b \le \sum b_i$. Ein optimales μ würde dann n Werte $\alpha_i \in \{0,1\}$ liefern, so daß gilt

a) $\sum \alpha_i \bullet b_i \ge b$

b) $\left| \bigcup_{\alpha_i=1} M_i \right|$ ist minimal

Angenommen, man hätte einen Algorithmus zur Konstruktion solcher optimaler Überdeckungen μ. Dieser muß auch dann eine optimale Lösung finden, wenn alle M_i disjunkt sind und M_i gerade die Kardinalität b_i hat, d.h. er bestimmt Werte $\alpha_i \in \{0,1\}$, so daß gilt

a) $\sum \alpha_i \bullet b_i \ge b$

b) $\sum \alpha_i \bullet b_i$ ist minimal

Auf dieses Teilproblem läßt sich nun das NP-vollständige Teilmengensummen-Problem (Subset Sum, [GaJo_79 Seite 223, SP13]) polynomial reduzieren, das darin besteht, zu entscheiden, ob Werte $\alpha_i \in \{0,1\}$ existieren, so daß für eine vorgegebene, aber beliebige Konstante b gilt

c) $\sum \alpha_i \bullet b_i = b$

Die Reduktion besteht einfach darin, durch μ das durch (a) und (b) beschriebene Problem zu lösen und nachzusehen, ob für die so bestimmten Werte α_i die Gleichung (c) erfüllt ist.

Damit folgt, daß das obige Problem NP-hart ist.

Die Zeitkomplexität der Rücksetzprozedur der Bank ist identisch mit der der Rücksetzprozedur zum Verfahren der maximalen Weitergabe, wobei allerdings die Länge der Listen L_G je nach Überdeckung im Mittel erheblich geringer sein wird als $g \bullet z \bullet p$.

4.2.3 Minimale Überdeckungen durch Standardwerte

Zu Beginn von 4.2.2.2 wurde begründet, daß die Speicherkomplexität eines Überdeckungsverfahrens wesentlich von ü, der Anzahl der Einnahmen in der Überdeckung einer Ausgabe, abhängt. Dieser Wert wird minimal, wenn jede Ausgabe durch genau eine Eingabe gedeckt wird.

Diesen Idealzustand kann man durch eine entsprechende Änderung des Zahlungsprotokolls erzwingen, indem die Beträge der Transaktionen auf einige wenige Standardwerte begrenzt werden und ein Zerteilen oder Zusammenfassen von Werten nicht erlaubt wird. Hierdurch erhöht sich natürlich die Anzahl der Transaktionen eines Gerätes im Mittel um einen Faktor, der im folgenden stets f genannt werden soll, auf p•z•f.

Nimmt man z.B. 20 Standardwerte der Höhe 1, 2, …, 2^{19} und nimmt an, daß jeder Betrag zwischen 1 und $2^{20}-1$ (≈1 000 000) gleich wahrscheinlich ist, so ist f=10. Bei etwas realistischeren Verteilungen, die kleineren Werten und runden Beträgen höhere Wahrscheinlichkeiten zuweisen, ist sogar f<10.

Betrachtet man nun eine beliebige Zahlung und die dabei übergebene M_G–Menge, so sieht man, daß die enthaltenen Vermerke zeitlich geordnet gerade angeben, wie ein anfangs von der Bank an ein Gerät G0 ausgegebener Betrag von Gerät zu Gerät weitergegeben wurde. Dies legt es nahe, diesen Betrag als einen Standardwert im Sinne einer „Banknote" zu betrachten und ihn mit dem von der Bank erzeugten Änderungsvermerk, der die Ausgabe des Standardwertes an G0 dokumentiert, zu benennen. Dieser Vermerk werde im folgenden die Notennummer N des Standardwertes genannt.

Für die Verwendung von Standardwerten läßt sich nun auch etwas über den mittleren Speicheraufwand pro Gerät sagen:

Ein Gerät benötigt im Mittel Speicherplatz für etwa

$$p•z•f • d$$

Vermerke, wobei d die mittlere Anzahl der bei einer Transaktion hinzukommenden Vermerke ist. Dabei werden sowohl die Ausgabe eines Standardwertes durch die Bank als auch das Abliefern bei ihr als Transaktion gezählt (eine andere Behandlung würde nichts wesentliches ändern).

Sei B die Zufallsvariable, die zu jedem Standardwert N die Gesamtzahl seiner Besitzer (gemäß Vielfachheit, aber ohne die Bank) angibt, also B(N)+1 = Anzahl der Weitergaben von N. Der i-te Besitzer speichert über N die Vermerke von der Ausgabe der Bank bis zur Einahme seines Nachbesitzers, also 2•i+2. Somit werden über N in den Geräten insgesamt

$$\sum_{i=1}^{B(N)} (2•i+2) \;=\; B(N)^2 + 3•B(N)$$

Vermerke gespeichert, vorausgesetzt, kein Gerät erhält N zweimal. Letzteres dürfte meist gelten, da g im Vergleich zu B(N) groß sein wird.

Nun ist d der Quotient aus der Gesamtzahl der entstehenden Vermerke und der Anzahl der Transaktionen der Geräte. Also gilt, wenn E den Erwartungswert und V die Varianz bezeichnet,

$$d \;=\; \frac{\sum_{N} \left(B(N)^2 + 3•B(N) \right)}{\sum_{N} 2•B(N)} \;=\; \frac{E(B^2)+3•E(B)}{2•E(B)} \;=\; \frac{1}{2} • \left(E(B) + \frac{V(B)}{E(B)} + 3 \right)$$

Hieraus folgt, daß man zur Minimierung des durchschnittlichen Speicherbedarfs (was zwar nicht unbedingt für den in den Geräten vorzusehenden Speicherplatz, wohl aber für den Zeitaufwand beim Rücksetzen optimal ist), das Verfahren so konkretisieren muß, daß von mehreren möglichen Standardwerten immer zuerst der mit der bisher kleinsten M_G–Menge weitergegeben wird, um die Varianz von B möglichst klein zu halten. Nimmt man wieder an, daß jeder mögliche Zahlungswert gleich wahrscheinlich ist, so kann man erwarten, daß

$$d \approx \frac{E(B)}{2}$$

ist. Bei einer realistischeren Verteilung der Zahlungen wird B allerdings für kleinere Standardwerte größer sein als für sehr große.

Werden w verschiedene Standardwerte der Größen 1, 2, …, 2^{w-1} verwendet und hat die Bank von jeder Größe s Stück in Umlauf gebracht, so läßt sich E(B) als

$$E(B) = \frac{p \bullet z \bullet f \bullet g}{s \bullet w}$$

berechnen, da mit den s•w Standardwerten p•z•f•g Transaktionen ausgeführt werden.

Der Geldumlauf im System ist dabei

$$U = s \bullet (2^w - 1)$$

und der mittlere Besitz der Geräte U/g; der mittlere Umsatz eines Gerätes bei gleichmäßiger Verteilung der Beträge $p \bullet z \bullet 2^{w-1} \approx (U/g) \bullet E(B)$.

Im Beispiel der 20 Standardwerte mit f=10 und E(B)=10 sind also bei gleichmäßigem Zahlungsverhalten in etwa p•z•50 Vermerke pro Gerät zu speichern, was sicher sehr viel weniger als p•z•g sein werden. Die obere Schranke von p•z•g•s•w, die der in 4.2.2.2 angegebenen von p•z•g entspricht, ist allerdings aus denselben Gründen auch hier scharf: In diesem Fall muß man einen Betrag, der der Summe aller ausgegeben Standardwerte entspricht, kreisen lassen.

Um die Zuordnung von M_G–Mengen zu Einnahmen zu speichern, kann man hier auf eine explizite Darstellung verzichten: Die Einnahmen werden in verbrauchte und unverbrauchte aufgespalten. Für erstere ist die Zuordnung bedeutungslos; sie können sequentiell in einem Speicherbereich abgelegt werden. Für letztere kann man eine Speicherung als Liste von Paaren (Einnahme, M_G–Menge) wählen, da die M_G–Mengen unverbrauchter Einnahmen stets disjunkt sind. Duplikate können ja lediglich auftreten, wenn ein Gerät einen Standardwert mehrmals erhält und damit ein Teil der erhaltenen M_G–Menge bereits früher erhalten wurde und im Speicherbereich der verbrauchten M_G–Mengen abgelegt ist. Da dort aber keine Zuordnung zu retten ist, können solche Duplikate leicht beseitigt werden. Im Gegensatz zu den allgemeinen Überdeckungsverfahren ist also nun garantiert, daß der Speicherbedarf nicht größer wird als bei maximaler Weitergabe.

Die Bestimmung der Überdeckung erfordert keinen nennenswerten Aufwand: je Zahlung sind lediglich ungefähr f geeignete Standardwerte zu bestimmen (was bei geeigneter Sortierung konstanten Aufwand erfordert) und die dazugehörenden M_G–Mengen zu übergeben und als verbraucht umzusortieren.

Die Rücksetzprozedur ist wiederum mit der der maximalen Weitergabe identisch, allerdings ist die Länge der Listen L_G erheblich kürzer (p•z•f•d), dafür aber ist als Anzahl der Transaktionen eines Gerätes p•z durch p•z•f zu ersetzen. Im Mittel ergibt sich bei einem sequentiellen Rücksetzen ein Zeitaufwand von

$$\Theta\left(g \bullet (1-p \bullet v) \bullet p \bullet z \bullet f \bullet d \bullet \left(\log(p \bullet v \bullet g) + \frac{p \bullet v}{2} \bullet \log(p \bullet z \bullet f) \right) \right)$$

Schritten.

Einziger Nachteil der Einschränkung auf Standardwerte ist das vom heutigen Bargeld bekannte „Wechselgeldproblem", d.h. daß eine im Prinzip mögliche Zahlung nicht stattfinden kann, weil der Zahlungswillige den zu zahlenden Betrag nicht in der passenden Stückelung besitzt (und der Empfänger nicht herausgeben kann).

Vermeidet man das Problem, indem nur ein minimaler Standardwert (der „Pfennig") zugelassen wird, so erhöht sich f auf den durchschnittlichen Zahlungsbetrag. Beseitigt man das Problem, indem man Geräten das Halbieren von Standardwerten erlaubt, so hat man im Grunde wieder ein allgemeines Überdeckungsverfahren, d.h. die Zuordnung von M_G–Mengen zu Einnahmen stellt wiederum ein komplexeres Problem dar. Erhalten bleibt allerdings der Vorteil, daß i.allg. nur wenige teilweise verbrauchte Einnahmen übrig bleiben werden.

4.2.4 Grenzen allgemeiner Weitergabeverfahren

Zunächst wird gezeigt, daß mit den Überdeckungsverfahren nicht alle Weitergabeverfahren, insbesondere nicht alle minimalen (d.h. mit minimalem Speicherbedarf) gegeben sind.

Dazu werden zwei Beispiele angegeben, wie man, ausgehend von einem minimalen Überdeckungsverfahren, d.h. einem mit feinstem μ und ohne zusätzliche Weitergabe von O_G-Mengen, auf die Aufzeichnung oder Weitergabe gewisser Änderungsvermerke verzichten kann. Beim ersten geschieht dies, indem man gewisse Transaktionen löscht, beim zweiten, indem ein Gerät die Überdeckung eines anderen ändert.

Beispiel 1

Wenn Geräte G1 und G2 zwei einander aufhebende Transaktionen durchführen, indem G1 einen Betrag b an G2 zahlt und später G2 den Betrag b an G1, und G2 bei der zweiten gerade die erste als Überdeckung wählt, so können sie alle Aufzeichnungen über diese Transaktionen löschen. G1 muß dabei zusätzlich die Ausgaben, die bei der ersten Transaktion zur Überdeckung verwendet wurden, wieder als unverbraucht kennzeichnen.

Daß diese Situation vorliegt, sieht G2 sowieso, und G1 erkennt es daran, daß die Menge M_{G2}, die es von G2 erhält, nur aus den Vermerken über die erste Transaktion und seiner eigenen, damals bestimmten Menge M_{G1} besteht.

Die Sicherheit wird dadurch nicht beeinträchtigt, da in der Zwischenzeit keine anderen Geräte von der ersten Transaktion erfahren haben, da der Betrag b nicht noch zur Überdeckung einer weiteren Ausgabe gereicht hätte. Wäre den Geräten gestattet, nach Belieben O_G-Mengen weiterzugeben, so müßten sich G1 und G2 entweder zusätzlich versichern, daß sie die Vermerke über die erste Transaktion noch nicht weitergegeben haben, oder sie müßten das Löschen auf den Fall beschränken, daß die Transaktionen direkt nacheinander stattfinden, was an den Transaktionskennzeichen erkennbar wäre, sofern diese fortlaufend gewählt werden.

Beispiel 2

Man betrachte die Situation, in der ein Gerät G1 für drei Ausgaben A1, A2 und A3 mit den Werten 2, 4 bzw. 2 mittels zweier Einnahmen E1 und E2 mit Werten 3 bzw. 5 die in Bild 6 links dargestellte Überdeckung μ bildete.

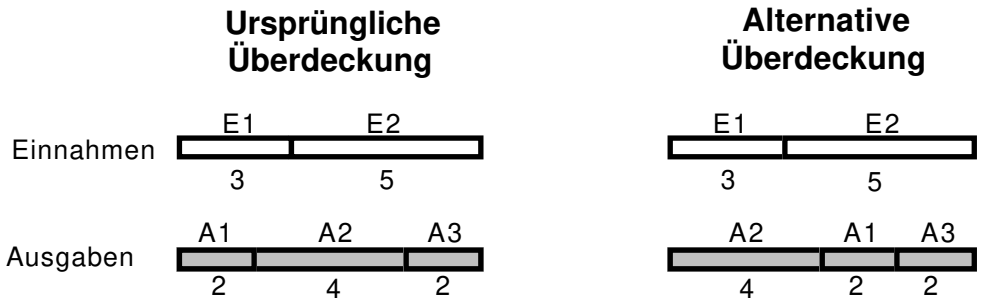


Bild 6 Beispiel eines Überdeckungswechsels

Es gilt also $\mu(A1)=\{E1\}$, $\mu(A2)=\{E1, E2\}$, $\mu(A3)=\{E2\}$. Dies ist eine feinste Überdeckung, die sich bei Verwendung des in Abschnitt 4.2.2.1 angegebenen Verfahrens zur Konstruktion linearisierbarer Überdeckungen zwangsweise ergibt, wenn die Transaktionen in der Reihenfolge E1, A1, E2, A2, A3 erfolgen.

Es ist nun möglich, daß ein Gerät G2 beide Ausgaben A1 und A3 erhält und $\mu(A1)$, $\mu(A3)$ und zusätzlich $\mu(A2)$ erfährt. Dazu genügt es z.B., daß es noch eine Zahlung (etwa vom Betrag 3) des ursprünglichen Empfängers G3 von A2 erhält, zu deren Deckung dieser A2 verwendet, und daß in den jeweiligen M_G-Mengen keine weiteren Änderungsvermerke von G1 sind.

Gibt G2 dann einen Betrag (etwa 4) aus, zu dessen Deckung es A1 und A3 verwenden möchte, so kann es darauf verzichten, den Änderungsvermerk über E1, der gemäß dem Überdeckungsverfahren zu A1 gehören würde, weiterzugeben, und damit auch dessen ganze M_G–Menge. Dies bedeutet, daß G2 statt des von G1 gewählten μ das in Bild 6 rechts dargestellte μ' verwendet, d.h. $\mu'(A1)=\{E2\}$, $\mu'(A2)=\{E1, E2\}$, $\mu'(A3)=\{E2\}$.

Die Sicherheit wird dadurch nicht beeinträchtigt, auch wenn G1 in O_{G1}-Mengen die Änderungsvermerke gemäß der ursprünglichen Überdeckung weitergibt: Wird ein Vermerk über A2 aufgefunden, so auch welche über E1 und E2, die bereits sämtliche Ausgaben überdecken. Wird der Vermerk über A2 nicht gefunden, aber der über A3, so auch der über E2, der in jedem Fall zur Überdeckung von A1 und A3 genügt. Wird nur ein Vermerk über A1 gefunden, so ist entweder einer über E1 oder einer über E2 dabei, was ebenfalls genügt.

Die Hoffnung, durch eine weitere Reduzierung der Weitergabe nicht nur in jenem anonymen Fall, wo das Verfahren der verteilten Kontostände nicht anwendbar ist, speichereffizientere Verfahren als die Überdeckungsverfahren zu finden, sondern zugleich auch in den anderen Fällen, insbesondere dem nicht anonymen, den Speicheraufwand unter den der verteilten Kontostände zu senken, kann allerdings nicht erfüllt werden. Genauer gesagt gilt, daß für die hier betrachteten Weitergabeverfahren der in den Geräten benötigte Speicherplatz mindestens proportional zu g ist. Es kann also beispielsweise nicht erreicht werden, daß in einem Gerät wie beim (unsicheren) Verfahren der einfachen Aufzeichnung (vgl. 4.1) nur soviel Vermerke gespeichert sein müssen, wie es Transaktionen durchgeführt hat.

Behauptung

Wenn ein sicheres Verfahren Transaktionen in der Form (G,b,T_G) aufzeichnet, alle aufgefundenen Änderungsvermerke nachvollzogen werden und dadurch jedes verlorene Gerät, dessen sämtliche Transaktionspartner nicht verloren sind, ohne Rücksetzabweichung rückgesetzt wird, so benötigen die Geräte Speicherplatz für mindestens g Transaktionen.

Beweis

Zum Beweis wird eine ähnliche Situation verwendet wie in Abschnitt 4.2.1.2: Sämtliche Geräte eines Systems können eine Folge $(Gi)_{i=1,...,g}$ bilden, bei der Gi für i=2,...,g-1 nur einen Betrag b von G(i-1) einnimmt und an G(i+1) wieder ausgibt und sonst keine Transaktionen durchführt.

Jedes G(i-1) muß den Vermerk (Gi,b,T_{Gi}) enthalten, da es die vorliegende Situation nicht von jener unterscheiden kann, in der Gi sofort nach dieser Transaktion verlorengeht. Dann wäre, falls G(i-1) gefunden wird, kein Partner von Gi verloren, so daß die Transaktion nachvollzogen werden müßte. Das ist, da auch G(i-1) den Vermerk darüber nicht mehr weitergegeben hat, nur möglich, wenn er bei G(i-1) gefunden wird.

Angenommen, Gg enthalte über irgendeine Ausgabe keinen Vermerk, d.h. für ein $i<g$ den Vermerk $(Gi,-b,T'_{Gi})$ nicht.

Dies ist unabhängig davon, welche der anderen Geräte nach ihren Transaktionen verlorengehen, da Gg darüber nichts erfährt. Es ist also möglich, daß alle Geräte außer Gg und G(i-1) verlorengehen. Dann hat einerseits Gg den Betrag b, andererseits erhält Gi denselben Betrag, da der Vermerk über seine Einnahme bei G(i-1) gefunden wird, der über seine Ausgabe jedoch nirgends. Dies steht im Widerspruch dazu, daß sich die Geldmenge im System nicht ändert.

Anmerkung

Man hätte auch gleich die im Text erwähnte stärkere Forderung an das Weitergabe- und Rücksetzverfahren stellen können, daß jede Transaktion, von der ein Partner überlebt, auch für den verlorenen Partner nachvollzogen werden können soll. Das wäre jedoch nicht völlig einsichtig. Beispielsweise würde sich in der in Bild 3 dargestellten Situation das korrekte Ergebnis ergeben, wenn man keine einzige der Transaktionen für G2 und G3 nachvollzöge, statt alle drei, wie eigentlich gewünscht.

Daß alle aufgefundenen Änderungsvermerke nachvollzogen werden, ist eine echt einschränkende Forderung an die zugelassenen Verfahren. So ist in dem beim Beweis verwendeten Beispiel beim Rücksetzen klar, weshalb der Rücksetzfehler auftritt, und es böte sich an, die Einnahme von Gi nicht nachzuvollziehen, da dieses den Betrag offensichtlich wieder ausgegeben haben muß, da er bei Gg real aufgefunden wurde. Schwieriger, aber nicht unmöglich, würde es schon, wenn G(g-1) statt Gg aufgefunden würde, da dann anhand der übrigen Änderungsvermerke von G(i-1) und G(g-1) entschieden werden müßte, welches der beiden den Betrag später hatte. Sobald man aber anfängt, die Änderungsvermerke nicht mehr als solche zu betrachten, sondern zur Codierung des Alters von anderen zu verwenden, ist es sinnvoller, gleich markierte Standardwerte zu verwenden (vgl. 4.3).

Dasselbe Beispiel kann auch als Beweis dienen, daß es nicht möglich ist, die Anzahl der Weitergaben der einzelnen Vermerke zu beschränken, z.B. auf zehnmal.

Entsprechend gilt auch, daß das Verfahren der verteilten Kontostände nicht dahingehend abgewandelt werden kann, daß die Geräte nicht mehr Speicherplatz für Kontostände von sämtlichen anderen vorsehen müssen. Gäbe es nämlich ein solches Verfahren, so ließe sich daraus sofort eines konstruieren, in dem die Geräte nicht mehr gleichzeitig Änderungsvermerke von allen anderen enthalten müßten, indem jeweils genau die Änderungsvermerke gespeichert würden, die zu den im anderen Verfahren gespeicherten Kontoständen führten.

4.3 Markierte Standardwerte

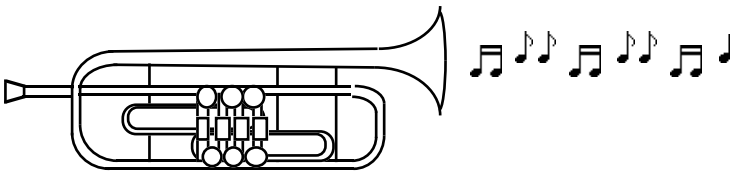
4.3.1 Protokoll, Sicherheit und Verlusttoleranz

4.3.1.1 Grundprinzip

Man kann im Verfahren der Standardwertüberdeckungen (vgl. 4.2.3) beim Rücksetzen statt der einzelnen Geräte einen einzelnen Standardwert N betrachten. Dazu bedeute, N werde einem verlorenen Gerät G „gutgeschrieben", daß ein Vermerk aufgefunden wird, der besagt, G habe N eingenommen, jedoch keiner des Inhalts, G habe N wieder ausgegeben. Somit erhält ein verlorenes Gerät G einen einmal besessenen Wert N genau dann gutgeschrieben, wenn der unmittelbare Vorbesitzer nicht verloren ist (der damit den Vermerk der Weitergabe von N an G der Bank übergibt), alle Nachbesitzer von N jedoch verloren sind (was trivialerweise immer dann erfüllt ist, wenn es keine Nachbesitzer gab).

Man sieht, daß jeder Standardwert am Schluß entweder im Besitz eines nicht verlorenen Gerätes ist oder genau einem verlorenen Gerät gutgeschrieben wird, nämlich dem Nachfolger des letzten nicht verlorenen Besitzers.

Zum Rücksetzen wichtig ist also nur, daß jedes Gerät aufzeichnet, welche Standardwerte es noch besitzt und an wen es welche Standardwerte weitergegeben hat, sowie daß den Weitergabevermerken der Bezug zueinander und ihre zeitliche Reihenfolge zu entnehmen ist. Diese Beobachtung führt zur Idee der markierten Standardwerte, die endlich erlaubt, auf die Weitergabe der immer länger werdenden Vorgeschichten der Transaktionen zu verzichten:



Die Form der Vermerke wird so geändert, daß einem Vermerk über die Weitergabe eines Standardwertes N an ein Gerät G sowohl die Nummer dieses Standardwertes als auch die Zahl z der bis dahin erfolgten Weitergaben von N zu entnehmen ist. Diese Nummer N, die in 4.2.3 die Form $(G0,b,T_B)$ hatte, braucht nun nur noch aus dem Nennwert und einer unter den Standardwerten dieses Nennwertes eindeutigen Kennzeichnung zu bestehen.

Da durch N und z bereits jede Transaktion eindeutig bezeichnet wird, kann auf ein Transaktionskennzeichen T_G verzichtet werden, außerdem ist der Betrag der Transaktion schon in N enthalten und ein Vorzeichen ist nicht mehr nötig, da nur noch Einnahmen gespeichert werden sollen (immer die Einnahme des Nachbesitzers beim zahlenden Gerät). Damit nehmen die Weitergabevermerke die Gestalt

$$(G,N,z)$$

an. Die Vermerke werden durch N sozusagen „markiert", wodurch im Gegensatz zu 4.2.3 nun jedem einzelnen Vermerk der Bezug zu einem bestimmten Standardwert anzusehen ist. Die Liste der von

einem Gerät aufgezeichneten Weitergabevermerke soll zur Vermeidung von Verwechslungen mit dem Verfahren der (unmarkierten) Standardwerte im folgenen WL_G, Weitergabeliste von G, genannt werden.

Zum Erreichen der Verlusttoleranz des in 4.2.3 beschriebenen Verfahrens reicht es nun, wenn in der z-ten Weitergabe eines Standardwertes N von G1 an G2 das Gerät G1 in WL_{G1} den Vermerk (G2,N,z) abspeichert und G2 sich (N,z) als erhalten merkt. Für letzteres werde eine weitere Liste, die Besitzliste BL_{G2}, vorgesehen (vgl. Bild 7). Zum Schluß könnte ein nicht verlorenes Gerät G der Bank neben WL_G auch BL_G direkt überspielen, es scheint aber praktischer, die noch im Besitz von G befindlichen Standardwerte mittels des normalen Zahlungsprotokolls an die Bank zu übertragen. Somit sind die Standardwerte, die nicht zuletzt im Besitz eines verlorenen Gerätes waren, am Ende in der Besitzliste der Bank zusammengefaßt.

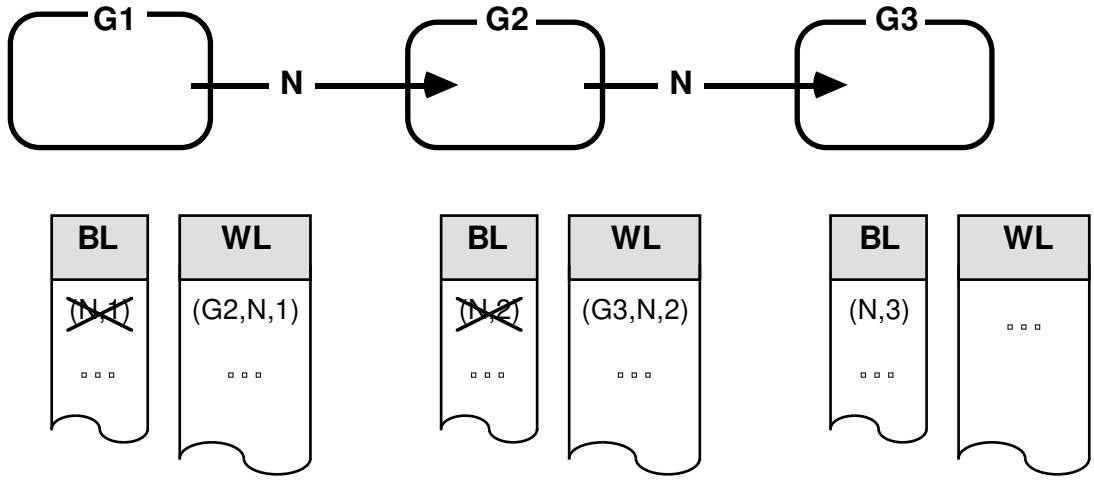


Bild 7 WL- und BL-Listen nach Weitergabe eines Standardwertes N

4.3.1.2 Rücksetzzeitpunkte

Im Gegensatz zu den Weitergabeverfahren kann man bei markierten Standardwerten auf eine gemeinsame Terminierung aller Geräte verzichten, wenn, wie den Geräten die maximale Lebensdauer p zugeordnet wurde, auch die Standardwerte eine maximale Gültigkeitsdauer p' erhalten, nach deren Ablauf ein Standardwert an kein anderes Gerät mehr weitergegeben werden darf.

Um hierdurch die Autonomie der Geräte möglichst wenig einzuschränken, werden wir davon ausgehen, daß ungültige Standardwerte gegenüber der Bank wie gültige verwendet werden können. Ein Gerät G, in dem ein Standardwert N ungültig wird, darf also N noch bis zu seinem eigenen Ungültigwerden behalten oder jederzeit davor mittels des normalen Zahlungsprotokolls bei der Bank einlösen. Dazu muß G die Bank nicht anhand eines eigenen Schlüssels von normalen sicheren Geräten unterscheiden können, wenn nur sie ungültige Standardwerte akzeptiert. Die Bank muß ungültig gewordene Standardwerte natürlich vorerst in ihrer Besitzliste BL_B aufbewahren, um sie nicht beim Rücksetzen einem anderen Gerät gutzuschreiben. (Noch gültige kann sie entweder in einem abgesonderten Teil von BL_B zur Weiterverwendung bereithalten oder, z.B. wenn die Restgültigkeitsdauer zu kurz ist, vorzeitig als ungültig deklarieren.)

Der Grund dafür, daß die feste endliche Gültigkeitsdauer der Standardwerte endgültiges Rücksetzen der Geräte nach vorherbestimmbarer Zeit erlaubt, ist, daß jeder einzelne Standardwert N ein eigenständiges kleines Zahlungssystem definiert: die Geräte dieses Systems sind diejenigen, die N besessen haben können, d.h. die frühestens p Zeiteinheiten vor dem Aktivieren von N und spätestens p' Zeiteinheiten danach selbst aktiviert wurden; der einzige Standardwert des Systems ist N (vgl. Bild 8).

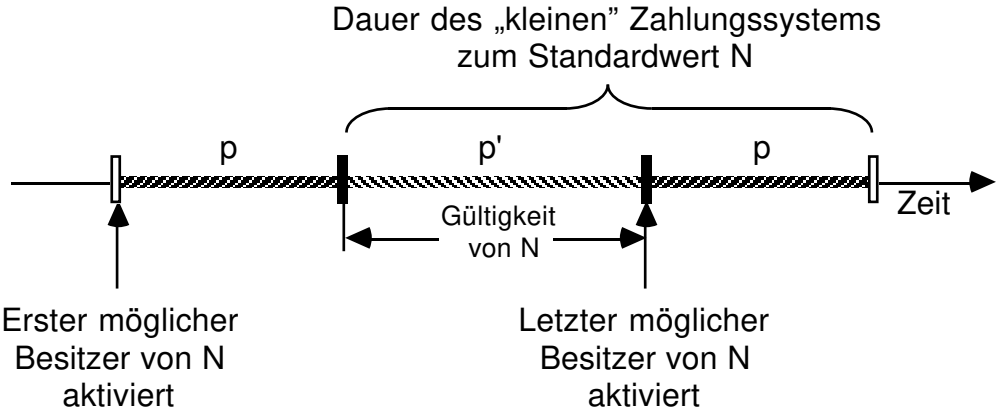


Bild 8 Dauer des „kleinen" Zahlungssystems zum Standardwert N

Das Rücksetzen geschieht im Grunde für jedes solche kleine Zahlungssystem getrennt, indem, falls N verloren ist, d.h. von keinem der Geräte seines Zahlungssystems wieder bei der Bank abgeliefert wird, aufgrund der N betreffenden Weitergabevermerke der „letzte" Besitzer von N (der zwangsläufig ebenfalls verloren ist) bestimmt wird und N diesem gutgeschrieben wird. Folglich kann das Rücksetzen bzgl. eines Standardwertes um die Zeit p nach dessen Ungültigwerden stattfinden.

Geht ein Gerät G verloren, so kann es spätestens dann vollständig rückgesetzt werden, wenn bzgl. aller Standardwerte, an deren „kleinen" Zahlungssystemen es hätte teilnehmen können, rückgesetzt werden kann, also (vgl. Bild 9) nach der Zeit p'+p nach seinem Ungültigwerden. Zum Rücksetzen von G genügen also auf jeden Fall die WL-Listen all der Geräte, die Informationen über von G besessene Standardwerte enthalten können, und der während der Dauer dieser kleinen Zahlungssysteme entstandene Teil von BL_B.

Man kann sich jedoch sogar auf die nach der Aktivierung von G ungültig gewordenen bzw. abgelieferten Geräte beschränken, denn ob G ein bestimmter Standardwert N gutgeschrieben wird, ergibt sich nur aus Aufzeichnungen von Geräten, die N an G weitergegeben haben können oder N nach G besessen haben können (vgl. Bild 9). Entsprechend muß auch nur der nach der Aktivierung von G entstandene Teil von BL_B betrachtet werden.

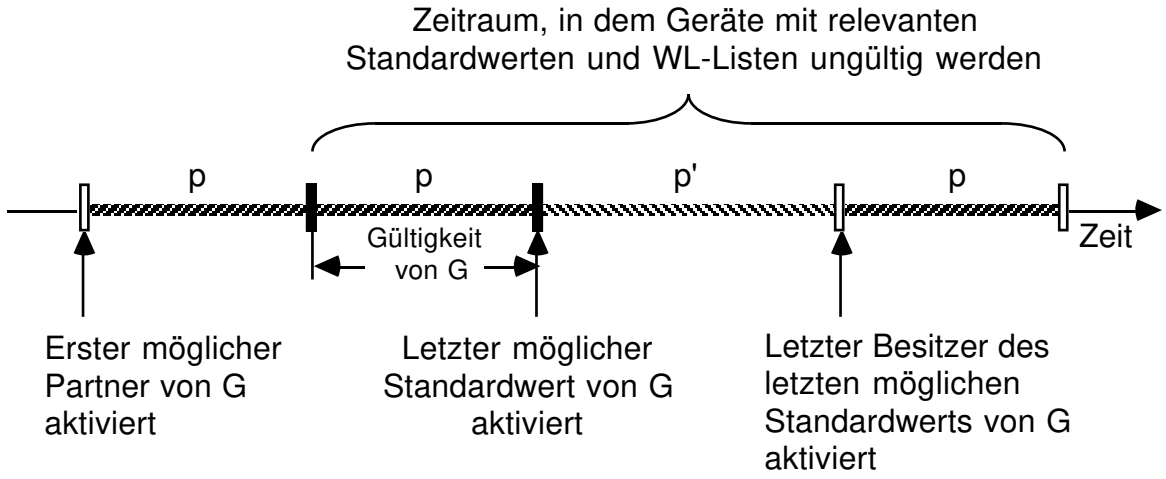


Bild 9 Für das Rücksetzen von G zu berücksichtigende andere Geräte

4.3.1.3 Umgang mit Zeitabweichungen

Damit die angegebenen Mengen relevanter Geräte bzw. Listen auch tatsächlich genau bestimmbar sind, sollten die Grenzen der „kleinen" Zahlungssysteme möglichst genau eingehalten werden. Da die Gültigkeitsdauern p und p' nur mit gewissen, durch die Ungenauigkeit der lokalen Geräteuhren bedingten Abweichungen eingehalten werden können, ist dies offenbar nicht absolut möglich.

Eine Möglichkeit zur Lösung dieses Problems wäre, die obigen Mengen in Abhängigkeit von den bekannten Abweichungen so zu vergrößern, daß die relevanten Geräte sicher enthalten sind.

Allerdings geht es auch einfacher und ohne Vergrößerung der Mengen: Jedes Gerät G1 kann anhand der Aktivierungszeitpunkte für jeden Standardwert N lokal entscheiden, ob es dem Zahlungssystem von N angehört, d.h. N besitzen darf, und für jedes Gerät G2, ob es ein möglicher Partner von G1 ist. Nehmen vor jedem Transfer von N beide Partner diese Prüfungen vor und findet ein Transfer nur dann statt, wenn die Prüfungen positiv ausfallen, so sind die Grenzen des Zahlungssystems von N sicher einzuhalten.

Wie man sieht, ist die absolute Begrenzung der Lebensdauer eines Standardwertes auf p' gar nicht notwendig: es würde ausreichen zu fordern, daß N nur zwischen Geräten des oben definierten Zahlungssystems von N ausgetauscht wird.

Um nun ein verlorenes Gerät tatsächlich rücksetzen zu können, muß die Bank allerdings einen absoluten Zeitpunkt wissen, wann ihr alle hierzu notwendigen WL-Listen und BL-Einträge vorliegen (wobei die Zeit der Bank als die absolute Bezugszeit betrachtet wird):

Geht man von einer bekannten und endlichen maximalen Abweichung Δ_1 der lokalen Geräteuhren aus und räumt man B_G nach Ungültigwerden von G ebenfalls nur eine bekannte Zeit Δ_2 ein, innerhalb derer er die Übergabe der letzten noch besessenen Standardwerte (d.h. der Liste BL_G) und der Liste WL_G an die Bank ermöglichen muß (andernfalls G als verloren betrachtet und für eine erneute Initialisierung untauglich wird, vgl. Kap. 2, Protokollskizze 1, und Abschnitt 3.2.2), so liegt der Bank zu jedem Gerät G spätestens $\Delta_1+\Delta_2$ Zeiteinheiten nach dem Ungültigwerden von G eine Verlustmeldung oder dessen WL-Liste und sämtliche von ihm besessenen Standardwerte vor.

4.3.1.4 Protokoll

Das Verfahren der markierten Standardwerte ist in der folgenden Protokollsizze 6 zusammengefaßt:

Initialisierung des sicheren Gerätes durch die Bank und B_G

[1] Wie in Protokollskizze 1. Zusätzlich erhält G seinen Aktivierungszeitpunkt und die Gültigkeitsdauern p und p' mitgeteilt.

[2] Für die Erstbestückung von G mit Standardwerten 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 eines Standardwertes von G1 an G2

[1-3] Wie in Protokollskizze 1.

[4] G1 und G2 prüfen anhand ihrer Aktivierungszeitpunkte, ob G1 und G2 mögliche Partner sind, d.h. ob G1 und G2 gleichzeitig gültig waren.
Ist dies nicht der Fall, so wird der Transfer abgebrochen.

[5] Eigentlicher Transfer

[5.1] G1 bestimmt einen (noch gültigen) Standardwert N, den G2 gemäß der Aktivierungszeitpunkte von G2 und N besitzen kann, und sendet das Paar (N,z) aus BL_{G1} an G2. Erhält G2 das Paar (N,z), so quittiert G2 (ggf. ebenfalls nach einer Prüfung, ob es N erhalten darf) und sendet (G2,N,z) an G1.
Für die Gültigkeit der Zahlung gilt das für Protokollskizze 1 Gesagte entsprechend.

[5.2] G1 fügt (G2,N,z) in seine Liste WL_{G1} und löscht (N,z) aus BL_{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 Standardwerte, die G1 haben könnte, ebenfalls ungültig sind (also p'), zum Schluß, bis auch alle anderen Geräte G2, die diese Standardwerte haben könnten, ungültig sind (also p), und schließlich noch solange, bis alle nicht-verlorenen Geräte ihre Aufzeichnungen der Bank übergeben haben (also $\Delta_1+\Delta_2$).
Geräte, die bereits ihre Liste WL_G der Bank übergeben haben, werden nicht zurückgesetzt.

[3] Nun werden G1 alle ungültig gewordenen Standardwerte N gutgeschrieben, 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 6 Verteilte Aufzeichnung: Standardwerttransaktionen

4.3.1.5 Sicherheit und Verlusttoleranz

Sicherheit und Verlusttoleranz des Verfahrens sind identisch mit denen des Verfahrens der Standardwertüberdeckungen (vgl. 4.2.3): unabhängig davon, welches Verfahren man wählt, wird ein verlorenes Gerät auf denselben Kontostand rückgesetzt; dies war gerade die Idee, die zu den markierten Standardwerten führte.

Die Sicherheit des Verfahrens erkennt man aber auch sofort, wenn man wieder je Standardwert N ein eigenes Zahlungssystem betrachtet: jedes kleine System ist offensichtlich sicher. Dies gilt auch dann, wenn man, wie in 4.3.1.3 begründet, die Forderung nach Gültigkeit von N in Schritt [5.1] des Zahlungsprotokolls streicht.

Für die Anonymisierung (vgl. Kap. 5) wie auch für eine effiziente Implementierung interessant ist die Beobachtung, daß es in Schritt [3] von „Ungültigwerden und Rücksetzen von G1" in Protokollskizze 6 genügt, nur solche Einträge (G3,N,z') auf z'<z zu prüfen, für die G3 ebenfalls verloren ist, da, wenn N nicht eingelöst wurde, der neueste gefundene Eintrag über N die Weitergabe an ein verlorenes Gerät aufzeichnet.

Wie schon bei den Überdeckungsverfahren in 4.2.2.1, so kann auch hier zur Erhöhung der Verlusttoleranz einem Gerät gestattet werden, zusätzlich Vermerke über frühere Transaktionen (also über Einnahmen seiner Partner, die es sowieso speichern muß, aber auch über eigene Einnahmen) weiterzugeben bzw. in einer gesonderten Optionalliste OL_G abzulegen und damit vorübergehend ungenutzten Speicherplatz sinnvoll auszunutzen.

Dabei brauchen nun keinerlei Zusammenhänge zwischen verschiedenen Vermerken mehr beachtet zu werden. Daher kann man sich jetzt z.B. auf zehnmalige Weitergabe jedes Vermerkes beschränken.

Allerdings kann es in diesem Fall wieder vorkommen, daß Vermerke über einen verlorenen Standardwert N in OL_G–Listen beliebig lange existieren und der Bank erst dann übergeben werden, wenn N längst einem verlorenen Gerät gutgeschrieben wurde. Jedoch können solche veralteten Vermerke nun vom aufzeichnenden Gerät G gelöscht oder von der Bank ignoriert werden, ohne die Sicherheit des Verfahrens zu beeinträchtigen. Veraltet ist ein Vermerk dabei, wenn sein „kleines" Zahlungssystem terminiert hat, d.h. um die Zeit p nach dem Ungültigwerden von N, und der Unterschied zu den Weitergabeverfahren besteht darin, daß die Geräte, die nach diesem Zeitpunkt den Vermerk haben, mit dem Standardwert selbst nichts mehr zu tun haben konnten.

In Protokollskizze 6 wurde diese Erweiterung nicht dargestellt.

Für die Sicherheit der Teilnehmer vor Betrugsversuchen der Bank gilt im Prinzip dasselbe wie für die Weitergabeverfahren (vgl. Ende von 4.2.1.1), jedoch mit „kleinen" Unterschieden.

Wie dort kann ein Besitzer eines nicht verlorenen Gerätes von der Bank nicht betrogen werden. Für den Besitzer B_G eines verlorenen Gerätes G erscheint die Situation jedoch ungünstiger: da hier auch Vermerke anderer Geräte für das Rücksetzen von G wichtig sind (nämlich von Geräten, die dieselben Standardwerte nach G besaßen), scheidet die für Weitergabeverfahren vorgeschlagene Möglichkeit, G alle es betreffenden Vermerke unterschreiben zu lassen, aus. Wie also soll das Hinzuerfinden von Vermerken verhindert werden?

Die mögliche Antwort auf diese Frage hängt davon ab, wem man vertraut (vgl. auch die Angreifermodelle in Kap. 5).

Mißtraut man manchen am Zahlungsprotokoll Beteiligten, etwa weil der Bank gestattet ist, Zahlungen selbst genau wie die sicheren Geräte durchzuführen, so muß zwangsläufig jede für G wichtige Rücksetzinformation anderer Geräte eine Authentikation von G enthalten. Mit anderen Worten: man muß Standardwertüberdeckungen mit den entsprechenden Authentikationen verwenden. (In Kap. 5 wird dies das Angreifermodell A3 sein.)

Vertraut man jedoch allen am eigentlichen Zahlungsprotokoll Beteiligten, d.h. wird dieses auch von der Bank nur mittels sicherer Geräte durchgeführt, so ist ein ähnliches Vorgehen wie bei den Weitergabeverfahren möglich: statt eines Signierschlüssels für jedes Gerät wird ein solcher Schlüssel für alle sicheren Geräte gemeinsam gewählt (d.h. von den Herstellern derselben) und vor allen anderen, Bank und Besitzer der Geräte eingeschlossen, geheimgehalten. Da solch ein Schlüssel zur Identifizierung der sicheren Geräte untereinander ohnenhin sinnvoll erscheint, kann natürlich auch gleich dieser genommen werden (vgl. Kap. 1). (In Kap. 5 wird dies das Angreifermodell A2 sein.) Damit ist wie für die Weitergabeverfahren die Erzeugung gefälschter Vermerke durch die Bank nicht möglich.

Um Unterschlagungen zu verhindern, gibt es auch hier dieselben beiden Methoden wie früher: Hat B_G auf einem zweiten Gerät G^* einen Rücksetzpunkt erstellt, so kann er von der Bank zumindest für jeden Standardwert, den G aufgrund der Informationen in G^* zum Zeitpunkt der Rücksetzpunkterstellung besessen hat, der G jedoch durch das Rücksetzen nicht zugesprochen wurde, einen Beweis verlangen, daß er nach G noch von einem weiteren Gerät besessen wurde (sei es, daß ihn ein anderes Gerät an die Bank übergab oder er einem anderen verlorenen Gerät zugesprochen wurde). Die zweite Möglichkeit, das gesamte Rücksetzprotokoll nachzurechnen bzw. von „Kontrollbanken" nachrechnen zu lassen, bleibt unverändert erhalten.

4.3.2 Aufwand

4.3.2.1 Aufwand der sicheren Geräte

Der Speicheraufwand der einzelnen sicheren Geräte bestimmt sich hier im wesentlichen durch die Listen BL_G und WL_G. Diese enthalten ohne zusätzliche Weitergabe zusammen über jede bisherige Einnahme von G einen Vermerk. Da ein Gerät (mit den Bezeichnungen aus 4.2.1.3 und 4.2.3) im Mittel p•z•f Transaktionen vornimmt, wird im Mittel auch höchstens Platz für

$$p \bullet z \bullet f$$

Vermerke benötigt. Die logarithmischen Faktoren sind hierbei wieder vernachlässigt. Der Speicherbedarf ist also von derselben Größenordnung wie beim Verfahren der einfachen Änderungsaufzeichnung.

Für die mehrfache Weitergabe hängt der Speicherbedarf von der verwendeten Weitergabestrategie ab:

Zur Beschreibung der verwendeten Strategie betrachte man den einem Vermerk V zugeordneten Weitergabebaum, in dem zu jedem Zeitpunkt jedes Gerät, das V aufzeichnet, einen bestimmten Platz

und damit entsprechend seiner Ordnung im Baum einen Namen innehat (vgl. Bild 10): der Baum besteht zu Beginn lediglich aus einer Wurzel mit zwei Blättern, wobei die beiden Blätter die an der durch V bezeichneten Zahlung beteiligten Geräte bezeichnen. Willkürlich sei der Zahlende, G1, der linke, der Empfänger, G2, der rechte Sohn. Gibt G2 an G3 den Vermerk weiter, und hatte G3 diesen Vermerk bereits erhalten, so ändert sich der Baum nicht; ansonsten wird das Blatt, das zuvor G2 innehatte, zum inneren Knoten und G2 bzw. G3 zu dessen linken bzw. rechten Sohn. Wird V m-fach weitergegeben, so ist dieser Weitergabebaum endlich und besitzt m Blätter.

Eine deterministische Strategie zur m-fachen Weitergabe zeichnet sich nun dadurch aus, daß sie durch einen einzigen Weitergabebaum mit m Blättern angegeben werden kann, der die Weitergabe aller Vermerke vollständig beschreibt, und daß jede Transaktion zur Weitergabe aller Vermerke, die noch weiterzugeben sind (d.h. bzgl. denen sich das Gerät in einem inneren Knoten befindet), genutzt wird. (Insbesondere heißt dies, daß die Weitergabe unabhängig vom Zeitpunkt, aufzeichnenden Gerät, Höhe der Transaktion usw. erfolgt!)

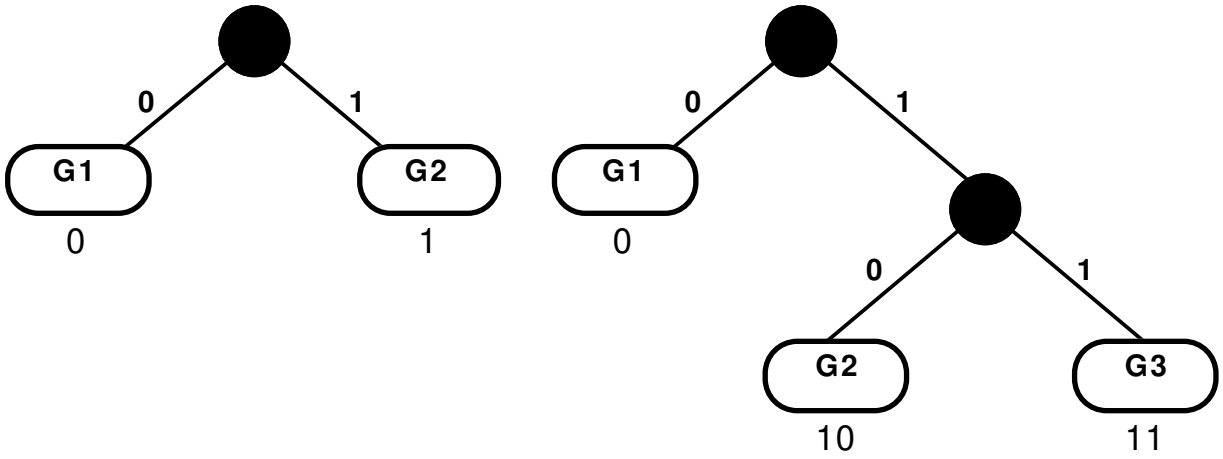


Bild 10 Weitergabebaum. Links ist der Anfangszustand dargestellt: nur die an der Zahlung beteiligten Geräte kennen V. Rechts ist die Situation nach der Weitergabe von V von G2 an G3 dargestellt.

Sinnvolle deterministische Weitergabestrategien sind z.B. gegeben durch:

- Einen ausgewogenen Baum mit $m = 2^k$ Blättern: dies heißt, daß jedes Gerät, das einen Vermerk V speichert, bei jeder Weitergabe von V die Hälfte aller Versionen von V, die es kennt, weitergibt.
- Einen nach links entarteten Baum der Tiefe m-1 mit m Blättern: dies heißt, daß das V erzeugende Gerät selbst V m mal weitergibt.

Wird ein Vermerk nun gemäß einer vorgegebenen deterministischen Strategie m-fach weitergegeben, so erhöht sich dieser Speicherbedarf der sicheren Geräte um den Faktor m, d.h. auf

$$m \bullet p \bullet z \bullet f$$

Beweis

Für jede deterministische Strategie zur m-fachen Weitergabe gibt es genau m-1 innere Knoten.

(Wie leicht einzusehen ist: Für m=1 gibt es keine inneren Knoten. Stimmt die Behauptung für m Blätter, so auch für m+1, da ein Weitergabebaum mit m+1 Blättern aus einem mit m

hervorgeht, in dem ein Blatt zum inneren Knoten wird, an den zwei neue Blätter gehängt werden, wodurch sich beide Anzahlen um 1 erhöhen.)

Besitzt ein Gerät zu jedem der m-1 inneren Knoten höchstens einen Vermerk, so ist alles gezeigt, denn dann kann es in jeder Transaktion höchstens m-1 alte Vermerke weitergeben. Zusammen mit dem Vermerk über die aktuell stattfindende Transaktion vergrößert sich damit im Partnergerät die Menge der aufzuzeichnenden Vermerke um höchstens m Stück, so daß, wie behauptet, maximal m•(Anzahl der Transaktionen) Vermerke aufgezeichnet werden müssen.

Angenommen sei nun, durch eine Transaktion zwischen G1 und G2 trete erstmals (bezogen auf eine beliebige Serialisierung gleichzeitig stattfindender Transaktionen) die Situation auf, daß ein Gerät, o.B.d.A. G1, zu einem inneren Knoten mit Namen x zwei verschiedene Vermerke V1 und V2 aufzeichne.

x kann dabei sicherlich nicht die Wurzel des Baumes sein, da pro Transaktion nur ein neuer Vermerk entsteht. Folglich hat x im Weitergabebaum einen eindeutig bestimmten Vaterknoten x'. Da die aktuelle Transaktion die erste sein soll, für die diese Situation auftritt, muß vor dieser Transaktion o.B.d.A. V1 nur in G1 und V2 nur in G2 aufgezeichnet gewesen sein, beide jedoch jeweils unter dem Namen x'.

Nach der Weitergabe von V1 durch G1 erhält G1 bzgl. V1 den Namen x'0; nach dem Empfang von V2 durch G1 erhält G1 bzgl. V2 den Namen x'1. Nach Annahme muß nun gelten x = x'0 = x'1, was offenbar einen Widerspruch darstellt.

Die Forderung, daß alle Vermerke immer weitergegeben werden, bedeutet eine gewisse Einschränkung der Verlusttoleranz, da im schlimmsten Fall zwei Geräte so viele aufeinanderfolgende Transaktionen miteinander durchführen, daß der Vermerk über die erste davon nur zwischen diesen beiden Geräten ausgetauscht wird.

Verbessert man aber die Verlusttoleranz, indem die Geräte die Annahme von Vermerken, die sie schon haben, verweigern, so ist der Speicherbedarf der einzelnen Geräte nicht mehr nur von der Anzahl der von ihnen selbst durchgeführten Transaktionen abhängig; z.B. würde für beliebeiges n ein Gerät G1, das eine Transaktion mit G2 durchführt, das zuvor n Transaktionen mit ein und demselben G3 durchführte, bei dieser Transaktion mindestens n Vermerke erhalten.

Man kann nun auch mühelos den Speicherbedarf der Geräte beschränken, indem man die Anzahl der mit einem Gerät durchführbaren Transaktionen beschränkt, z.B. auf ein festes Vielfaches von p•z•f. Außerdem ist es wieder sinnvoll, einen erschöpften Speicher durch Übergabe der Vermerke an die Bank zu leeren. Damit dürfte der Speicherbedarf der Geräte einem praktischen Einsatz dieses Verfahrens nicht im Wege stehen.

Der Zeitaufwand für eine einzelne Zahlung (bei Vernachlässigung der Weitergabe zusätzlicher Vermerke) ist bestimmt durch die Suche des Zahlenden nach durchschnittlich f passenden Standardwerten. Ohne Einrechnung des Aufwandes, der entsteht, wenn der Zahlende erst mit der Bank kommunizieren muß, um Geld zu wechseln, ist dies natürlich wieder ein Knapsack-Problem, das aber für vernünftige Nennwerte, z.B. w Zweierpotenzen wie in 4.2.3, linear in w gelöst werden kann. Der Kommunikationsaufwand ist für jede Transaktion konstant, also je Zahlung linear in f.

4.3.2.2 Aufwand zum Rücksetzen

Im folgenden wird zur Vereinfachung nur der Fall der einfachen Weitergabe betrachtet; der allgemeinere Fall der m-fachen Weitergabe kann völlig analog behandelt werden, wenn man beachtet,

daß die WL-Listen um den Faktor m länger, die BL-Listen, die Listen der verlorenen Geräte und der verlorenen Standardwerte jedoch gleichlang sind wie für m=1.

In Protokollskizze 6 wurde zum Rücksetzen jeweils ein einzelnes verlorenes Gerät G betrachtet. Um dieses rückzusetzen, muß die Bank

- zunächst aus allen für G relevanten WL-Listen herausfiltern, welche Standardwerte G jemals nachweislich besaß,
- die erhaltene, im Mittel p•z•f/2 Elemente umfassende Liste sortieren,
- schließlich aus dieser Liste aufgrund aller relevanten Einträge in BL_B und aller relevanten WL-Listen alle Standardwerte streichen, die G nicht als letzter besaß und
- B_G die übrigen Standardwerte (bzw. deren Gegenwert) gutschreiben.

Aufgrund der Überprüfung sämtlicher WL-Listen im vorletzten Schritt ergibt dies je verlorenem Gerät insgesamt einen mittleren Zeitaufwand von

$$\Theta\left(g \bullet p\bullet z\bullet f \bullet \log\left(\frac{p\bullet z\bullet f}{2}\right) \right)$$

wobei sinnvollerweise von $n < p\bullet z\bullet f\bullet g$ ausgegangen wurde; n bezeichne die Anzahl der Standardwerte, die sich gleichzeitig im System befinden, einschließlich der verlorenen.

Es wird stets davon ausgegangen, daß sich die Standardwerte gleichmäßig auf die Geräte verteilen.

Wesentlich sinnvoller als die obige Betrachtung eines einzelnen Gerätes ist es jedoch, zu überlegen, wie alle p•v•g während eines Zeitraums p verlorenen Geräte effizient zurückgesetzt werden können.

Eine p•v•g-malige Ausführung des obigen Verfahrens ist dabei wenig effizient, da dabei die gesamten WL-Listen und BL-Einträge dieses Zeitraums p•v•g-mal durchgegangen werden müßten. Sinnvollerweise wird man daher versuchen, möglichst viele Geräte mit gemeinsamen relevanten WL-Listen und BL-Einträgen gleichzeitig rückzusetzen.

4.3.2.2.1 Minimaler Aufwand bei gleichzeitiger Systemterminierung

Der zum Rücksetzen günstigste Fall ist die gleichzeitige Systemterminierung, da dann alle verlorenen Geräte gemeinsam zurückgesetzt werden können.

Obwohl man die gleichzeitige Systemterminierung für praktische Belange nicht erzwingen wollen wird, wird der Aufwand zunächst für diesen Fall ausführlich beschrieben, da sich einerseits der Aufwand der Prozeduren bei versetztem Ungültigwerden hieraus leicht herleiten läßt und andererseits das vorläufige Wegfallen der Betrachtungen, welche Listen zu welchem Zeitpunkt bearbeitet werden müssen, die Verständlichkeit erhöht.

Bei realistischen Parametern wird der Hauptaufwand beim Rücksetzen durch die Bearbeitung der WL-Listen entstehen, so daß es sinnvoll erscheint, diesen Schritt zu optimieren.

Aus den WL-Listen werden (vgl. die Bemerkung nach Protokollskizze 6) nur diejenigen Einträge benötigt, die die Weitergabe eines verlorenen Standardwertes an ein verlorenes Gerät aufzeichnen. Zweckmäßigerweise werden also die WL-Listen einmal sequentiell durchgegangen und jeder Eintrag mit der zuvor vorsortierten kürzeren der beiden Listen der verlorenen Standardwerte und der verlorenen Geräte verglichen. Dies ist sicherlich die der p•v•g verlorenen Geräte, außer wenn viele Benutzer leere Geräte absichtlich verlieren. Ergebnis ist die etwa g•p•z•f • (p•v)/2 Einträge enthaltende Liste VL der verlorene Geräte betreffenden Weitergabevermerke.

Damit ist auch klar, daß die Rücksetzprozedur bei gleichzeitiger Systemterminierung einen Mindestaufwand von

$$\Omega(g \bullet p \bullet z \bullet f \bullet \log(p \bullet v \bullet g))$$

hat.

Aus der verbliebenen Liste VL müssen nun zumindest die Einträge, die verlorene Standardwerte betreffen, nach den Standardwerten sortiert werden, um sie dem Alter nach vergleichen zu können.

Hierfür wird sinnvollerweise die kürzere der beiden benötigten Listen, d.h. die der gefundenen Standardwerte oder VL, vorsortiert. Geht man davon aus, daß der größere Teil der Standardwerte nicht verlorengeht, so hat erstere Liste etwa die Länge n. Es scheinen somit folgende zwei Vorgehensweisen günstig:

1. $g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 < n$: Man sortiert zuerst die Liste VL nach Standardwerten, wobei man von mehreren Einträgen zum selben Standardwert nur den neuesten behält. Sodann wird BL_B einmal durchgegangen und für jeden auftretenden Standardwert N in VL ein N betreffender Eintrag ggf. gestrichen.

   Dies verursacht einen Aufwand von

   $$\Theta(g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 \bullet \log(g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2) + n \bullet \log(g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2))$$

   Unter Verwendung der Ungleichung $g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 < n$ läßt sich dies zu

   $$\Theta(n \bullet \log(g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2))$$

   vereinfachen.
2. $g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 \geq n$: Man bestimmt zunächst allein anhand von BL_B, welche Standardwerte verloren sind. Dies bedeutet, daß BL_B sortiert wird und im Ergebnis geprüft wird, welche der (mit fortlaufender Numerierung) ausgegebenen Standardwerte fehlen. Es wird dabei eine Liste der verlorenen Standardwerte angelegt, die nachher zu jedem auch noch die neuste darüber gefundene Aufzeichnung aufnehmen soll. Diese hat etwa die Länge $p \bullet v \bullet n$.

   Nun wird für jeden Eintrag aus VL geprüft, ob der betroffene Standardwert in der Liste der verlorenen Standardwerte auftritt, und ggf. die Aufzeichnung dort eingetragen, sofern sie neuer ist als eine dort evtl. bereits vorhandene. Dies erfordert einen Aufwand von

   $$\Theta(n \bullet \log(n) + g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 \bullet \log(p \bullet v \bullet n))$$

Daß die Entscheidung jeweils das effizientere Vorgehen erlaubt, ist nun leicht einzusehen:

- Für $g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 < n$ ist schon $n \bullet \log(n)$ allein größer als jeder Summand des ersten Verfahrens;
- für $g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 \geq n$ ist $n \bullet \log(n)$ kleiner als beide und es gilt sowieso $p \bullet v \bullet n < g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2$, da über jeden verlorenen Standardwert mindestens ein Eintrag existiert.

Zum Schluß wird in jedem Fall anhand der übriggebliebenen Liste der Länge $p \bullet v \bullet n$ jeder verlorene Standardwert dem dabei vermerkten Besitzer gutgeschrieben. Der Aufwand hiervon ist zu vernachlässigen.

Insbesondere für den Fall, daß das zweite Verfahren verwendet werden muß, läßt sich die anfangs gemachte Aussage, daß der Hauptaufwand i.allg. in der Bearbeitung der WL-Listen bestehe, nun belegen:

Der restliche, durch das zweite Verfahren verursachte Aufwand läßt sich grob zu $O(g \bullet p \bullet z \bullet f \bullet p \bullet v \bullet \log(n))$ zusammenfassen.

Wäre dies mehr als $\Omega(g \bullet p \bullet z \bullet f \bullet \log(p \bullet v \bullet g))$, so wäre asymptotisch

$$p•v • \log(n) > \log(p•v•g).$$

Setzt man x=1/(p•v), so heißt das

$$\log(n) > x • \log(g/x) = - x • \log(x/g).$$

Wie man leicht nachrechnet, ist die rechte Seite für $x < g/e$, also $p•v•g > e$, monoton steigend. Man kann sich auf diesen Fall beschränken, da der umgekehrte Fall, daß höchstens 2 Geräte verlorengehen, trivial ist (und außerdem meist $g•p•z•f•(p•v)/2 < n$, also Verwendung des anderen Verfahrens, zur Folge hat) . Daher wird die Ungleichung bei festen g und n am ehesten für kleines x, d.h. großes p•v erfüllt. Nimmt man z.B. an, daß für den Verlustanteil $p•v \leq 1/5$ gilt, was bei geeignetem p sicher der Fall ist, so folgt $\log(n) > 5 • \log(g/5)$, d.h. $n > (g/5)^5$ oder $n/g > g^4/5^5$. Für g>100 bedeutet dies z.B. n/g > 32000. Eine derartige mittlere Anzahl von Standardwerten pro Gerät erscheint unsinnig.

In diesem Fall ist also der Gesamtaufwand der Rücksetzprozedur bei gleichzeitiger Systemterminierung

$$\Omega(g•p•z•f • \log(p•v•g)).$$

Bei Verwendung des ersten Verfahrens sind eher Fälle möglich, wo nicht die Bearbeitung der WL-Listen, sondern von BL_B den Hauptaufwand verursacht. Asymptotisch gilt dies, wenn

$$n • \log(g•p•z•f•(p•v)/2) > g•p•z•f • \log(p•v•g).$$

Wählt man y so, daß $g•p•z•f = (1+y)•n$, d.h. daß y die mittlere Anzahl der Weitergaben eines Standardwertes ohne die ursprüngliche Ausgabe durch die Bank ist, so ist obiges äquivalent zu

$$\log(g•p•z•f•(p•v)/2) > (1+y) • \log(p•v•g),$$

d.h.

$$p•z•f/2 > (p•v•g)^y.$$

Wird die Autonomie des Zahlungssystems wirklich ausgenutzt und ist beispielsweise $y \geq 10$, so ist dies, sobald eine nennenswerte Zahl von Geräten verlorengeht, wieder unsinnig. Für y=1 allerdings bedeutet es nur, daß weniger Geräte verlorengehen, als pro Gerät Transaktionen vorgenommen werden, was durchaus denkbar ist.

In diesen Fällen kann man jedoch das Verfahren wiederum nicht verbessern, da auch BL_B bereits in der günstigsten Weise, d.h. durch Vergleich mit der kürzesten in Frage kommenden Liste, bearbeitet wird.

Beim zweiten Verfahren wird man das Vorsortieren von BL_B, wenn eine Bitreihung über die Nummern sämtlicher ausgegebener Standardwerte in einem Hauptspeicher Platz findet, durch Abhaken der in BL_B befindlichen Standardwerte in einer solchen Reihung vornehmen. Bei konkreten Parameterwerten kann es, wenn der Platz auch für eine entsprechende Reihung von Paaren (G,z) reicht, günstig sein, das Verfahren so abzuwandeln, daß das Suchen in der Liste verlorener Standardwerte ebenfalls durch Indizieren in der längeren Reihung über sämtliche ausgegebenen Standardwerte ersetzt wird.

Die entsprechenden Aufwände für eine m-fache Weitergabe erhält man durch Multiplikation der Listenlängen mit m. Insbesondere ergibt sich als Hauptaufwand

$$\Omega(g • m • p•z•f • \log(p•v•g))$$

Zu guter Letzt sei nochmals betont, daß alle Aussagen dieses Abschnitts asymptotischer Art sind, also insbesondere die Bedingungen für die Optimalität des einen oder anderen Verfahrens im Einzelfall etwas anders lauten können. Konkrete Kriterien und Aufwandsaussagen sind jedoch aus den obigen leicht herzuleiten und dürften sich von jenen, da keine großen Konstanten vernachlässigt wurden und

die Einzelschritte der Verfahren im wesentlichen aus Speicherzugriffen (inkl. Adreßrechnung) und Vergleichen bestehen, nur um nicht allzu große Faktoren unterscheiden.

4.3.2.2.2 Rücksetzen ohne gleichzeitige Systemterminierung

4.3.2.2.2.1 Parameter

Für das Verfahren ohne gemeinsame Systemterminierung ist zu den Systemparametern folgendes zu bemerken:

- p ist nach wie vor die Gültigkeitsdauer der Geräte. Als Preis für die größere Flexibilität beim Übergang von einer Periode zur nächsten ist gegenüber der gemeinsamen Systemterminierung aber die Autonomie der Geräte während dieser Zeit stärker eingeschränkt, da zum Wechselgeldproblem das hinzutritt, daß Standardwerte, die man besitzt, ungültig werden.
- p' muß folglich mindestens so groß wie p gewählt werden, damit wenigstens die Standardwerte, die ein Gerät G bei seiner Aktivierung von der Bank erhält, während der gesamten Gültigkeitsdauer von G ebenfalls gültig bleiben.

Wenn man die Zeitpunkte, zu denen Standardwerte ungültig werden können (und die wegen der endlichen Genauigkeit sowieso diskret gewählt werden müssen), nicht zu dicht wählt, so ist die Autonomie jedoch wenigstens in der dazwischenliegenden Zeit wieder nur durch das Wechselgeldproblem beschränkt. Diese Zeitpunkte werden im folgenden Basiszeitpunkte genannt.

- a sei der (feste) Abstand zwischen den Basiszeitpunkten.

Damit möglichst selten der Fall eintritt, daß ein gerade eingenommener Standardwert sofort ungültig wird, sollten die Basiszeitpunkte nur zu exotischen Zeiten, z.B. morgens um 3 Uhr liegen.

Wenn man die Protokollvariante verwendet, in der ein ungültiger Standardwert zwischen Geräten, die beide dessen kleinem Zahlungssystem angehörten, noch ausgetauscht werden darf, ist das Problem, daß ein soeben erst erhaltener und sofort ungültig gewordenener Standardwert schon nach kurzer Zeit nicht mehr verwendet werden kann, stark reduziert, da er noch an alle Geräte, die nicht in dieser kurzen Zeit ausgegeben wurden, weitergegeben werden kann. In den meisten Situationen, wo man keine Möglichkeit hat, einen ungültigen Standardwert einfach bei der Bank zu tauschen, wird zudem auch der Partner keine Möglichkeit gehabt haben, an solch ein neues Gerät zu kommen.

Durch die Einführung der Basiszeitpunkte kann im ursprünglichen Protokoll, wenn man weiterhin jederzeit einen Standardwert bei der Bank abheben kann, nicht mehr jeder die volle Zeit p' gültig sein. Man kann dies aber, wenn für p' ein Vielfaches von a gewählt wurde, so umdeuten, daß man sich alle Standardwerte als zu einem Basiszeitpunkt ausgegeben denkt; beim Abheben eines Standardwertes bei der Bank erhält man einen mit dem gerade aktuellsten Ausgabedatum. Es bietet sich an, auch Geräte nur zu Basiszeitpunkten ungültig werden zu lassen, wonach für p dasselbe wie für p' gilt. Hiervon wird im folgenden ausgegangen.

Das Verhalten der Geräte zu den Basiszeitpunkten wird dabei so gewählt, daß ein Gerät, das zu einem bestimmten Zeitpunkt ungültig wird, mit einem, das zur selben Zeit aktiviert wird, keine Transaktion vornehmen kann; ebenso soll es keinen Standardwert annehmen, der zu diesem Zeitpunkt ausgegeben wird oder der zum Zeitpunkt der Aktivierung von G ungültig wird.

Ebenfalls angenommen wird eine Gleichverteilung der Zeitpunkte des Ungültigwerdens von Geräten und Standardwerten, d.h. zu einem Basiszeitpunkt werden g•(a/p) Geräte und n•(a/p') Standardwerte ungültig.

Außerdem wird wie in Abschnitt 4.2.1.3 vereinfachend angenommen, daß p•v•g Geräte in jedem Zeitraum p verlorengehen. In der Tat würden diesmal bei kleinem a immer gleichviele Geräte gerade verloren sein. Wenn stets noch h vorhanden sind, gehen jedoch in jedem Zeitraum p eigentlich nur p•v•h verloren. Da Geräten, die überhaupt verlorengehen, dies im Mittel nach ihrer halben Gültigkeitsdauer zustößt, sind zu jedem Zeitpunkt p•v•h/2 schon verloren, also gilt $h = g - p•v•h/2$. Daraus folgt $h = g/(1+pv/2)$.

Δ_1 ist als Uhrabweichung gegen p zu vernachlässigen.

Δ_2 kann sicher als O(p) angenommen werden, da, zumindest solange man am Zahlungssystem weiter teilnimmt, sowieso in jedem Zeitraum p ein Kontakt mit der Bank nötig ist. Evtl. wird man es sogar wesentlich kleiner wählen: Es ist nicht verboten, ein Gerät schon vor dem eigentlichen Ungültigkeitstermin für ungültig zu erklären, somit besteht die wesentliche Einschränkung durch Δ_2 darin, daß ein Gerät spätestens um $p+\Delta_2$ nach der Ausgabe neu initialisiert werden muß. Verkürzt man innerhalb dieses Zeitraums p zugunsten von Δ_2, so ist der einzige positive Effekt für den Besitzer, daß er frühzeitiger angehalten ist, diesen Termin nicht zu vergessen.

$\Delta_1+\Delta_2$ wird im folgenden zur Vereinfachung der Prozedurtexte auch als ganzzahliges Vielfaches von a angenommen.

Bei der folgenden Beschreibung der Änderung der Rücksetzprozeduren gegenüber 4.3.2.2.1 werden wir davon ausgehen, daß nach jedem Basiszeitpunkt (genauer $\Delta_1+\Delta_2$ danach) alle aufgrund neu abgelieferter Listen möglich gewordenen zur Prozedur gehörigen Berechnungen durchgeführt werden, ohne auf weitere Listen zu warten. Zumindest bezüglich derjenigen unter ihnen, die sich als kritisch für die Wartezeit der Benutzer bis zum Rücksetzen ihrer verlorener Geräte herausstellen werden, ist das gerechtfertigt: wenn eine Zusammenfassung von Listen über mehrere Basiszeitpunkte vom Aufwand her günstiger wäre, so sollte man besser a vergrößern, damit Geräte, die die Bank noch nicht benötigt, nicht frühzeitig ungültig werden.

4.3.2.2.2.2 Bearbeiten der WL-Listen

Auch ohne gleichzeitige Systemterminierung wird man asymptotisch den geringsten Gesamtaufwand erreichen, wenn zunächst die langen WL-Listen mit dem geringstmöglichen Aufwand, d.h. durch Vergleich mit einer nach Gerätenummern sortierten Liste VGL verlorener Geräte, zu Listen VL verkürzt werden. Es ist zu betrachten, wann ein bestimmter Teil der WL-Listen, die anfangs nach dem Ablieferungszeitpunkt geordnet sind, bearbeitet werden kann und welche Liste verlorener Geräte dabei genau vorliegen muß.

1. **Wartezeit:** Wird eine Liste WL_G zu einem bestimmten Zeitpunkt t_{WL} abgeliefert, so sind die Geräte G1, mit denen G Transaktionen durchführen konnte, spätestens zum letzten Basiszeitpunkt b_{WL} vor t_{WL} ausgegeben worden, also zur Zeit $b_{WL}+p$ ungültig. Daher steht zur Zeit $b_{WL}+p+\Delta_1+\Delta_2$ fest, ob sie verloren sind (vgl. Bild 11).
2. **Hinteres Ende von VGL:** Nach den Betrachtungen aus 1. müssen, wenn die zu einem Zeitpunkt t_{WL} aus dem Intervall $(b_{WL}, b_{WL}+a]$ abgelieferten WL_G bearbeitet werden, die neuesten in VGL enthaltenen Geräte die mit dem Ungültigkeitstermin $b_{WL}+p$ sein.
3. **Vorderes Ende von VGL:** Andererseits wurde (vgl. wieder Bild 11) G frühestens zur Zeit $t_{WL}-(\Delta_1+\Delta_2)$ ungültig, also, wenn t_{WL} wieder aus $(b_{WL}, b_{WL}+a]$ stammt, genauer frühestens um $b_{WL}+a-(\Delta_1+\Delta_2)$. Daher müssen die ältesten in VGL enthaltenen Geräte den Ungültigkeitstermin $b_{WL}+a-(\Delta_1+\Delta_2)-p+a$ haben. Ältere können gelöscht werden.

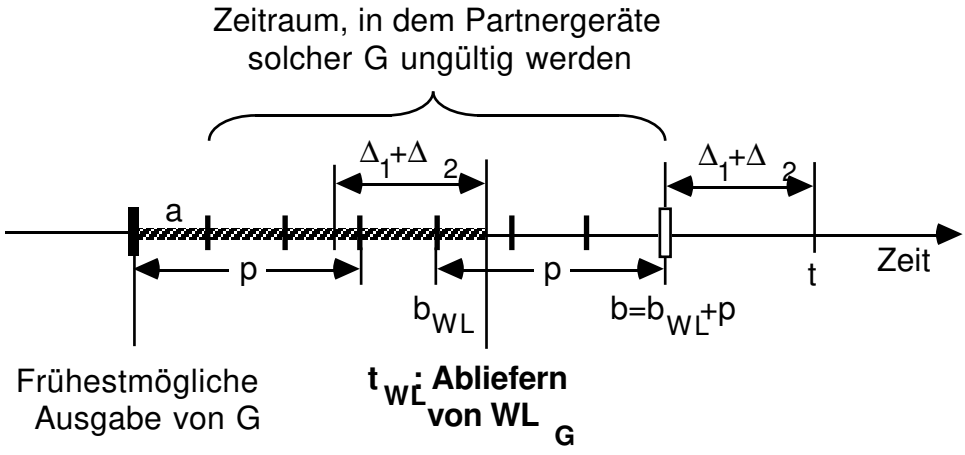


Bild 11 Für das Bearbeiten einer Liste WL_G zu berücksichtigende verlorene Geräte

Alternativ könnte man die gültige Liste VGL vom gerade betrachteten WL_G abhängig machen. Geht man davon aus, daß die Gerätenummern fortlaufend ausgegeben wurden, so besteht diese Auswahl nur in der Bestimmung von Anfang und Ende des gerade nötigen Teiles, der, wenn b_G der genaue Ungültigkeitstermin von G war, die G1 mit Ungültigkeitsterminen von b_G-p+a bis b_G+p-a enthält; für die eigentlich noch gültigen G genügen die von b_G-p+a bis b_{WL}+p.

Wenn man alle abgelieferten Geräte, die eigentlich noch gültig wären, zum Ungültigkeitszeitpunkt b_{WL}+a hinzunimmt, was erlaubt ist, da das dann für sie verwendete VGL das nötige umfaßt, so sind zu jedem Zeitpunkt t_{WL} mögliche Ungültigkeitszeitpunkte genau die Basiszeitpunkte in $[t_{WL}-(\Delta_1+\Delta_2), t_{WL}+a)$. Ist Δ_2 nicht wesentlich größer als a, so sind dies nur wenige, so daß man sogar die Listen WL_G gleich beim Erhalt nach dem Ungültigkeitstermin ablegen könnte, um die Bestimmung von VGL zu vereinfachen.

Da diese Alternativen den Aufwand asymptotisch nicht verringern, wird im folgenden nur das zuerst beschriebene Verfahren weiter behandelt. Damit ergibt sich folgender Anfang für die Schritte der Rücksetzprozedur, die die Bank zu einem Zeitpunkt $t = b+\Delta_1+\Delta_2$, wobei b und somit auch t ein Basiszeitpunkt ist, ausführen muß (b entspricht dem bisherigen b_{WL}+p):

[1] Bestimmung der verlorenen Geräte
- [1.1] Die seit dem vorigen Basiszeitpunkt als nicht verloren gemeldeten Geräte werden nach Gerätenummern (möglichst mit dem Ungültigkeitszeitpunkt als Präfix) in die bisherige Liste nicht verlorener Geräte, NVGL, einsortiert.
- [1.2] Durch Vergleich des den Ungültigkeitszeitpunkt b betreffenden Teils von NVGL mit den Nummern aller ausgegebener Geräte werden die verlorenen Geräte dieses Ungültigkeitszeitpunktes bestimmt und an die bisherige (sortierte) Liste verlorener Geräte, VGL, angefügt, die damit sortiert bleibt.
- [1.3] In NVGL wird der den Ungültigkeitszeitpunkt b betreffende Teil gelöscht.

[2] WL zu VL kürzen:
Es werden diejenigen WL-Listen betrachtet, die im Zeitraum (b-p, b-p+a] abgeliefert wurden, und derjenige Teil von VGL mit den bis b ungültig gewordenen Geräten.
- [2.1] Für jeden Eintrag (G1, N, z) wird G1 in VGL gesucht.
- [2.2] Falls G1 dort gefunden wird, wird der Eintrag (G1, N, z) hinten an VL angefügt, andernfalls gelöscht.

[3] In VGL werden nun die verlorenen Geräte gelöscht, die beim nächsten, mit Ablieferungszeitpunkt b-p+a beginnenden Schritt nicht mehr benötigt werden, d.h. die mit Ungültigkeitszeitpunkt b-p+a-(Δ_1+Δ_2)-p+a.

Protokollskizze 7 Beginn der Rücksetzprozedur zu einem Zeitpunkt b+Δ_1+Δ_2

Der Aufwand dieses Prozedurteils wird nach wie vor vom Durchgehen der WL-Listen, also hier Schritt [2.1] dominiert. Dabei wird jeder WL-Eintrag mit einer etwa doppelt so langen Liste verlorener Geräte verglichen wie bei gleichzeitiger Systemterminierung (nämlich denen eines Zeitraums 2p-a+Δ_1+Δ_2 statt bisher p). Daher ist ein Suchschritt mehr erforderlich. Asymptotisch ist also der Zeitaufwand nach wie vor

$$\Theta(g \bullet p \bullet z \bullet f \bullet \log(p \bullet v \bullet g)).$$

Der Speicheraufwand ist im wesentlichen der für die WL-Listen einer Periode benötigte; da deren Verarbeitung aber nur sequentiell erfolgt, muß es sich nicht um einen Hauptspeicher handeln. Würden die ungültigen Geräte physisch abgeliefert, könnte die Speicherung sogar einfach in der Aufbewahrung dieser Geräte bestehen.

Für das weitere Vorgehen, d.h. das Herausfiltern der Einträge, die verlorene Standardwerte betreffen, aus den VL, gibt es analog zu 4.3.2.2.1 zwei Verfahren.

4.3.2.2.2.3 Verfahren 1: Vorsortieren der WL-Listenreste

Bei diesem Verfahren werden gewisse VL-Listen nach der Nummer der Standardwerte sortiert und in der resultierenden Liste Einträge, die nicht verlorene Standardwerte betreffen, anhand eines einmaligen Durchgangs durch BL_B (das nach dem Entstehungszeitpunkt geordnet ist) gestrichen. Dabei ist zum einen zu betrachten, wann ein zu einer bestimmten Zeit entstander Teil von BL_B bearbeitet werden kann, zum anderen, mit welchen VL-Einträgen er zu vergleichen ist. Daraus ergibt sich auch, wann welche Teile von VL fertig behandelt sind.

Wird der zu einem Zeitpunkt t_{BL} entstandene Teil von BL_B bearbeitet, so sind die betroffenen Einträge in WL-Listen dadurch gekennzeichnet, daß sie Standardwerte betreffen, die zu dieser Zeit der Bank zurückgebracht werden können.

1. **Wartezeit:** Da die betroffenen WL-Einträge vor t_{BL} entstanden sind, wird das sie enthaltende Gerät spätestens um die Zeit p nach dem letzten Basiszeitpunkt b_{BL} vor t_{BL} ungültig, also spätestens zur Zeit $t_{WL}=b_{BL+p}+\Delta_1+\Delta_2$ abgeliefert.

   Bis sie zu VL verarbeitet sind, muß man gemäß 4.3.2.2.2.2 und weil t_{WL} selbst Basiszeitpunkt ist, also $t_{WL}=b_{WL}$+a, dann noch einmal p-a+Δ_1+Δ_2 warten.

   Die Bearbeitung kann also für den im Zeitraum (b_{BL}, b_{BL}+a] entstandenen Teil von BL_B um b_{BL}+2p-a+2(Δ_1+Δ_2) erfolgen.
2. **Hintere Grenze von VL:** Die betroffenen Standardwerte müssen zur Zeit t_{BL} und, äquivalent dazu, auch zur Zeit b_{BL}, schon gültig gewesen sein.
3. **Vordere Grenze von VL:** Andererseits können die Standardwerte, die gerade zurückgebracht werden, nur so alt sein, daß zur Zeit t_{BL}-Δ_1-Δ_2 noch ein zu ihrem kleinen Zahlungssystem gehörendes Gerät gültig war (vgl. Bild 12), also auch noch zum nächsten Basiszeitpunkt b" ab t_{BL}-Δ_1-Δ_2. (Dabei ist b"=b_{BL}-Δ_1-Δ_2+a.) Sie wurden also frühestens um p+p'-a vor b" ausgegeben.

Die Einträge in VL, die ältere Standardwerte betreffen, können also zum Gutschreiben verwendet und dann gelöscht werden.

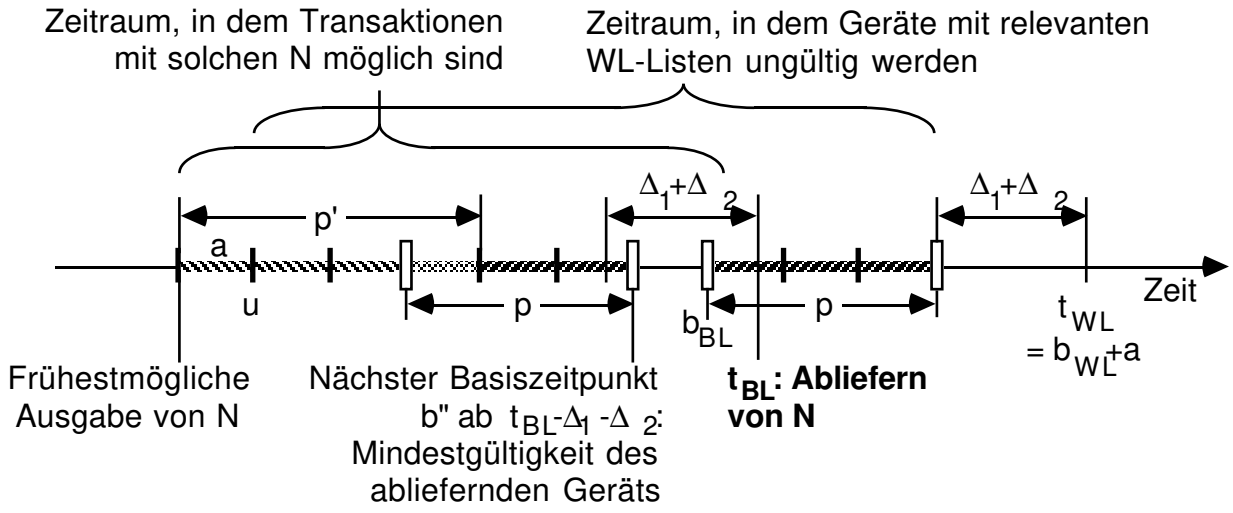


Bild 12 Beim Bearbeiten eines Teils von BL_B zu berücksichtigende Teile der VL-Listen

Damit ergibt sich folgende Fortsetzung der Rücksetzprozedur aus 4.3.2.2.2.2 zu einem Zeitpunkt $t=b+\Delta_1+\Delta_2$, wobei b und t Basiszeitpunkte sind:

[4] Erstellen der passenden VL-Liste:

[4.1] Der neue, d.h. in Schritt [2] entstandene, Teil von VL wird in den bisherigen (sortierten) einsortiert, wobei von mehreren Einträgen zum selben Standardwert jeweils nur der neueste behalten wird.

[4.2] Sei $b_{BL}=b-2p+a-(\Delta_1+\Delta_2)$.
Weiter betrachtet wird zu diesem Zeitpunkt nur der Teil von VL, der Standardwerte betrifft, die bis b_{BL} ausgegeben wurden. Sind die Standardwerte fortlaufend numeriert ausgegeben, so befindet sich dieser Teil zusammenhängend am Anfang von VL.

[5] Behandlung des Teils von BL_B, der im Zeitintervall $(b_{BL}, b_{BL}+a]$ entstand:

[5.1] Für jeden darin enthaltenen Standardwert N wird gesucht, ob er in einem Eintrag von VL vorkommt.

[5.2] Wenn ja, wird jener Eintrag aus VL gelöscht (bzw. als zu löschen gekennzeichnet und am Schluß in einem Durchgang gelöscht).

[5.3] Der betrachtete Teil von BL_B wird gelöscht.

[6] Behandlung des Restes von VL:
Es können die Einträge (G1, N, z) endgültig bearbeitet werden, für die N zum nächsten von BL_B behandelten Zeitpunkt, also nach $b_{BL}+a$, nicht mehr betrachtet werden muß.

Setze $b"=b_{BL}-(\Delta_1+\Delta_2)+a$. Dann sind genau die Einträge, für die N zur Zeit b"–p–p'+a ausgegeben wurde, zu löschen. Dies ist wieder ein fortlaufender Anfang von VL.

[6.1] Für jeden Eintrag (G1, N, z) wird N dem Gerät G1 gutgeschrieben.

[6.2] Dann wird dieser Eintrag aus VL gelöscht.

[7] Obwohl die Bank hierzu nicht unbedingt etwas Gesondertes tun muß, sei erwähnt, daß nun diejenigen verlorenen Geräte vollständig rückgesetzt sind, für die alle N, die sie besitzen konnten, gutgeschrieben sind, d.h. für deren Ungültigkeitszeitpunkt u gilt, daß u-a ≤ b"–p–p'+a , d.h. u ≤ t-p'-3p-3(Δ_1+Δ_2)+4a.

Protokollskizze 8 Fortsetzung 1 der Rücksetzprozedur zu einem Zeitpunkt b+Δ_1+Δ_2

Der Aufwand wird wieder für eine Periode der Länge p betrachtet.

1. **Schritt [4]:** Der Aufwand für das Einsortieren unterscheidet sich, unabhängig von a, vom reinen Sortieraufwand bei gleichzeitiger Systemterminierung asymptotisch nur durch die Länge *l* der Liste VL, die jeweils vorliegt. Einerseits kann ja der Aufwand für das Erzeugen einer sortierten Liste durch die Verteilung auf mehrere Zeitpunkte nicht abnehmen, andererseits ist der Aufwand bei geeigneter Organisation selbst dann noch $\Theta(l \bullet \log(l))$ pro Periode, wenn jeder Eintrag einzeln einsortiert wird.

   Da die Standardwerte, auf die sich die Einträge beziehen, frühestens (vgl. Bild 12) zum Zeitpunkt b"-p-p'-a = b-p'-3p+3a-2(Δ_1+Δ_2) und spätestens (vgl. Bild 11) zum Zeitpunkt b_{WL} = b-p ausgegeben wurden, stammen sie aus einem Zeitraum der Länge p'+2p-3a+2(Δ_1+Δ_2) statt früher p. Also ist VL höchstens etwa um den Faktor p'/p+2 größer als bisher, und der Aufwand dieses Schrittes beträgt höchstens

   $$\Theta(g \bullet p' \bullet z \bullet f \bullet (p \bullet v)/2) \bullet \log(g \bullet p' \bullet z \bullet f \bullet (p \bullet v)/2)).$$

   Die folgende Auswahl der Grenze des in Schritt 5 zu betrachtenden Teils ist zu vernachlässigen.
2. **Schritt [5]:** Hier ist es sofort klar, daß sich der Aufwand vom entsprechenden bei gleichzeitiger Systemterminierung nur durch die Länge der Liste VL unterscheidet, in der jeder BL-Eintrag gesucht wird. Da nun die neuesten vorkommenden Standardwerte von b_{BL}≈b-2p stammen, ist dieser VL-Teil höchstens etwa um den Faktor p'/p+1 länger als bisher. Daher ist der Aufwand dieses Teilschrittes pro Periode höchstens

   $$\Theta(n \bullet \log(g \bullet p' \bullet z \bullet f \bullet (p \bullet v)/2)).$$
3. **Schritt [6]:** Dieser ist schon im Vergleich zu Schritt [4] zu vernachlässigen, denn er besteht nur aus einem Durchgang durch die Liste, da die zu einem Zeitpunkt zu betrachtenden Einträge fortlaufend am Anfang von VL stehen.

Wie man sieht, überwiegt wieder der Aufwand beim Durchgehen von BL_B.

Der Gesamtaufwand hat sich asymptotisch nicht geändert, sofern p' nur um einen konstanten Faktor größer als p ist (und dann auch praktisch nicht sehr, da im bei Verwendung dieses Verfahrens größerenTerm nur der Logarithmus von p' vorkommt). Diese Annahme ist auch sinnvoll, da p' wie p in die Wartezeit der Benutzer bis zum Rücksetzen verlorener Geräte eingeht.

Im anderen Fall kann man sich noch fragen, ob durch eine genauere Abschätzung der Länge von VL die Abhängigkeit von p' zu beseitigen wäre, denn es sind ja in VL nicht (wie oben gezählt) alle Transaktionen verlorener Geräte mit Standardwerten, die in dem betrachteten Zeitraum ausgegeben wurden, enthalten (je nach der Länge von p' können die neueren dieser Standardwerte sogar noch gültig sein). Die Liste enthält aber in jedem Fall Vermerke über alle Transaktionen mit verlorenen Geräten, die in einem Zeitraum der Länge p' endend bei b_{BL} über solche Standardwerte entstanden, die frühestens mit Ende dieses Zeitraums abgeliefert wurden (denn diese sind einerseits schon einsortiert, da das speichernde Gerät G bis b_{BL}+p-a, also noch vor den Geräten, nach denen sich die

Wartezeit bestimmt, ungültig wurde, und andererseits noch nicht gelöscht, da der sie betreffende Teil von BL_B noch nicht bearbeitet ist). Letzteres trifft im Mittel auf die Hälfte aller Transaktionen mit verlorenen Geräten in diesem Zeitraum zu, also auch bereits auf g•p'•z•f•(p•v)/4.

4.3.2.2.2.4 Verfahren 2: Vorsortieren von BL_B

Bei diesem Verfahren wird zunächst ein gewisser Teil von BL_B nach den Nummern der Standardwerte sortiert und daraus eine Liste VSL verlorener Standardwerte bestimmt. Dann werden bei einem einmaligen Durchgang durch VL diejenigen Vermerke, die sich auf Standardwerte aus VSL beziehen, bestimmt und dort eingetragen.

Für beide Teilschritte sind wieder die Wartezeiten und die Grenzen der Listen, mit denen verglichen wird, zu betrachten.

A. Genaue Bearbeitung von BL_B: Für das Einsortieren der neuen BL_B-Einträge muß auf nichts gewartet werden. Welche der Standardwerte eines bestimmten Ungültigkeitszeitpunktes b_{Ung} verloren sind, ergibt sich genau aus dem zu diesem Zeitpunkt gehörenden Teil von BL_B (der zusammenhängend ist, wenn man wieder annimmt, daß die Nummern der Standardwerte aufsteigend vergeben werden).

Da die letzten Geräte, die diese Standardwerte besitzen können, zur Zeit b_{Ung}-a ausgegeben wurden, werden sie spätestens zur Zeit $t:=b_{Ung}-a+p+\Delta_1+\Delta_2$ abgeliefert. Zu diesem Zeitpunkt kann also der Vergleich mit den Nummern aller Standardwerte des Ungültigkeitszeitpunktes b_{Ung} erfolgen und dann der entsprechende Teil von BL_B gelöscht werden.

B. Genaue Bearbeitung von VL: Die VL_G sind gemäß 4.3.2.2.2.2 nach dem Abgabezeitpunkt t_{VL} von G sortiert, VSL nun nach den Nummern der Standardwerte.

1. **Wartezeit:** Einerseits muß natürlich gewartet werden, bis die VL_G überhaupt aus den WL_G erstellt worden sind, nach 4.3.2.2.2.2 also bis $b_{VL}+p+\Delta_1+\Delta_2$, wenn b_{VL} der letzte Basiszeitpunkt vor t_{VL} ist.

   Andererseits muß ein Standardwert, der in VL_G erwähnt wird, spätestens zur Zeit b_{VL} ausgegeben, also zur Zeit $b_{Ung}=b_{VL}+p'$ ungültig geworden sein (vgl. Bild 13). Die benötigte Liste VSL liegt nach A. also zum Zeitpunkt $b_{VL}+p'+p-a+\Delta_1+\Delta_2$ vor.

   Da der zweite Zeitpunkt später ist, kann insgesamt die Bearbeitung der VL_G, die aus den im Zeitraum $(b_{VL}, b_{VL}+a]$ abgelieferten WL_G hervorgingen, zum Zeitpunkt $t=b_{VL}+p'+p-a+\Delta_1+\Delta_2$ erfolgen.
2. **Hintere Grenze von VSL:** Aus 1. geht bereits hervor, daß die neuesten aus VSL zu betrachtenden Standardwerte bei der Bearbeitung der VL_G aus dem Zeitraum $(b_{VL},b_{VL}+a)$ das Ungültigkeitsdatum $b_{Ung}=b_{VL}+p'$ haben müssen. Dies sind ohnehin die neuesten darin enthaltenen, so daß keine Teilliste ausgewählt werden muß.
3. **Vordere Grenze von VSL:** Andererseits wurde (vgl. wieder Bild 13) G frühestens zur Zeit $t_{VL}-(\Delta_1+\Delta_2)$ ungültig, also, wenn t_{VL} wieder aus $(b_{VL}, b_{VL}+a]$ stammt, genauer frühestens um $b_{VL}+a-(\Delta_1+\Delta_2)$. Daher müssen die ältesten in VSL enthaltenen Standardwerte den Ungültigkeitstermin $b'=b_{VL}+a-(\Delta_1+\Delta_2)-p+a$ haben. Ältere können gelöscht werden.

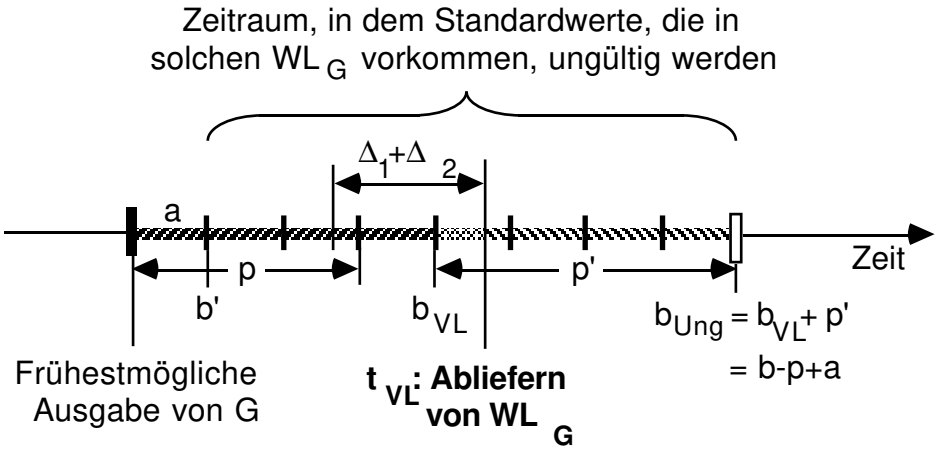


Bild 13 Für das Bearbeiten einer Liste VL_G zu berücksichtigende Standardwerte

Damit ergibt sich folgende Fortsetzung der Rücksetzprozedur aus 4.3.2.2.2.2 zu einem Zeitpunkt $t=b+\Delta_1+\Delta_2$, wobei b und t Basiszeitpunkte sind:

[4] Bestimmung verlorener Standardwerte:

[4.1] Alle seit dem vorigen Zeitpunkt entstandenen BL-Einträge werden in die vorige (sortierte) Liste BL einsortiert.

[4.2] Nun werden die verlorenen Standardwerte des Ungültigkeitszeitpunktes $b_{Ung}=b–p+a$ bestimmt. Dazu wird in einem Durchgang der zu b_{Ung} gehörige Teil von BL_B auf fehlende Nummern getestet. Diese werden an die (sortierte) Liste VSL verlorener Standardwerte angefügt, die damit sortiert bleibt.

[4.3] Der bearbeitete Teil von BL_B wird gelöscht.

[5] Kürzung von VL auf verlorene Standardwerte:
Setze $b_{VL}=b-p'-p+a$. Es werden die im Zeitraum $(b_{VL}, b_{VL}+a]$ abgelieferten VL_G betrachtet.

[5.1] Für jeden Eintrag (G1, N, z) wird gesucht, ob N in VSL steht.

[5.2] Wenn ja, wird (G1, z) zu diesem N in VSL eingetragen, es sei denn, dort befände sich bereits ein Eintrag (G2, z') mit z'>z.

[5.3] Die bearbeiteten VL werden gelöscht.

[6] Gutschreiben:

[6.1] Die Standardwerte des Teils von VSL, der zum nächsten Zeitpunkt nicht mehr betrachtet werden muß, d.h. die mit Ungültigkeitstermin $b'=b_{VL}+a-(\Delta_1+\Delta_2)-p+a$, werden dem nun in VSL dazu eingetragenen G1 gutgeschrieben.

[6.2] Dieser Teil von VSL wird gelöscht.

[7] Wieder sei erwähnt, daß nun die verlorenen Geräte vollständig rückgesetzt sind, für die alle N, die sie besitzen konnten, gutgeschrieben sind, d.h. für deren Ungültigkeitszeitpunkt u gilt, daß $u \le b'–p'+a = b-2p'-2p-(\Delta_1+\Delta_2)+4a$.

Protokollskizze 9 Fortsetzung 2 der Rücksetzprozedur zu einem Zeitpunkt $b+\Delta_1+\Delta_2$

Der Aufwand wird wieder für eine Periode der Länge p betrachtet, und es ist nach wie vor offensichtlich, daß alle übrigen Schritte gegen das Sortieren von BL oder das Durchgehen der VL (also Schritte [4.1] bzw. [5.1]) zu vernachlässigen sind.

1. **Schritt [4.1]:** Der Aufwand für das Einsortieren der BL-Teile unterscheidet sich vom entsprechenden bei gleichzeitiger Systemterminierung nur durch die Länge der jeweils vorliegenden Liste BL (vgl. Aufwand für Schritt [4] in 4.3.2.2.2.3).

   In dieser befinden sich höchstens Standardwerte mit Ungültigkeitszeitpunkten von b_{Ung}=t–(Δ_1+Δ_2)-p+a bis t+p'-a, also aus einem Zeitraum der Länge p'+p+(Δ_1+Δ_2)-a statt bisher t, so daß der Aufwand O(p'/p•n • log(p'/p•n)) ist.

   Dieser Aufwand kann allerdings reduziert werden, indem die Bank nicht alle abgegebenen Standardwerte im selben BL_B ablegt, sondern nur solche sortiert, die schon ungültig sind oder bald ungültig werden. Heißt „bald" beispielsweise „innerhalb der Zeit p", so sind in BL nur Standardwerte mit Ungültigkeitszeitpunkten von b_{Ung} bis t+p, also aus einem Zeitraum der Länge 2p+(Δ_1+Δ_2), so daß der Aufwand wie bei gleichzeitiger Systemterminierung

   $$\Theta(n \bullet \log(n))$$

   beträgt.
2. **Schritt [5.1]:** Der Aufwand unterscheidet sich vom bisherigen nur durch die Länge der Liste VSL, in der jeder Eintrag gesucht wird. Diese enthält die verlorenen Standardwerte der Ungültigkeitszeitpunkte von b' bis b_{Ung}, also aus einem Zeitraum p'+p+Δ_1+Δ_2-a statt bisher p. Sie ist also etwa um den Faktor p'/p+1 länger als bisher, und der Aufwand beträgt nun

   $$\Theta(g \bullet p \bullet z \bullet f \bullet (p \bullet v)/2 \bullet \log(p' \bullet v \bullet n))$$

4.3.2.2.2.5 Abschließende Bemerkungen

Die Diskussion aus 4.3.2.2.1, wann welches der beiden Verfahren zu bevorzugen ist und ob tatsächlich das Durchgehen der WL-Listen, nach dem optimiert wurde, den Hauptaufwand verursacht, gilt im wesentlichen nach wie vor, insbesondere natürlich dann, wenn p' sich nur um einen kleinen Faktor von p unterscheidet. Da zudem konkrete Ergebnisse ohne genauere Kenntnis der Parameter nicht zu erhalten sind, sei hier auf eine Anpassung der dortigen Ergebnisse verzichtet.

Je nach den konkreten Parametern kann auch die am Ende von 4.3.2.2.1 erwähnte Variante des zweiten Verfahrens, bei der nicht nur das Sortieren von BL_B, sondern auch das anfängliche Durchgehen der WL-Listen durch Indizieren in einer Reihung R über sämtliche ausgegeben Standardwerte ersetzt wird, günstig sein. Dieses ist wesentlich einfacher als die bisher beschriebenen:

1. **Wartezeit:** Sämtliche zu einem Zeitpunkt t abgelieferten Standardwerte und WL-Listen können sofort eingeordnet werden.

   Sei nun N ein verlorener Standardwert mit einem Ungültigkeitszeitpunkt b*. Daß N verloren ist, steht fest, sobald alle Geräte, die N besitzen könnten, d.h. die bis b*-a ausgegeben wurden, abgeliefert sind, also zur Zeit t=b*-a+p+Δ_1+Δ_2.

   Da auch Vermerke über N nur in diesen Geräten sein können, steht zur selben Zeit t fest, welchem Gerät N gutgeschrieben wird.
2. **Hinteres Ende von R:** Selbst wenn noch gültige Standardwerte wie in 4.3.2.2.2.4 nicht einsortiert werden, so können doch über sie bereits Vermerke abgegeben werden, so daß R sich bis zu den neuesten ausgegebenen Standardwerten erstrecken muß.
3. **Vorderes Ende von R:** Nach 1. sind die ältesten in einem Zeitraum (b,b+a] noch in R nötigen Standardwerte die des Ungültigkeitszeitpunktes b* mit t=b+a, d.h. b*=b–p+2a–(Δ_1+Δ_2).

R umfaßt also Standardwerte eines Zeitraums a+(b+p')-b*=p'+p-a+Δ_1+Δ_2, hat also etwa die Länge

$$(p'/p+1) \bullet n.$$

Dies bestimmt vor allem den Hauptspeicheraufwand dieses Verfahrens.

Der Zeitaufwand ist weniger interessant, denn das Durchgehen der WL-Listen, obwohl praktisch schnell, erfordert asymptotisch den Aufwand

$$\Theta(g \bullet p \bullet z \bullet f \bullet \log(n)),$$

der höher als der der anderen Verfahren ist.

Optimal ist bei diesem Verfahren die Wartezeit bis zum vollständigen Rücksetzen eines verlorenen Gerätes, da sämtliche der Bank vorliegende Information sofort verarbeitet wird: p'-a nach dessen Ungültigkeitszeitpunkt sind alle in Frage kommenden Standardwerte ungültig, so daß zusammen mit der Zeit $p-a+\Delta_1+\Delta_2$ aus 1. die gesamte Wartezeit $p'+p-2a+\Delta_1+\Delta_2$ beträgt.

Eine Zusammenfassung der Bewertung aller Verfahren dieses Kapitels 4 findet sich nach der Erweiterung dieser Verfahren um Anonymität in den Bildern 21 bis 23.

5 Anonymisierung

In Kapitel 4 wurden Verfahren zur verteilten Änderungsaufzeichnung vorgestellt und deren Sicherheit diskutiert. Im folgenden soll betrachtet werden, wie die Verfahren so realisiert werden können, daß sie weiterhin die dort gezeigten Sicherheitseigenschaften besitzen, aber die Anonymität der Teilnehmer gewahrt bleibt. (Für eine genauere Diskussion von Anonymität sei nochmals auf [PWP_87] verwiesen.)

Hierzu soll in 5.1 kurz diskutiert werden, welche Angreifermodelle zugrunde zu legen sind. Sodann werden in 5.2 Lösungen für die aufgezeigten Probleme in möglichst allgemeiner Form angegeben. In 5.3 schließlich werden die anonymisierten Protokolle der Verfahren aus Kapitel 4 angegeben und die Komplexitätszunahme durch die Anonymisierung bewertet.

5.1 Angreifermodelle

Ziel eines Angriffs auf die Anonymität ist es, aus (regulär oder irregulär) erhaltenen Informationen auf den Zahlungsfluß zwischen den Teilnehmern des Zahlungssystems zu schließen, d.h. festzustellen, wer wann an wen wieviel bzw. welches Geld gezahlt hat (und im weiteren Sinne auch „weshalb", d.h. in welchem Zusammenhang, aber das ist nicht mehr direkt ein Angriff auf das Zahlungssystem).

Im folgenden werden nur durch die Verlusttoleranz neu hinzukommende Informationen betrachtet. Hinsichtlich der „normalen" Daten, die während jeder Zahlung anfallen, insbesondere bei den Rahmenprotokollen (d.h. für Initialisierung, Identifikation der Besitzer gegen ihre Geräte und der Geräte untereinander) sei auf Kapitel 2 verwiesen; wiederholt sei, daß die Geräte dazu keine Identität benötigten. Daneben kann es noch Kontextwissen geben, etwa erhalten durch direkte Beobachtung eines Benutzers bei der Bezahlung mittels seiner elektronischen Brieftasche.

Da die Kommunikation zwischen sicheren Geräten sowie die zwischen sicheren Geräten und der Bank als nicht abhörbar angenommen werden kann (indem sie geeignet mit nur sicheren Geräten bzw. nur sicheren Geräten und der Bank bekannten Schlüsseln verschlüsselt wird), und durch Verwendung eines Datenschutz garantierenden Kommunikationsnetzes [PfPW_86] (vgl. Kap. 2) auch die Verkehrsdaten dieser Kommunikation vor Außenstehenden geschützt werden können (z.B. die Länge der Aufzeichnungen der Geräte bestimmter Personen), verbleiben als mögliche Angreifer nur diejenigen, die gemäß Protokoll Verlusttoleranzinformationen erhalten, also einerseits die Besitzer sicherer Geräte (z.B. zum Zwecke der Sicherheit gegen Betrugsversuche der Bank, vgl. jeweils die Schlußabschnitte von 4.2.1.1 und 4.3.1.5), andererseits natürlich die Bank.

Man kann sich jedoch (mit geringen Einschränkungen) auf unsichere Bankgeräte als die einzigen zu betrachtenden Angriffspunkte beschränken:

Ein normaler Besitzer B_G eines sicheren Gerätes G kann Informationen über andere Geräte aus drei Quellen erhalten: beim Erhalt der Vermerke eines lokalen Rücksetzpunktes G^*, bei der „Nachrechnung" des Rücksetzergebnisses der Bank und bei der Übergabe der Änderungsaufzeichnung von G an die Bank.

Die erste Quelle läßt sich sinnvoll schließen, indem nur Rücksetzpunkte mit lokaler Sicht erlaubt werden: das Gerät G^*, das als Rücksetzpunkt für G dienen soll, wird G fest zugeordnet und nimmt nur Transaktionen mit G vor. Damit ist klar, daß G^* alle G direkt betreffenden Vermerke von G selbst erhalten haben muß und es diese Vermerke getrost an B_G übergeben kann. Alle G nicht direkt betreffenden Vermerke sind für die Kontrolle der Bank durch B_G irrelevant, so daß G^* sie nicht an B_G übergeben muß (wohl aber an die Bank!). Alternativ hierzu könnte man auch einen Rücksetzpunkt

G^* verwenden, der zwar immer noch fest G zugeordnet ist und nur G betreffende Änderungsvermerke an B_G übergibt, der aber auch mit anderen Geräten Transaktionen vornehmen kann. Damit kann natürlich der Fall auftreten, daß G^* Änderungsvermerke über G von anderen Geräten erhält und an B_G übergibt, was aber keine ersichtliche praktische Bedeutung für die Anonymität anderer Geräte hat.

Bei der Nachrechnung des Rücksetzergebnisses befindet sich jedes nachrechnende Gerät (oder auch jede „Kontrollbank") in derselben Situation wie die eigentliche Bank, so daß auch gleich diese als Angreifer betrachtet werden kann.

Um jedoch die Anonymität der Besitzer verlorener Geräte vor anderen Teilnehmern in dem Fall, daß die Bank nicht angreift (was natürlich der wahrscheinliche ist), nicht gar zu sehr zu schmälern, erscheint es sinnvoll, die Fähigkeit des Nachrechnens der gesamten Rücksetzprozedur einigen wenigen „Kontrollbanken" zu überlassen. Zur Überprüfung des Rücksetzergebnisses für ein einzelnes verlorenes Gerät G durch B_G anhand des lokalen Rücksetzpunktes G^* sind bei den Weitergabeverfahren ohnenhin nur von G selbst erzeugte Vermerke relevant, so daß hier keines anderen Besitzers Anonymität geschmälert wird. Bei den markierten Standardwerten muß die Bank lediglich zu jedem Standardwert, den G gemäß G^* besitzen könnte, aber gemäß der gesamten Änderungsaufzeichnung nicht mehr besitzt, einen weiteren Vermerk als Beweis vorlegen.

Die potentielle Gefahr der dritten Quelle ist dieselbe wie die der ersten: aus der speziellen Zusammensetzung der Änderungsaufzeichnung des eigenen Gerätes könnte ein Besitzer B_G Rückschlüsse auf seine Zahlungspartner ziehen. Dieselben Schlüsse (wenn vielleicht auch mit weniger Interesse) könnte aber auch die Bank ziehen, wenn sie die Änderungsaufzeichnung von G im Zusammenhang erhält. Damit ist auch dieses Problem auf den Schutz vor der Bank reduziert.

Im folgenden werden daher „Bank" und „Angreifer" synonym verwendet werden. Die noch zu betrachtenden möglichen Informationsquellen des Angreifers sind damit (vgl. Bild 14):

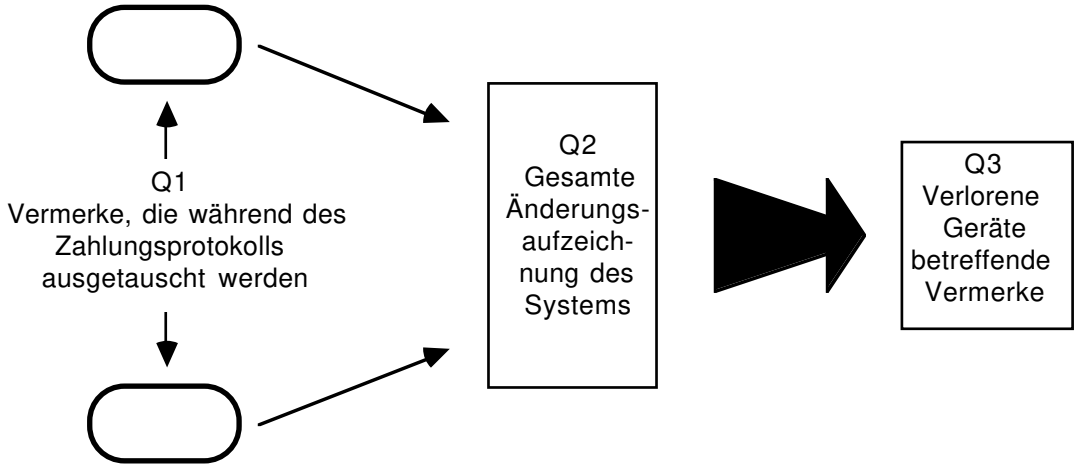


Bild 14 Informationsquellen des Angreifers

Q1 Die Änderungsvermerke, wie sie die Transaktionspartner während des Zahlungsprotokolls austauschen.

Q2 Die gesamte Änderungsaufzeichnung des Systems, die von allen Geräten gemeinsam angefertigt wird und aus der die zum Rücksetzen notwendigen, also verlorene Geräte betreffenden, Vermerke ausgewählt werden müssen. Sie wird im nicht anonymen Fall bei Ungültigwerden der Geräte an die Bank übergeben.

Q3 Diejenigen Vermerke aus der gesamten Änderungsaufzeichnung, die zum Rücksetzen der verlorenen Geräte notwendig sind. Dies sind in den in Kapitel 4 beschriebenen Verfahren jeweils die von den verlorenen Geräten selbst erzeugten.

Erhält der Angreifer aus einer dieser Quellen Vermerke, so kann er natürlich zusätzlich auch versuchen, aus den Begleitumständen der Übergabe der Vermerke an eines seiner Geräte Schlußfolgerungen zu ziehen. (In Analogie zur Situation bei Kommunikationsnetzen kann man also auch hier zwischen den Inhaltsdaten, den eigentlichen Vermerken, und den Verkehrsdaten, den Begleitumständen der Übergabe, unterscheiden.)

Die Ausschöpfung der drei Quellen durch den Angreifer muß durch gerätetechnische oder kryptographische Techniken verhindert werden. Beide sollen im folgenden als im idealen Sinne „sicher" betrachtet werden (vgl. Kap. 1).

Da es wenig sinnvoll erscheint, in obiger Auflistung dem gerätetechnischen Schutz eines Punktes Qi zu vertrauen, wenn dem Schutz des Punktes Qi-1 nicht ebenfalls vertraut wird, gibt es je nach dem Vertrauen, das man in den Schutz durch sichere Geräte setzt, vier sinnvolle Angreifermodelle (vgl. Bild 15).

A0. Das einfachste, vertrauensseligste Angreifermodell geht davon aus, daß alle drei Quellen durch sichere Geräte geschützt sind. Da der Angreifer damit überhaupt keine Informationen erhält (auch keine Verkehrsdaten), sind alle in Kapitel 4 beschriebenen sicheren Verfahren bereits anonym. Daher braucht dieses Modell im folgenden nicht weiter betrachtet zu werden.

Die „Realisierung" des Modells erfordert, daß ein sicheres Gerät nur mit von ihm geprüften echten Geräten kommuniziert und das gesamte Rücksetzprotokoll der Bank (Einsammeln der Änderungsaufzeichnungen, Rücksetzen verlorener Geräte) ebenfalls von einem sicheren Bankgerät ausgeführt wird, das die Rücksetzinformationen auch vor der Bank geheimhält. Dies setzt allerdings voraus, daß die Bankgeräte ebenso sicher gebaut werden können wie „elektronische 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.

A1. Das nächst kompliziertere Angreifermodell erhält man, wenn zwar die Rücksetzdaten über nicht verlorene Geräte immer noch durch sichere Geräte vor dem Angreifer geschützt sind, aber die Bank zum Rücksetzen die Vermerke über verlorene Geräte erhält und diese (sinnvollerweise durch unsichere Geräte, bei denen damit die Probleme aus A0 nicht auftreten) zurücksetzt.

Mit anderen Worten: die Quellen Q1 und Q2 sind immer noch durch sichere Geräte zu schützen, was erfordert, daß ein sicheres Gerät von einem Kommunikationspartner feststellen kann, ob es sich ebenfalls um ein sicheres Gerät handelt, und daß auch die Bank das Zahlungsprotokoll nur mittels sicherer Geräte ausführen kann. Dies läßt sich durch die Annahme rechtfertigen, daß die sicheren Benutzergeräte durch von der Bank unabhängige und im Ganzen betrachtet vertrauenswürdige Organisationen hergestellt werden (vgl. Kap. 1), und die Authentikation eines Partners als sicheres Gerät völlig von der als elektronische Brieftasche getrennt werden kann.

Die Quelle Q3 kann bezüglich ihrer Inhalte nicht geschützt werden, da die Bank diese zum Rücksetzen benötigt; zu schützen sind hier nur die entstehenden Verkehrsdaten. Die Anonymität der Besitzer verlorener Geräte ist daher ab dem Angreifermodell A1 mit verloren. Genauer: die Bank erfährt das, was in den Vermerken steht (also die Anzahl und Höhe der Transaktionen und ggf. die

markierten Standardwerte, nicht aber unbedingt die Transaktionspartner). Dazu weiß sie das Pseudonym des Besitzers B_G, unter dem dieser das verlorene Gerät G besaß, insbesondere dasjenige andere Gerät oder Konto, auf das er das Geld nach dem Rücksetzen erhalten möchte, nicht aber unbedingt den Namen von B_G und alle weiteren Geräte und Konten, die er besitzt.

Mittels Kontextwissens kann sie manchmal sogar den Namen von B_G erhalten: Als Beispiel nehme man beim Verfahren der markierten Standardwerte an, ein Gerät der Bank (oder eines mit ihr verbündeten Benutzers) habe genau einen Standardwert N des Betrages b gezahlt, und zwar an das später verloren gegangene Gerät G. Da die Bank sich selbst gegenüber behaupten kann, ihr Gerät sei verloren, muß sie natürlich alle Vermerke über ihr eigenes Gerät auswerten können, insbesondere denjenigen, der die Weitergabe des Standardwerts N (gekennzeichnet durch den Betrag b) an ihr Gerät vermerkt. Aus allen Vermerken über verlorene Geräte kann die Bank damit auch denjenigen heraussuchen, der die nächste Weitergabe, eben die von ihrem Gerät an das verlorene Gerät G, bezeichnet. Damit kann sie B_G mit dem Partner in einer bestimmten Transaktion gleichsetzen; kennt sie diesen Partner namentlich, so ist B_G deanonymisiert.

Eingeschränkt gilt die Kritik an A0 auch an A1: Die sicheren Geräte müssen das Auswählen der zum Rücksetzen wichtigen Vermerke übernehmen. Genau dies verursacht aber in den Verfahren aus Kapitel 4 den Haupaufwand der Rücksetzprozedur (wenn auch zumeist die von sicheren Geräten zu behandelnden Listen erheblich kürzer sein werden als die gesamte Änderungsaufzeichnung und sich somit die Last auf alle Geräte verteilt) und erfordert sehr kommunikationsaufwendige Verfahren zum Bekanntmachen der verlorenen Geräte und zum Einsammeln der diese betreffenden Vermerke. Die sicheren Geräte der Bank sollten natürlich nochmals leistungsfähiger als normale Benutzergeräte sein, denn sie müssen sicher mehr Transaktionen vornehmen als diese. Ebenso sollten sie zur Erhöhung der Verlusttoleranz zuverlässiger als diese gebaut sein. All dies bedeutet, daß im Vergleich zum nicht anonymen Fall die normalen Benutzergeräte und erst recht die sicheren Bankgeräte wiederum komplexer werden müssen.

Daher ist es sinnvoll, auch für stärkere Angreifermodelle Schutzmaßnahmen zu suchen.

A2. Im nächststärkeren Angreifermodell ist nun neben Q3 auch die Gesamtheit der Rücksetzinformationen, also die Quelle Q2, nicht mehr durch sichere Geräte geschützt, d.h. die Bank erhält wie im nicht anonymen Fall beschrieben von allen sicheren Geräten bei deren Ungültigwerden deren Änderungsaufzeichnung (wenn auch möglicherweise in kryptographisch geschützter Form), wählt die verlorene Geräte betreffenden Vermerke hierunter aus und setzt mittels unsicherer Geräte die verlorenen zurück. Die während einer Zahlung ausgetauschten Vermerke sind jedoch noch immer durch sichere Geräte geschützt, so daß auch hier die Bank für Zahlungen sichere Geräte verwenden muß.

Die Voraussetzungen für die Anwendbarkeit von A2 sind ziemlich dieselben wie die für A1, jedoch müssen die sicheren Geräte nicht mehr die Auswahl der verlorene Geräte betreffenden Vermerke übernehmen, so daß die Hauptkritik an A0 und A1 nicht mehr zutrifft.

Es wird sich zeigen, daß die Geräte, mit denen die Bank Transaktionen vornimmt, nicht sicher sein müssen, solange garantiert ist, daß sichere Geräte diese unsicheren Bankgeräte von sicheren Benutzergeräten unterscheiden können: nimmt man an, daß man einen Mechanismus für das Modell A2 gefunden hat, der es erlaubt, beim Ungültigwerden des Gerätes G der Bank die von G aufgezeichneten Vermerke in einer Form zu übergeben, die die Anonymität der Besitzer nicht verlorener Geräte nicht gefährdet, so kann man diesen Mechanismus auch für die Übergabe von Vermerken während einer Transaktion mit der Bank verwenden. Hierzu wird der Teil des Zahlungsprotokolles, in dem der Austausch von Vermerken geregelt ist, geändert:

- Die Bank, von der anzunehmen ist, daß sie einmal erhaltenen Vermerke nicht mehr verliert, gibt keine Vermerke an das sichere Benutzergerät weiter.
- Das sichere Gerät, das den Partner als unsicheres Bankgerät erkannt hat, übergibt seine Vermerke der Bank in derselben Form, wie ein sicherer Partner sie bei seinem Ungültigwerden an die Bank übergeben würde. Einmal übergebene Vermerke werden nicht mehr weitergegeben; im Verfahren der einfachen markierten Standardwerte können sie einfach gelöscht werden; bei Verfahren, in denen ein Gerät einen Vermerk mehrfach erhalten kann, müssen sie zum Vergleich aufbewahrt werden.

In dieser äquivalenten Form ist A2 das angemessenste der vier hier vorgestellten Angreifermodelle, da es von der Bank nicht erwartet, irgendwelche sicheren Geräte für ihre Aufgaben einzusetzen, umgekehrt aber die aus Sicherheitsgründen als sicher anzunehmenden Benutzergeräte auch für die Anonymitiät als sicher betrachtet.

A3. Das letzte Angreifermodell geht davon aus, daß keine der Informationsquellen durch sichere Geräte geschützt ist, d.h., daß ein sicheres Gerät von einem Kommunikationspartner nicht feststellen kann, ob es sich um ein sicheres Gerät eines Benutzers oder um ein möglicherweise unsicheres Bankgerät handelt.

Damit stellt A3 das Pendant zu A0 dar: basiert die Anonymität in A0 völlig auf der Unausforschbarkeit fremder Geräte, so wird auf diese hier völlig verzichtet. Zur Gewährleistung der Anonymität von B_G kann nur auf kryptographische Hilfsmittel und die Sicherheit des Gerätes G selbst vertraut werden. Da ein anonymer Benutzer immer nur unter den nicht angreifenden, also wirklich sicheren Geräten verborgen sein kann, ist es natürlich auch in A3 praktisch notwendig, daß die große Mehrheit der Benutzergeräte sicher ist; es wird lediglich angenommen, daß die kleine Minderheit angreifender Geräte nicht von den vertrauenswürdigen zu unterscheiden ist.

Das Angreifermodell A3 ist unter den hier gemachten Annahmen das allgemeinste.

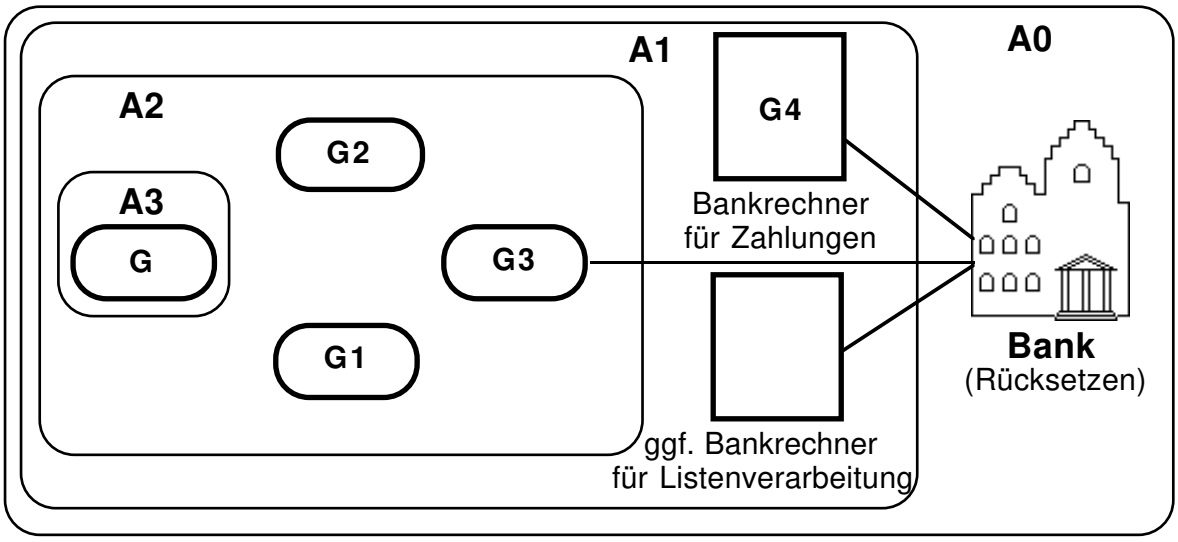


Bild 15 Angreifermodelle. Die Kästen geben an, welchen Geräten vertraut werden muß: In A0 sämtlichen Geräten; in A1 allen Geräten, die das Zahlungsprotokoll ausführen können (also auch den entsprechenden leistungsfähigeren Geräten der Bank), und denen, die die verlorene Geräte betreffenden Vermerke aussortieren; in A2 nur normalen Geräten; in A3 wird nur dem eigenen Gerät unbedingt vertraut.

Ziel der folgenden Abschnitte wird also sein, aufzuzeigen, wie die Anonymität der Benutzer in A1 bis A3 gewährleistet werden kann.

Ein Schutzmechanismus, der einen Angriff im Modell Ai erfolglos macht, stellt natürlich zugleich einen Schutzmechanismus für das Modell A(i-1) dar. Umgekehrt kann, da schon in A1 nicht möglich, auch in A2 und A3 die Anonymität der Besitzer verlorener Geräte (im obigen Sinne) nicht geschützt werden.

5.2 Schutzmechanismen

Um einen Angriff gegen die Anonymität eines nicht verlorenen Gerätes G aussichtslos zu machen, muß, wie oben erwähnt, die Frage „Wann hat G wieviel bzw. welches Geld an wen gezahlt bzw. von wem erhalten?" unbeantwortbar gemacht werden.

Die Realisierung dieses Zieles soll in drei Schritten vorgenommen werden.

5.2.1 Verbergung des Inhalts der Vermerke nicht verlorener Geräte

Im ersten Schritt wird dafür gesorgt, daß die Bank nur genau die Änderungsvermerke lesen kann, die sie benötigt, d.h. nur die verlorene Geräte betreffenden.

5.2.1.1 Verbergung des Inhalts im Modell A1

Im Angreifermodell A1 ist dies höchst einfach: Vermerke über nicht verlorene Geräte werden erst gar nicht an die Bank weitergegeben.

Die Bestimmung, welche Vermerke verlorene Geräte betreffen und daher weitergegeben werden müssen, kann anhand einer von der Bank erstellten und veröffentlichten Liste der Gerätekennzeichen der verlorenen Geräte erfolgen. Damit diese Liste auch wirklich nur Geräte bezeichnet, deren Besitzer ein Rücksetzen wünschen, sollte das Kennzeichen eines Gerätes G im Normalfall der Bank nicht bekannt und daher von G und B_G gemeinsam während der Initialisierung von G gewählt werden.

Damit nicht betrügerisch zwei Besitzer ihre Geräte auf denselben Kontostand setzen lassen, muß die Bank die Liste der erhaltenen Kennzeichen auf Doppelte hin prüfen. (Eine weitergehende Kontrolle ist nicht notwendig: Übergibt ein Besitzer ein Kennzeichen, das kein Gerät verwendete, so wird sein Gerät trivialerweise auf den Wert 0 gesetzt. Übergibt er das Kennzeichen eines anderen, nicht verlorenen Gerätes, d.h. eines, dessen Änderungsaufzeichnung abgegeben wird, so erhält er dessen neuesten Kontostand gutgeschrieben, der aber nach Konstruktion der Verfahren schon aufgrund seiner eigenen Änderungsaufzeichnung ebenfalls auf 0 steht.)

Die Übergabe der Vermerke an die Bank könnte für Verfahren mit mehrfacher Weitergabe theoretisch (wie in 4.2.1.3 geschildert) auch indirekt erfolgen, indem die aufzeichnenden Geräte binärbaumförmig ihre Aufzeichnungen mischen. Dies würde jedoch den tatsächlichen Speicheraufwand der Geräte weiter erhöhen, eine sehr kommunikationsaufwendige verteilte Rücksetzprozedur erfordern und zudem die Zuverlässigkeit des Rücksetzens verringern, da bei einem baumartigen Einsammeln der Vermerke jedes während des Einsammelns verlorengehende Gerät alle Aufzeichnungen seiner Söhne im Baum mit verliert.

5.2.1.2 Verbergung des Inhalts im Modell A3

5.2.1.2.1 Verschlüsselung zum Schutz des Inhalts

Im Angreifermodell A3 (und damit auch A2) kann die Verbergung des Inhalts der Vermerke über nicht verlorene Geräte geschehen, indem das einen Vermerk erzeugende Gerät G diesen vor der Weitergabe mit einem nur ihm und B_G bekannten, von G und B_G gemeinsam gewählten Schlüssel s_G eines symmetrischen Kryptosystems verschlüsselt. Im Verlustfall muß natürlich die Bank s_G (oder einen Wert, aus dem s_G leicht zu berechnen ist) von B_G erhalten.

Damit nicht betrügerisch zwei Besitzer ihre Geräte auf denselben Kontostand setzen lassen, muß nur die Liste der erhaltenen Schlüssel, wie in 5.2.1.1 die der Kennzeichen, auf Doppelte hin geprüft werden.

5.2.1.2.2 Anonyme Kennzeichnung

In jedem Fall ergibt sich jedoch für die Angreifermodelle A2 und A3 das Problem, wie die Bank im Verlustfall die zu einem verlorenen Gerät G gehörenden Vermerke feststellen, ihr diese Zuordnung jedoch im Normalfall verwehrt werden kann. Hierzu müssen die Vermerke, die die Bank erhalten kann, in einer Weise gekennzeichnet sein, die für nicht verlorene Geräte G1 anonym bleibt, d.h. den Namen von G1 nicht erkennen läßt und auch nicht die Tatsache, daß alle seine Vermerke vom selben Gerät erzeugt wurden.

5.2.1.2.2.1 Verschlüsselung mit Redundanz

Das Verbergen des Urhebers eines Vermerks vor der Bank geschieht im einfachsten Fall gleichzeitig mit der Verbergung des Inhalts durch die Verschlüsselung mit s_G. Ein zusätzliches Kennzeichen ist nicht notwendig, ebensowenig das bisher im Inhalt der Vermerke befindliche, denn die Tatsache, daß der übrige Inhalt eines Vermerkes (im folgenden stets mit V bezeichnet) mit s_G verschlüsselt ist, kennzeichnet G bereits eindeutig als dessen Urheber – sofern die Eindeutigkeit der Schlüssel garantiert ist. (Diese Eindeutigkeit kann garantiert werden, indem jedes Gerät G der Bank bei der Initialisierung das Bild von s_G unter einer speziell für diesen Zweck fest gewählten Einwegfunktion übergibt und die Bank mehrfach auftretende Bilder zurückweist.) Um allerdings erkennen zu können, ob mit s_G verschlüsselt wurde, muß entweder V Redundanz enthalten oder vor der Verschlüsselung von G um einen hinreichend redundanten Teil r erweitert worden sein, d.h. statt $s_G(G,V)$ kann

$$s_G(r,V)$$

mit einem in der Länge oder für andere Zwecke besser als G passenden Teil r verwendet werden.

Um die verlorene Geräte betreffenden Vermerke aus einer umfassenden Liste erhaltener Vermerke herauszufiltern, muß hier jeder der erhaltenen Vermerke einmal probeweise mit jedem Schlüssel eines verlorenen Gerätes entschlüsselt werden.

5.2.1.2.2.2 Pseudozufällige Kennzeichen

Statt die Zuordnung der Vermerke zu den verlorenen Geräten durch probeweises Entschlüsseln und Prüfung der Redundanz vorzunehmen, kann jeder Vermerk V auch wie im nicht anonymen Fall mit einem expliziten Gerätekennzeichen versehen werden, das G eindeutig bezeichnet. Um nicht durch Vergleich der unverschlüsselten Gerätekennzeichen feststellen zu können, ob verschiedene Einträge

vom selben Gerät G erzeugt wurden, wählt G für jeden Vermerk V ein eigenes Gerätekennzeichen Z_V, das mit anderen Kennzeichen von G in keiner leicht feststellbaren Beziehung steht. Der Inhalt V muß natürlich weiterhin mit s_G verschlüsselt werden, so daß ein Eintrag die Form

$$Z_V, s_G(r,V)$$

annimmt (der redundante Teil r kann im Prinzip entfallen).

Die Erzeugung der Z_V geschieht am einfachsten, indem G seine Kennzeichen als Blöcke aus der Ausgabe eines (kryptographisch starken) Pseudozufallsbitfolgengenerators (PRNG, [BlBS_86]) wählt (vgl. Bild 16). Bezeichnet $(q_G)^i$ den i-ten aus q_G abgeleiteten Block und ist V der i-te Vermerk von G, so ist also

$$Z_V = (q_G)^i$$

Der Startwert q_G (für Quelle) des PRNG muß dann wie der Schlüssel s_G von B_G im Verlustfall der Bank übergeben werden.

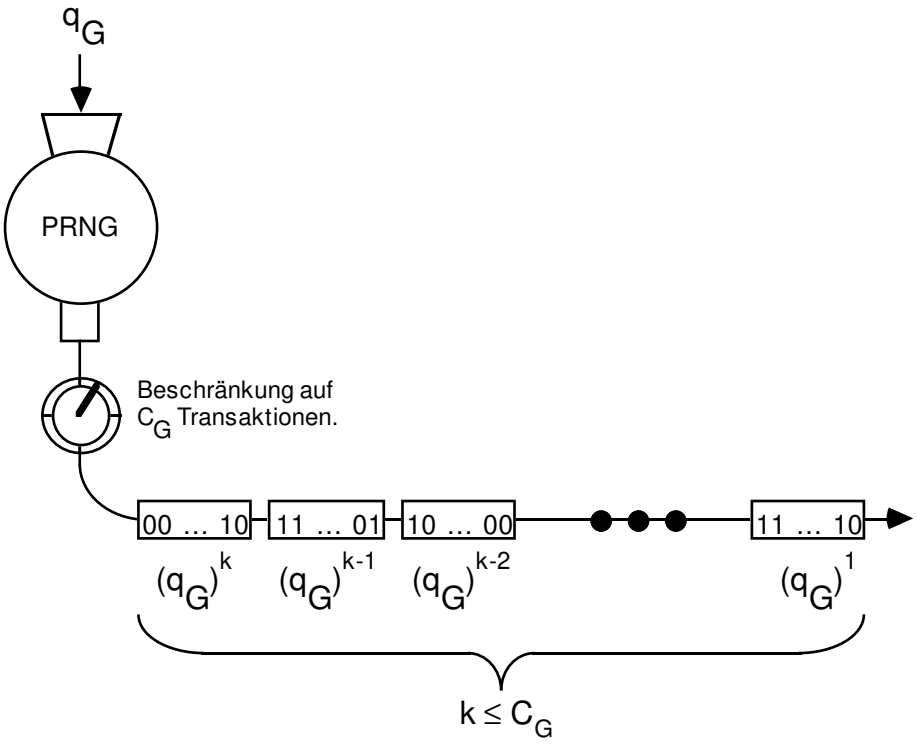


Bild 16 Erzeugung pseudozufälliger Gerätekennzeichen. Die Anzahl k der Kennzeichen des Gerätes G wird beschränkt, z.B. auf das c_G-fache der im Mittel von einem Gerät vorgenommenen Transaktionen.

Um ein verlorenes Gerät G rücksetzen zu können, muß die Bank anhand der Gerätekennzeichen der ihr vorliegenden Vermerke die G betreffenden feststellen. Die Kenntnis von q_G alleine genügt zur Lösung dieser Aufgabe i.allg. nicht. Ist jedoch bekannt, daß G maximal C_G Kennzeichen aus q_G erzeugt hat, so kann die Bank eine Liste aller möglichen Kennzeichen G's erzeugen, sortieren und jedes erhaltene Kennzeichen mit logarithmischem Aufwand darin suchen (was meist günstiger sein wird als obiges probeweises Entschlüsseln, vgl. 5.3).

Um dieses Verfahren allgemein anwenden zu können, muß die Anzahl der möglichen Transaktionen künstlich beschränkt werden, etwa indem jeder Benutzer C_G für sein Gerät G festsetzt (wobei größere C_G mehr Gebühren kosten sollten).

Es bezeichne c den Quotienten aus dem Mittelwert der C_G und der mittleren Anzahl der Transaktionen der Geräte. Damit kann also ein Gerät im Mittel höchstens c • p•z Zahlungen vornehmen. Naturgemäß ist c≥1. Im folgenden wird c stets als kleine Konstante, etwa c=5, angenommen.

5.2.2 Verbergung des aufzeichnenden Gerätes

Auch ohne Kenntnis des Inhalts eines Vermerkes (erst recht aber natürlich mit dieser Kenntnis) kann der Angreifer versuchen, aus der Kenntnis über das aufzeichnende Gerät Schlüsse zu ziehen. Beispiele für solche Schlußfolgerungen sind:

- Erhält die Bank in einem Weitergabeverfahren einen Vermerk von genau zwei Geräten G1 und G2, so ist die Wahrscheinlichkeit sehr groß, daß der Vermerk eine Transaktion zwischen G1 und G2 bezeichnet. Erhält sie einen Vermerk über ein verlorenes Gerät G2 von genau einem Gerät G1, so ist die Situation noch schlimmer, denn dann erfährt sie sogar den genauen Betrag und den Partner, eben G2, der Zahlung des nicht verlorenen Gerätes G1.
- Für das Verfahren der markierten Standardwerte (ohne mehrfache Weitergabe) gilt entsprechendes sogar für jede Übergabe: erhält die Bank hier einen Weitergabevermerk von G1, so war G1 der Zahlende; ist der Empfänger verloren, so weiß sie sogar, welchen Standardwert G1 einmal besaß, der wievielte Besitzer dieses Standardwerts G1 war und an wen, eben G2, er ihn weitergab.

Die Beispiele gelten offenbar für jedes Modell, in dem der Angreifer die Vermerke über verlorene Geräte von den aufzeichnenden Geräten erhält, also in allen noch behandelten Angreifermodellen.

Um diese Anonymitätseinbußen zu vermeiden, müssen daher, als zweiter Schritt der Anonymisierung, die Änderungsaufzeichnungen anonym der Bank übergeben werden, d.h. die Bank soll zu einem erhaltenen Änderungsvermerk nur feststellen können, ob er von einem sicheren Gerät stammt, nicht aber, von welchem. Zusätzlich kann die Beziehung zwischen Vermerken, vom selben Gerät aufgezeichnet worden zu sein, verborgen werden. (Dies gilt natürlich nur für die Vermerke, die beim Ungültigwerden an die Bank übergeben werden, in A2 und A3 jedoch nicht für die, die während des normalen Zahlungsprotokolls an den Partner, also evtl. den Angreifer, übergeben werden.)

Bei einer hinreichend großen Anzahl von Benutzern ist in allen in Kapitel 4 beschriebenen Verfahren garantiert, 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.

Damit sind die Voraussetzungen für die Anwendung eines Datenschutz garantierenden Kommunikationssystemes gegeben (das einerseits sowieso sinnvoll ist und eine Voraussetzung für jedes anonyme digitale Zahlungssystem ohne sichere Geräte darstellt, das aber andererseits auch speziell zu diesem Zweck virtuell aufgebaut werden kann): alle sicheren Geräte übersenden mittels eines solchen der Bank anonym ihre Änderungsaufzeichnung (im Idealfall, um auch den Zusammenhang zwischen den von einem Gerät aufgezeichneten Vermerken zu verbergen, jeden Vermerk einzeln) und erhalten dafür von der Bank jeweils 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 für alle ihre Vermerke 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 reinitialisiert werden und welche zurückgesetzt werden müssen (oder wollen).

Verzichtet ein Besitzer, dessen Gerät die Änderungsaufzeichnung bereits übersandt hat, auf die Reinitialisierung oder läßt gar sein Gerät rücksetzen, so bringt ihm dies keinerlei Vorteile: sein Gerät wird wertlos für ihn und er kann kein bereits ausgegebenes Geld zurückerhalten (da in seiner Aufzeichnung all seine Ausgaben dokumentiert sind). Die Gesamtsicherheit der Systeme bleibt, wie man leicht den jeweiligen Beweisen entnehmen kann, ebenfalls erhalten.

Es sei angemerkt, daß die (in jedem Fall stark eingeschränkte) Anonymität der Besitzer verlorener Geräte bei den Weitergabeverfahren etwas verbessert werden kann, wenn die Übergabe der Änderungsaufzeichnungen auch anonym vor den Besitzern der sicheren Geräte erfolgt:

Kann nämlich ein Besitzer B_G die Übergabe der Änderungsaufzeichnung seines Gerätes G an die Bank beobachten, so kann er natürlich, unabhängig davon, ob die Vermerke einzeln oder zusammenhängend übergeben werden, der Bank mitteilen, welche es waren. Diese kann davon diejenigen lesen, die verlorene Geräte betreffen. Bei einem Weitergabeverfahren stammen diese i.allg. größtenteils nicht von Transaktionen mit G; befindet sich jedoch unter ihnen ein Vermerk über einen ungewöhnlichen Betrag b, erinnert B_G sich an eine Transaktion über den Betrag b und ist die Liste der Vermerke von G nicht gar zu lang, so ist es sehr wahrscheinlich, daß es sich um dieselbe Transaktion handelt. Damit ist der Zusammenhang zwischen dem Partner von B_G in dieser Transaktion und dem Kennzeichen des verlorenen Gerätes hergestellt. (B_G alleine kann natürlich mit seiner Beobachtung nichts anfangen, da er sie ohne Hilfe der Bank nicht lesen und auch zu keinen anderen Aufzeichnungen in Beziehung setzen kann.)

Wird zur anonymen Übersendung das perfekte Senderanonymität bietende überlagernde Senden verwendet, so heißt dies, daß die sicheren Geräte bereits bei der Initialisierung in ausreichendem Maße Schlüssel ausgetauscht haben müssen (im Idealfall sehr lange Schlüssel, jeweils paarweise zwischen allen Geräten) und auch der genaue Zeitraum, in dem die Übergabe stattfinden muß, bereits festgelegt worden sein muß. Als weniger aufwendige Alternative bietet sich daher der Einsatz umcodierender MIXe an, wofür lediglich bei der Initialisierung den sicheren Geräten die Schlüssel der verwendbaren MIXe mitgeteilt werden müssen. (Für eine Erklärung der angesprochenen Verfahren sei auf [PfPW_86] verwiesen.)

Beim Verfahren der markierten Standardwerte ist der obige Angriff zwar auch möglich (und ohne zusätzliche Weitergabe stammen auch alle Vermerke aus Transaktionen von G), aber schwächer als der in 5.1 beim Angreifermodell A1 geschilderte, in dem die Vermerke der verlorenen Partnergeräte von G anhand der Standardwerte identifiziert werden. Daher sind Maßnahmen zu seiner Vermeidung sinnlos.

Mit den oben genannten Verfahren ist garantiert, daß ein Angreifer höchstens die Änderungsaufzeichnungen auswerten kann, die verlorene Geräte betreffen (Schritt 1, 5.2.1), und daß alle Schlußfolgerungen, die er ziehen kann, auf der Darstellung der Aufzeichnungen, nicht aber auf den Umständen der Übergabe beruhen (Schritt 2, 5.2.2).

Damit ist die Anonymisierung im Modell A1 abgeschlossen.

5.2.3 Verhinderung statistischer Auswertungen in A2 und A3

In den Angreifermodellen A2 und A3 verbleibt als letzter und kompliziertester Schritt, dem Angreifer die „statistische" Auswertung der nicht verlorene Geräte betreffenden Vermerke zu verwehren. Hierzu muß garantiert werden, daß zwischen zwei beliebigen verschiedenen von nicht verlorenen Geräten

erzeugten Vermerken für den Angreifer kein Zusammenhang erkennbar wird, auch wenn die beiden Vermerke vom selben Gerät erzeugt wurden oder dieselbe Transaktion bezeichnen.

Durch die Verschlüsselung und anonyme Kennzeichnung (vgl. 5.2.1.2) sind alle Relationen zwischen Vermerken außer der „trivialen" Relation der Gleichheit bereits verborgen, denn es wird angenommen, daß jedes verwendete Kryptosystem jede nicht triviale Relation zwischen Vermerken verbirgt, also keine solche Relation zwischen zwei Vermerken V1 und V2 (etwa „vom selben Gerät erzeugt" oder „betrifft denselben Standardwert") aufgrund der Verschlüsselungen s1(V1) und s2(V2) effizient berechnet werden kann.

(Auch ein nicht deterministisches Kryptosystem hilft in diesem Zusammenhang jedoch nicht ohne weiteres, die Gleichheit zu verbergen, da hier gleiche Vermerke nicht durch mehrfaches Verschlüsseln desselben Vermerkinhaltes entstehen, sondern durch Weitergeben fertig verschlüsselter Vermerke.)

Die Möglichkeit, daß ein Vermerk mehrfach aufgezeichnet wird, ist in allen in Kapitel 4 beschriebenen Verfahren mit Ausnahme des der einfachen markierten Standardwerte (das daher mit obigen Maßnahmen auch bereits in idealer Weise anonymisiert ist!) gegeben.

Die Möglichkeiten der Auswertung der Gleichheit ergeben sicher nicht sehr viel Information für den Angreifer, sind aber auch nicht völlig vernachlässigbar, da für jedes Verfahren mit mehrfacher Weitergabe die Anzahl der Kopien eines Vermerkes mit dessen Alter korreliert ist.

Hinzu kommt, falls der Zusammenhang zwischen den von einem Gerät aufgezeichneten Vermerken nicht verborgen wird:

- Die transitive Hülle der Relation „G1 hat mit G2 eine Transaktion vorgenommen" (also des nackten Zahlungsflusses) ist eine Obermenge der Relation „G1 und G2 haben gleiche Vermerke in ihren Aufzeichnungen".
- Im Verfahren der maximalen Weitergabe zeichnen sich zwei Geräte G1 und G2, die miteinander ihre letzte Transaktion vor Terminierung des Systems durchführten, durch übereinstimmende Änderungsaufzeichnungen aus.

Die Möglichkeit, daß die Geräte bereits während der Abgabe der Aufzeichnungen dafür sorgen, daß von mehrfach aufgezeichneten Vermerken nur eine Version die Bank erreicht, entspräche beinahe einer Rückkehr zum Angreifermodell A1, da wieder ein aufwendiges Koordinierungsverfahren nötig wäre und der Vergleich mit allen bisher abgegebenen Vermerken einen Aufwand ähnlicher Größenordnung erfordert wie das Heraussuchen der verlorene Geräte betreffenden Vermerke. Diese Möglichkeit soll daher im folgenden nicht mehr betrachtet werden.

Der aus Anonymitätssicht ideale Zustand wäre erreicht, wenn ein ein Gerät G betreffender Vermerk nach jeder Weitergabe in den möglichen Bereich des Angreifers (also in A2 bei Weitergabe an ein Bankgerät, in A3 bei jeder Weitergabe) seine Darstellung änderte und ohne Zutun G's niemand einen Zusammenhang zwischen verschiedenen Versionen davon erkennen könnte.

Ein Verschlüsselungsverfahren, das dies unter der Annahme A3 in allgemeiner Form leistet und zugleich gestattet, unter Mitwirkung G's die G betreffenden Vermerke effizient zu finden und zu lesen, ist uns nicht bekannt. (Zudem würde ein solches Verfahren die Speicherkomplexität der Weitergabeverfahren weiter steigern, da ein Gerät einen mehrfach erhaltenen Vermerk auch mehrfach speichern müßte, d.h. der Speicheraufwand wüchse unbegrenzt exponentiell in der Anzahl der Transaktionen.)

5.2.3.1 Verbergung der Gleichheit zweier Vermerke in Modell A2

5.2.3.1.1 Unterschiedliche Verschlüsselung mit Redundanz

Wohl bekannt ist jedoch eine Lösung, die unter Annahme von A2 allgemein einsetzbar ist und natürlich wieder auf der Verschlüsselung der Vermerke beruht: gleiche Vermerke werden vor Weitergabe an den Angreifer einfach unterschiedlich verschlüsselt (vgl. Bild 17).

Ist V ein G1 betreffender Vermerk, so muß hierzu jedes Gerät G2, das V aufzeichnet, für V eine eigene Verschlüsselungsfunktion bestimmen. Geht G1 verloren, so muß natürlich die Bank von B_{G1} (wie bereits den Schlüssel s_G, vgl. 5.2) die von den aufzeichnenden Geräten verwendeten Verschlüsselungsfunktionen (genauer die zugehörigen Entschlüsselungsfunktionen) erhalten. Dies ist das eigentliche und die Anwendbarkeit der Idee stark einschränkende Problem.

Unter Annahme von A2 kann dieses Problem jedoch sehr leicht gelöst werden: jedem Vermerk V von G1 wird der Schlüssel s_{G1} beigefügt, so daß zwischen den sicheren Geräten das Paar (V,s_{G1}) weitergegeben wird. Übergibt jedoch ein sicheres Gerät G2 den Vermerk V in den Bereich des Angreifers, so wählt sich G2 zuvor eine Zufallszahl $r_{V,G2}$ und verschlüsselt V unter Hinzufügung von Redundanz als

$$s_{G1}(r_{G2,V},V)$$

(d.h. als Verschlüsselungsfunktion wird gewählt $[x \rightarrow s_{G1}(r_{G2,V},x)]$).

Im Verlustfall erhält die Bank von G1 wie oben den Schlüssel s_{G1} und kann damit anhand der beigefügten Redundanz alle G1 betreffenden Vermerke erkennen und entschlüsseln.

Ohne Kenntnis von s_{G1} verbirgt jedoch die Verschlüsselung jede zusätzliche Information über Relationen zwischen V und anderen Vermerken vor der Bank.

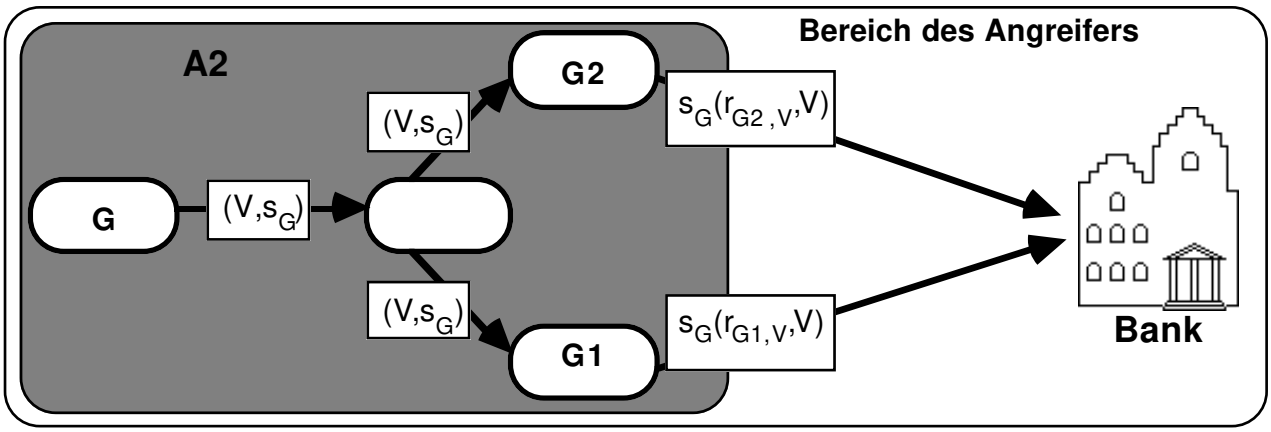


Bild 17 Verschlüsselungen des Vermerkes V unter Annahme des Angreifermodelles A2 (sicherer Bereich grau unterlegt). Zwischen den sicheren Geräten wird (V,s_G) weitergereicht; vor der Übergabe in den Bereich des Angreifers verschlüsselt das übergebende Gerät G2 (bzw. G1) den Vermerk V mit s_G unter Hinzufügung eines von ihm gewählten pseudozufälligen Teils $r_{G2,V}$ (bzw. $r_{G1,V}$).

5.2.3.1.2 Pseudozufällige Kennzeichen

Auch hier kann man versuchen, wie in 5.2.1.2.2.2 zusätzliche pseudozufällig erzeugte Kennzeichen zu verwenden, wobei allerdings jedes einen Vermerk aufzeichnende Gerät für diesen ein anderes Kennzeichen verwenden muß.

Damit die Bank im Verlustfall allein nach Angaben von B_{G1} wieder alle möglichen Kennzeichen des Gerätes G1 erzeugen kann, muß G1 für jeden seiner Vermerke V und für jedes V möglicherweise aufzeichnende Gerät ein eigenes Kennzeichen vorherbestimmen. Hierzu muß G1 in der Lage sein, jedes V möglicherweise aufzeichnende Gerät mit einem eindeutigen Namen zu versehen, wobei die Zuordnung entweder a priori bei der Erzeugung V's, d.h. in Abhängigkeit von den Gerätekennzeichen der anderen Geräte, oder dynamisch anhand der Weitergabe V's, d.h. in Abhängigkeit vom Zahlungsfluß, geschehen kann.

5.2.3.1.2.1 A priori festgelegte Kennzeichen

Eine a priori festgelegte Bezeichnungsweise müßte, da jedes Gerät V aufzeichnen kann, alle g Geräte des Systems umfassen. Die im Prinzip einfache Möglichkeit, dem Vermerk V eine Liste aus g Paaren $(Gi,Z_{V,i})$ anzuhängen, der jedes Gerät Gi sein Kennzeichen $Z_{V,i}$ für V entnehmen könnte, scheidet aus Aufwandsgründen aus, da sie den bei den Weitergabeverfahren, für die der Einsatz dieses Kennzeichnungsverfahrens sinnvoll sein könnte, ohnehin schon hohen Speicheraufwand der sicheren Geräte um einen weiteren Faktor g erhöhen würde.

Statt dessen muß diese Zuordnung durch eine von G vergleichsweise kurz beschreibbare Funktion vorgenommen werden. Im Verlustfall muß die Bank natürlich wieder alle für V verwendeten Kennzeichen möglichst einfach erzeugen können, wobei sie jedoch, um die Anonymität der aufzeichnenden Geräte nicht zu gefährden, die Zuordnung selbst nicht erfahren darf.

Um dies zu erreichen, müßten die eigentlichen g Kennzeichen wie in 5.2.1.2.2.2 pseudozufällig aus einem V zugeordneten Startwert q_V erzeugt werden, der selbst wiederum pseudozufällig aus einem Startwert q_G erzeugt wurde. Das i-te aus q_V abgeleitete Kennzeichen sei mit $(q_V)^i$ bezeichnet. Die Zuordnung der Kennzeichen zu den Geräten würde durch eine Permutation π der Werte von $\{1,\ldots,g\}$ vorgenommen, die G eigens für V wählt und die die Bank niemals erhält, da sie andernfalls den Kennzeichen der Vermerke über verlorene Geräte das aufzeichnende, nicht verlorene Gerät ansähe. Dies wäre interessantere Information als die, die durch dieses Verfahren verborgen werden sollte; insbesondere wäre, wenn die Bank einen Vermerk nur einmal erhält, mit großer Wahrscheinlichkeit der nicht verlorene Partner des verlorenen Gerätes bestimmt.

Zwischen den Geräten würden damit die Vermerke in der Form

$$(V, s_G, q_V, \pi_V)$$

weitergegeben. Ein Gerät Gi, das V der Bank übergäbe, berechnete sein Kennzeichen für V als den $\pi_V(Gi)$-ten aus q_V abgeleiteten Block, was kurz mit

$$Z_{V,i} := (q_V)^{\pi_V(Gi)}$$

bezeichnet werden soll (vgl. Bild 18). Statt $Z_{V,i}$ sequentiell zu berechnen, könnte dies gemäß des Schemas aus [GoGM_84] auch mit in g logarithmischem Aufwand geschehen.

Eine explizite Angabe von π scheidet allerdings wieder aus Speichergründen aus; da $g! \geq 2^g$ für $g>3$, würde dies mindestens g bit je Vermerk erfordern. Statt dessen müßte man sich wieder auf eine kurz, d.h. beispielsweise mit $f(g) = O(\log(g))$ bits, beschreibbare Teilmenge der g! möglichen Permutationen beschränken. Leider kann man für die so beschreibbaren Permutationen keine Pseudozufälligkeit erwarten, (d.h. daß die Bank ihnen mit vernünftigem Aufwand überhaupt keine Information entnehmen könnte), da selbst der Aufwand, sie alle auszuschreiben, nur $2^{f(g)} \bullet g$ beträgt,

im Beispiel also $O(g^2)$. (Das Grundproblem ist also, daß g als Speicheraufwand der sicheren Geräte zwar nicht, als Zeitaufwand des Angreifers aber durchaus akzeptabel ist).

Zumindest in dem Fall, daß nicht verlorene Geräte ihre Änderungsaufzeichnung als Ganzes abliefern, könnte die hier gewonnene Information zur Deanonymisierung nicht verlorener Geräte führen, im anderen ist die zu gewinnende Information zwar minimal, das gleiche galt jedoch für die zu verbergende. Daher erscheint der Einsatz eines solchen Verfahrens nicht sinnvoll.

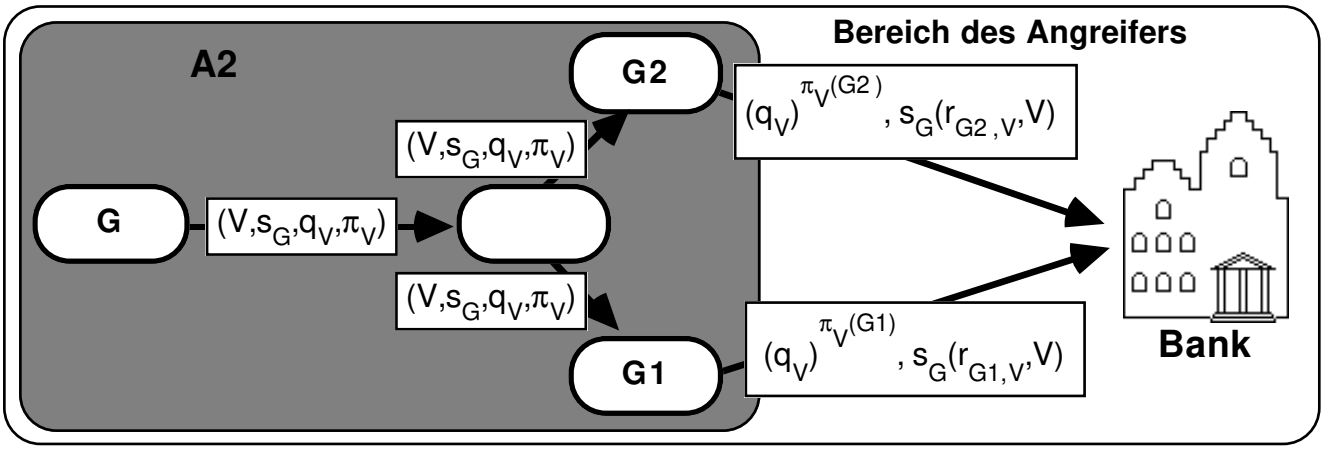


Bild 18 Verschlüsselungen und pseudozufällige Kennzeichnungen des Vermerkes V unter Annahme des Angreifermodelles A2 (sicherer Bereich grau unterlegt). Zwischen den sicheren Geräten wird (V,s_G,q_V,π_V) weitergereicht; vor der Übergabe in den Bereich des Angreifers bestimmt das übergebende Gerät G2 sein Kennzeichen $(q_V)^{\pi_V(G2)}$ für V und verschlüsselt den Vermerk mit s_G unter Hinzufügung eines von ihm gewählten pseudozufälligen Teils $r_{G2,V}$. Analog geht G1 vor.

5.2.3.1.2.2 Dynamisch bestimmte Kennzeichen

Trivial ist eine dynamisch bestimmte Bezeichnungsweise, wenn nur das einen Vermerk erzeugende Gerät diesen weitergibt (was nur beim Verfahren der markierten Standardwerte mit mehrfacher Weitergabe möglich ist), da es einfach bei jeder Weitergabe ein neues pseudozufälliges Kennzeichen erzeugen kann.

Wird der Vermerk auch von anderen Geräten weitergegeben, so ist ein Beispiel der dynamischen Bestimmung, welches davon welches Kennzeichen verwendet, die anhand des in Abschnitt 4.3.2.1 eingeführten Weitergabebaumes. Hierzu wird angenommen, daß der Weitergabebaum die tiefste Tiefe t habe und damit alle Blätter einen t Stellen langen Namen tragen. Übergibt G3 den Vermerk V, für den er im zugehörigen Weitergabebaum den Namen x trägt, der Bank, so ergänzt er ggf. den Namen x durch Anhängen beliebiger Bits auf den Namen eines x nachfolgenden Blattes und wählt als eigentliches Kennzeichen das x-te aus einem Startwert q_V ableitbare Kennzeichen (vgl. 5.2.3.1.2.1).

Der Baum enthält maximal 2^t verschiedene Kennzeichen, die im ungünstigsten Fall jedoch alle von der Bank zum Auffinden des Vermerkes V erzeugt werden müssen. Eine dynamisch bestimmte Bezeichnungsweise bietet daher gegenüber der oben geschilderten a priori festgelegten Bezeichnungsweise nur dann Vorteile, wenn die maximale Anzahl 2^t der Aufzeichnungen von V

unterhalb von g liegt (was in den Verfahren aus Kapitel 4 nur für die markierten Standardwerte mit mehrfacher Weitergabe erreicht werden kann).

Da ein Gerät einen Vermerk höchstens t mal weitergeben kann, sind durch $2^t < g$, also $t < \log(g)$, die möglichen Weitergabestrategien eingeschränkt.

Jedoch ist, wie in 5.2.3.1.2.1, auch durch ein solches Verfahren die Anonymität der aufzeichnenden, nicht verlorenen Geräte gefährdet, sofern nicht alle aufgezeichneten Vermerke einzeln abgeliefert werden, da diesmal den Vermerken der Zahlungsfluß während ihrer Entstehung anzusehen ist, denn die Bank erfährt bei der Erzeugung der pseudozufälligen Kennzeichen deren Reihenfolge. (Das betrifft auch das zu Beginn genannte triviale Verfahren.) Um dies zu vermeiden, müssen die Kennzeichen wieder permutiert werden, was, wie in 5.2.3.1.2.1 beschrieben, nur zu völliger Anonymität führt, wenn jede Permutation der gegebenen Länge möglich ist. Damit ist das Verfahren äquivalent dazu, daß zwischen den sicheren Geräten anstelle von q_V und π eine Liste von Paaren aus einem Namen im Weitergabebaum und dem zugehörigen Kennzeichen verwendet werden.

Da das Verfahren ohnehin nur für markierte Standardwerte mit mehrfacher Weitergabe anwendbar ist, ist es nun möglich, die maximale Anzahl der einen Vermerk aufzeichnenden Geräte soweit zu beschränken, daß der Speicheraufwand der sicheren Geräte nicht wesentlich vergrößert wird, zumal ein Gerät zu einem Vermerk nur solange die Permutation des Weitergabebaums speichern muß, wie es diesen noch an andere weitergeben muß, und auch nur den Teil davon, der es und seine Nachfolger betrifft. Bei der Darstellung als Paarliste heißt dies genauer, daß kein solches Paar jemals gleichzeitig in zwei Geräten gespeichert ist.

5.2.3.2 Verbergung der Gleichheit zweier Vermerke in Modell A3

Als Notkonstruktionen für das Angreifermodell A3 bieten sich zwei Möglichkeiten an:

Zum einen kann man direkt das für A2 geschilderte Verfahren anwenden. Geht man jedoch von A2 zum allgemeineren Modell A3 über, so folgt, daß nur G1 selbst die Rolle von G2 spielen kann (vgl. Bild 19). Mit anderen Worten: ein Vermerk V kann nicht beliebig weitergegeben werden, sondern nur von dem V erzeugenden Gerät (was wieder nur für das Verfahren der markierten Standardwerte mit mehrfacher Weitergabe einen Sinn ergibt). Damit wird allerdings auch wieder die zusätzliche Verwendung pseudozufälliger Kennzeichen (wie am Ende von 5.2.3.1.2 beschrieben) möglich.

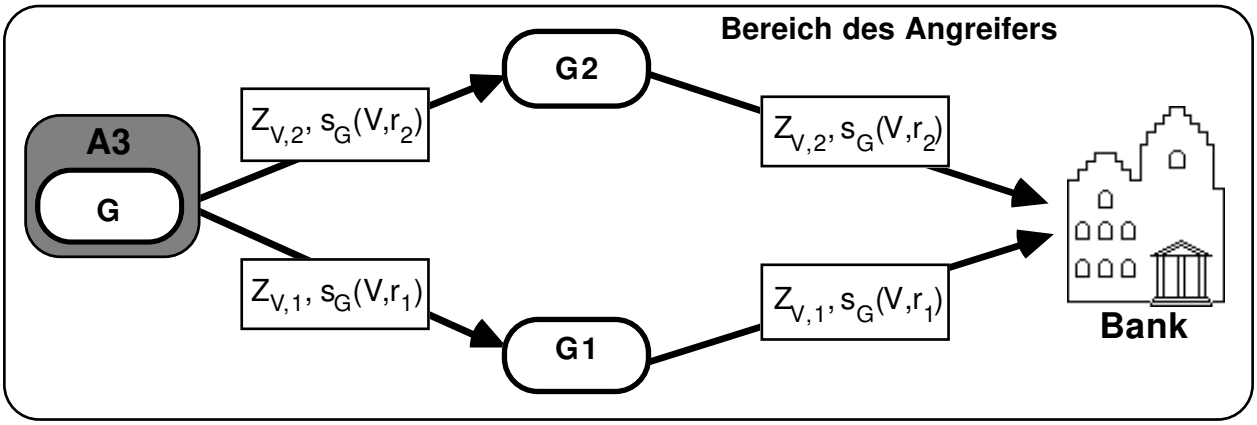


Bild 19 Verschlüsselungen des Vermerkes V unter Annahme des Angreifermodelles A3 (grau unterlegt). Der Vermerk V wird nur vom erzeugenden Gerät weitergereicht, das diesen vor der Übergabe redundant verschlüsselt. Die zusätzlichen, von G pseudozufällig erzeugten Kennzeichen $Z_{V,i}$ sollen das Auffinden der G betreffenden Vermerke im Verlustfall erleichtern und können auch entfallen.

Zum anderen kann man natürlich den in der Realität nur geringen Unterschied zwischen A2 und A3 ignorieren bzw. ihn verkleinern, indem man annimmt, daß in Transaktionen mit einem sicheren Gerät sich die Bank gemeinhin freiwillig zu erkennen gibt, ein sicheres Gerät jedoch nicht von sich aus erkennen kann, wenn es mit der Bank (bzw. mit einem sich als elektronische Brieftasche ausgebenden unsicheren Bankgerät) kommuniziert. Wenn man nun ein für A2 entwickeltes Verfahren zur Verbergung der Gleichheit verwendet, ist das zwar nicht perfekt, man kann jedoch in der Praxis hoffen, den unerkannten Anteil des Angreifers stark verringert zu haben (vgl. Bild 20).

Verschlüsselt zumindest jedes wirklich sichere Gerät jeden Vermerk vor jeder erkannten Übergabe an die Bank verschieden, so bleibt dem Angreifer lediglich die Auswertung der Gleichheit von Vermerken in den Aufzeichnungen seiner eigenen Geräte und in den Aufzeichnungen, die seine Geräte in Transaktionen mit sicheren Geräten unverschlüsselt erhielten.

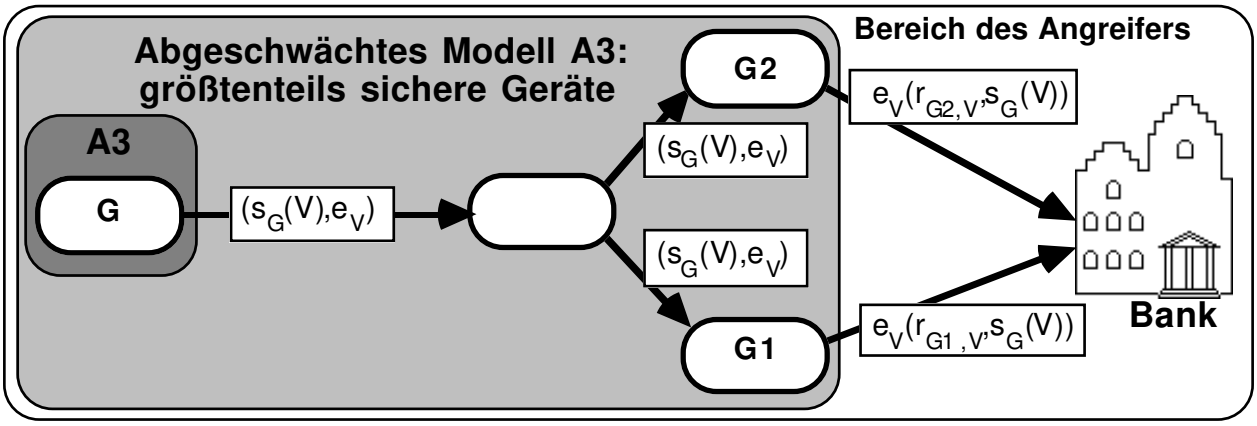


Bild 20 Verschlüsselungen des Vermerkes V unter Annahme des abgeschwächten Angreifermodelles A3 (sicherer Bereich dunkel-, teilweise sicherer hellgrau unterlegt). Die Vermerke werden bereits zwischen den Geräten verschlüsselt weitergereicht, die Verbergung der Gleichheit von Vermerke geschieht jedoch erst bei der Übergabe an die Bank.

Die Anonymitätseinbuße, die durch diese „absichtliche Ungenauigkeit" entsteht, darf natürlich nur nur die Auswertbarkeit der Relation „Gleichheit" betreffen, nicht jedoch den Inhalt von Vermerken. Daher muß die Verwendung des ursprünglichen Schlüssels s_{G1} auf die Verbergung des Inhalts der Vermerke von G1 vor allen anderen Geräten beschränkt werden, d.h. diese werden von G wieder von Anfang an als $s_{G1}(V)$ verschlüsselt, G1 gibt s_{G1} niemals weiter und die Bank erhält ihn nur im Falle des Verlustes von G1.

Damit ist klar, daß ein solches Verfahren zwar für alle Überdeckungsverfahren möglich ist, nicht jedoch für verteilte Kontostände, da ein speicherndes Gerät G2 verschiedene Kontostände desselben Gerätes G1 nicht mehr als solche erkennen könnte, wodurch zumindest der Speicherplatzvorteil des Verfahrens dahin wäre.

Um dem Angreifer das Auswerten der Gleichheit möglichst schwer zu machen, ist nun ein Verfahren gesucht, das es jedem speichernden Gerät G2 erlaubt, Vermerke vor der Übergabe an die Bank wie oben zusätzlich zu verschlüsseln, es dem möglichen Angreifer aber nicht erlaubt, der Bank übergebene verschlüsselte Vermerke zu erkennen, auch wenn er die verwendeten Schlüssel und unverschlüsselten Vermerke von seinen nur scheinbar sicheren Geräten erhält. Dies ist offensichtlich gerade die durch asymmetrische Kryptosysteme erbrachte Funktion, so daß sich folgendes Vorgehen anbietet: Zusätzlich zu s_{G1} wählt sich jedes Gerät G1 ein Schlüsselpaar eines asymmetrischen Kryptosystems, bestehend aus öffentlichem Schlüssel e und privatem Schlüssel d. Zwischen den (hoffentlich) sicheren Geräten wird das Paar $(e,s_{G1}(V))$ weitergegeben. Damit e für die nur scheinbar sicheren Geräte des Angreifers nicht die Rolle eines Gerätekennzeichens für G1 erhält, muß G1, wie in 5.3.1 für die Gerätekennzeichen Z_V beschrieben (vgl. Bild 15), für jeden Vermerk V ein eigenes Schlüsselpaar (e_V,d_V) bestimmen. (Natürlich dienen die pseudozufällig erzeugten Gerätekennzeichen Z_V nicht direkt als Schlüsselpaar, sondern nur zur Initialisierung des Schlüsselerzeugungsalgorithmus des verwendeten Kryptosystems.)

Vor der Übergabe des Vermerkes $s_{G1}(V)$ an die Bank wird dieser wie oben mit e_V als

$$e_V(r_{G2,V},s_{G1}(V))$$

verschlüsselt. Geht G1 verloren, so erhält die Bank den Schlüssel s_{G1} und den zur Erzeugung der Schlüsselpaare verwendeten Startwert q_{G1} von B_{G1} und kann damit die G1 betreffenden Vermerke erkennen und auswerten.

5.3 Protokolle, Aufwand

In den vorangegangenen beiden Abschnitten wurden allgemein Angreifermodelle und Schutzmaßnahmen für Verfahren der verteilten Änderungsaufzeichnung beschrieben. Hierbei zeigte sich, daß unter der Annahme

- des sinnvollsten Angreifermodells A2 und
- der Existenz und Verwendung idealer sicherer Geräte und Kryptosysteme,

sich alle in Kapitel 4 vorgestellten Verfahren hinsichtlich der Besitzer nicht verlorener Geräte perfekt anonymisieren lassen.

Die resultierenden Protokolle sollen im folgenden angegeben und hinsichtlich ihrer Komplexität mit dem nicht anonymen Fall verglichen werden.

Da bei allen Weitergabeverfahren für perfekte Anonymität auf zusätzliche pseudozufällige Kennzeichnung verzichtet werden mußte, die Anonymitätseinbuße beim Verzicht auf die Verbergung der Gleichheit von Vermerken unter der Voraussetzung, daß alle Vermerke einzeln abgeliefert werden, aber sehr gering zu sein scheint (vgl. Anfang von 5.2.3), wird auch das nicht perfekt anonyme Verfahren der pseudozufälligen Kennzeichnung nach 5.2.1.2.2.2 einbezogen.

Das Modell A2 wird in der Form betrachtet werden, daß sichere Geräte zwischen sicheren und unsicheren Geräten unterscheiden können, aber die Bank nur unsichere Geräte verwendet. Dies erfordert natürlich, daß die Zahlungsprotokolle Transaktionen mit einem sicheren Gerät und Transaktionen mit der unsicheren Bank unterschiedlich behandeln.

Es sei erwähnt, daß alle Verfahren zur verteilten Änderungsaufzeichnung auch in ihrer anonymisierten Version gestatten, die Aufzeichnung eines Gerätes in einem „Rücksetzpunkt" zu sichern, indem ein Gerät anonym all seinen Besitz an ein zweites, sichereres transferiert und sofort wieder von diesem zurückerhält.

5.3.1 Weitergabeverfahren

5.3.1.1 Protokolle

Die anonymisierten Versionen der in 4.2 beschriebenen Weitergabeverfahren unterscheiden sich vom nicht anonymen Fall so minimal, daß auf eigene Protokollskizzen verzichtet werden kann; statt dessen genügt es, nur die Änderungen gegenüber dem nicht anonymen Fall anzugeben. Dabei braucht nur zwischen Überdeckungsverfahren und verteilten Kontoständen unterschieden zu werden.

In der **Initialisierungsphase** müssen die sicheren Geräte zusätzlich die Schlüssel s_G und bei Verwendung zusätzlicher Kennzeichen die Startwerte q_G festlegen.

Im **Zahlungsprotokoll** werden in den Vermerken die Gerätekennzeichen G ersetzt: statt (G,b,T_G) bzw. im Verfahren der verteilten Kontostände, vgl. 4.2.1.4, (G,K_G,T_G)) haben sie nun die Form

$$(s_G,b,T_G) \text{ bzw. } (s_G,K_G,T_G)$$

bzw. bei Verwendung zusätzlicher Kennzeichen die Form

$$(Z_V,s_G(b,T_G)) \text{ bzw. } (Z_V,s_G(K_G,T_G))$$

Im folgenden soll mit L^* stets angedeutet sein, daß ein aufzeichnendes Gerät Gi im Falle reiner Verschlüsselung mit Redundanz die Vermerke der Liste L mit Redundanz verschlüsselt hat, d.h. die Vermerke nehmen die Form

$$s_G(r_i,b,T_G) \text{ bzw. } s_G(r_i,K_G,T_G)$$

an, wobei r_i ein vom aufzeichnenden und übergebenden Gerät Gi pseudozufällig für jeden Vermerk getrennt gewählter Teil ist.

Die Art der Weitergabe richtet sich bei reiner Verschlüsselung mit Redundanz nach dem Partner:

- Ist der Partner ein unsicheres Bankgerät, so erhält er die Liste in der verschlüsselten Form L^*. Die Vermerke in L müssen in späteren Transaktionen nicht mehr weitergegeben werden.

  Da ein Vermerk von einem Gerät nicht mehrmals mit derselben Verschlüsselung und Kennzeichnung der Bank übergeben werden sollte, müssen die Vermerke der Liste L als bereits weitergegeben gekennzeichnet werden. Ohne zusätzliche Kennzeichen würde natürlich auch die Verwendung eines anderen zufälligen Teiles r genügen und bereits übergebene Vermerke könnten gelöscht werden.

  Von der Bank erhält ein Gerät keine Vermerke, da der Bank übergebene Informationen nach Annahme nicht verloren gehen können (abgesehen davon, daß die Bank keine Vermerke im Klartext weitergeben könnte).
- Ist der Partner ein sicheres Benutzergerät, so wird wie im nicht anonymen Fall verfahren, wobei allerding gelöschte oder zum Löschen markierte Vermerke nicht mehr weitergegeben werden.

Beim **Ungültigwerden** werden der Bank von den nicht verlorenen Geräten die Listen L verschlüsselt als L^* anonym übergeben (vgl. 5.2.2), von den Besitzern verlorener Geräte erhält die Bank deren Schlüssel s_G und ggf. deren Startwerte q_G.

5.3.1.2 Aufwand

Da die sicheren Geräte auch im nicht anonymen, verlusttoleranzlosen Fall zur Gewährleistung der Sicherheit über die Fähigkeit zum Verschlüsseln verfügen müssen, ändern sich durch die Anonymisierung die prinzipiellen Anforderungen an die sicheren Geräte nicht.

Der Speicherbedarf der Geräte erhöht sich im Vergleich zum nicht anonymen Fall um einen konstanten Faktor, der bestimmt ist durch die Länge der Schlüssel s_G bzw. der Kennzeichen Z_V und verschlüsselter Nachrichten im Vergleich zu den im nicht anonymen Fall verwendeten Gerätekennzeichen G.

Die folgende Betrachtung des Rücksetzaufwands der Bank beschränkt sich auf die Verfahren der maximalen Weitergabe (4.2.1), der verteilten Kontostände (4.2.1.4) und der minimalen Überdeckungen durch Standardwerte (4.2.3), da schon im nicht anonymen Fall der Aufwand nur für diese einigermaßen genau angegeben werden kann.

Zum Rücksetzen muß die Bank wie im nicht anonymen Fall zunächst aus der Liste der erhaltenen Vermerke die verlorene Geräte betreffenden herausfiltern. Nur von diesem Schritt, der aber meistens (bei verteilten Kontoständen sogar immer) den Hauptaufwand ausmacht, muß der Aufwand neu bestimmt werden, da der Rest der Rücksetzprozedur mit den entschlüsselten Vermerken über die verlorenen Geräte völlig wie bisher verläuft.

Die maximale Länge der Liste der erhaltenen Vermerke ist bei maximaler Weitergabe $g \bullet p \bullet z \bullet g$, bei Kontoständen $g \bullet g$ und bei Standardwertüberdeckungen $g \bullet p \bullet z \bullet f \bullet d$. Die Tatsache, daß die Bank schon während des Zahlungsprotokolles Vermerke erhält, ändert nämlich an der maximalen Gesamtlänge nur dann etwas, wenn ein Vermerk insgesamt mehr als g mal abgeliefert werden kann, d.h. nur bei redundanter Verschlüsselung ohne zusätzliche Kennzeichnung, wenn solche Vermerke nicht als gelöscht gekennzeichnet, sondern sofort gelöscht werden. Da dieses Löschen auch den maximalen Speicheraufwand der sicheren Geräte nicht verbessert, sollte es daher nicht verwendet werden.

5.3.1.2.1 Verschlüsselung mit Redundanz

Bei Kennzeichnung durch Verschlüsselung mit Redundanz geschieht die Auswahl der verlorene Geräte betreffenden Vermerke durch probeweises Entschlüsseln jedes der erhaltenen Vermerke mit jedem der $p \bullet v \bullet g$ erhaltenen Schlüssel der verlorenen Geräte.

Hierdurch wird gegenüber dem nicht anonymen Fall der in $p \bullet v \bullet g$ logarithmische Suchschritt durch einen linearen ersetzt, so daß sich der Aufwand bei allen Verfahren im O-Kalkül um den Faktor

$$\frac{p \bullet v \bullet g}{\log(p \bullet v \bullet g)}$$

erhöht, wozu noch ein konstanter Faktor kommt, da Entschlüsseln aufwendiger als die Grundoperationen des Suchens ist.

Bei Verzicht auf das Verbergen der Gleichheit von Vermerken innerhalb dieses Verfahrens könnte je nach den Parametern das Vorsortieren der $g \bullet p \bullet z \bullet g$ bzw. $g \bullet g$ bzw. $g \bullet p \bullet z \bullet f \bullet d$ erhaltenen Vermerke zum Zwecke der Beseitigung mehrfach auftretender Vermerke vor den Entschlüsselungsversuchen günstig sein. Asymptotisch dominiert dann der Sortieraufwand, so daß der Aufwand gegenüber dem nicht anonymen Fall um den Faktor

$$\frac{\log(g \bullet p\bullet z\bullet g)}{\log(p\bullet v\bullet g)} \text{ bzw. } \frac{\log(g\bullet g)}{\log(p\bullet v\bullet g)} \text{ bzw. } \frac{\log(g \bullet p\bullet z\bullet f\bullet d)}{\log(p\bullet v\bullet g)}$$

steigt.

5.3.1.2.2 Pseudozufällige Kennzeichen

Bei Verwendung zusätzlicher pseudozufälliger Kennzeichen muß zur Auswahl der verlorene Geräte betreffenden Vermerke zunächst für jedes der p•v•g verlorenen Geräte jedes seiner im Mittel c•p•z möglichen Kennzeichen erzeugt und sodann mit den Kennzeichen der g • p•z•g bzw. g•g bzw. g • p•z•f•d erhaltenen Vermerke verglichen werden. Der Aufwand der Erzeugung fällt dabei im O-Kalkül weg, da dieselbe Liste danach noch einmal mit nicht konstantem Aufwand pro Eintrag durchgearbeitet wird; praktisch kann er jedoch bei gewissen Parametern wesentlich sein, da die Erzeugung eines einzelnen Kennzeichens als kryptographische Operation relativ langsam ist. Zum Vergleich wird die kürzere der zu vergleichenden Listen wieder vorsortiert.

Für die drei Verfahren ist dies genau dann die Liste der erzeugten Kennzeichen, wenn

$$c\bullet p\bullet z \bullet p\bullet v\bullet g \;\le\; g \bullet p\bullet z\bullet g \text{ bzw. } g\bullet g \text{ bzw. } g \bullet p\bullet z\bullet f\bullet d,$$

d.h.

$$c \bullet p\bullet v \;\le\; g \text{ bzw. } \frac{g}{p\bullet z} \text{ bzw. } f\bullet d,$$

was, geht man z.B. von $p\bullet v \le \frac{1}{5}$ und $c \le 50$ aus, bei allen Systemen ab einer gewissen Größe erfüllt sein dürfte.

Damit muß im Aufwand der Suchfaktor $\log(p\bullet v\bullet g)$ durch den Faktor $\log(c\bullet p\bullet z \bullet p\bullet v\bullet g)$ ersetzt werden. Der Aufwand erhöht sich also um den Faktor

$$\frac{\log(c\bullet p\bullet z \bullet p\bullet v\bullet g)}{\log(p\bullet v\bullet g)} \;=\; 1 + \frac{\log(c\bullet p\bullet z)}{\log(p\bullet v\bullet g)},$$

(für $c\bullet p\bullet z < p\bullet v\bullet g$ also im O-Kalkül gar nicht).

5.3.1.2.3 Vergleich der Kennzeichnungsverfahren

Bei Verzicht auf das Verbergen der Gleichheit von Vermerken erweist sich bei allen drei betrachteten Weitergabeverfahren die Verwendung zusätzlicher pseudozufälliger Kennzeichen als der reinen Verschlüsselung mit Redundanz und Vorsortieren der Liste der erhaltenen Vermerke überlegen, da, wie gerade in 5.3.1.2.2 gezeigt, die Liste der c•p•z • p•v•g erzeugten Kennzeichen kürzer ist als die der g • p•z•g bzw. g•g bzw. g • p•z•f•d erhaltenen.

Daher ist nur noch zwischen dem perfekt anonymen Verfahren der unterschiedlichen Verschlüsselung mit Redundanz und dem nicht ganz anonymen der pseudozufälligen Kennzeichen abzuwägen. Die Aufwände verhalten sich dabei wie p•v•g zu $\log(c\bullet p\bullet z \bullet p\bullet v\bullet g)$, d.h. letzteres ist günstiger, wenn

$$\log(c\bullet p\bullet z \bullet p\bullet v\bullet g) \le p\bullet v\bullet g \quad\Leftrightarrow\quad c\bullet p\bullet z \le \frac{2^{p\bullet v\bullet g}}{p\bullet v\bullet g},$$

was für größere Systeme meist gilt: ist z.B. $p\bullet v\bullet g \ge 20$, so ist es für $c\bullet p\bullet z \le 50\,000$ erfüllt.

Somit ist bei Verwendung eines Weitergabeverfahrens im Einzelfall zu entscheiden, ob der Rücksetzaufwand des perfekt anonymen Verfahrens zu verkraften ist, im anderen Fall kann man auf pseudozufällige Kennzeichen ausweichen.

Es sei zum Schluß angemerkt, daß speziell beim Verfahren der maximalen Weitergabe und der Verwendung zusätzlicher Kennzeichen auf die Festlegung von C_G verzichtet werden kann, wenn die

Bank die Aufzeichnungen der Geräte im Zusammenhang übergeben bekommt: da jede Liste L_G mit jedem Vermerk über ein Gerät H auch alle früheren Vermerke über H enthält, könnte die Bank mit der Suche nach Vermerken über H in L_G aufhören, sobald sie ein Kennzeichen von H nicht mehr gefunden hat.

Damit kann zum Rücksetzen darauf verzichtet werden, gleich zu Beginn die gesamte Liste der p•v•g • c•p•z Kennzeichen verlorener Geräte zu erzeugen, sondern diese kann fallweise, d.h. wenn in einer Liste L_G einmal alle schon erzeugten Kennzeichen eines Gerätes gefunden wurden, erweitert werden. Dabei ist aber auf den Aufwand zu achten, da jede Erweiterung einen erneuten Durchgang durch die maximal g • p•z•g erhaltenen Vermerke verursacht.

5.3.2 Markierte Standardwerte

5.3.2.1 Protokolle

Wie für die Weitergabeverfahren unterscheiden sich auch hier die anonymisierten Versionen nur minimal von den nicht anonymen:

Die **Initialisierungsphase** sowie das **Ungültigwerden** werden wie in 5.3.1 für die Weitergabeverfahren beschrieben gehandhabt.

Im **Zahlungsprotokoll** wird wieder nur die Form der Vermerke geändert.

Diesmal stehen zur perfekten Anonymisierung zwei Alternativen zur Auswahl, weshalb im Gegensatz zu den Weitergabeverfahren auf eine zusätzliche Betrachtung nicht perfekt anonymer Verfahren verzichtet wird. Dabei bezeichne m die maximale Zahl von Geräten, die gemäß der vorgegebenen Weitergabestrategie denselben Vermerk aufzeichnen können. Es handelt sich für einen Vermerk jeweils um die unterschiedliche (bei m>1) Verschlüsselung mit Redundanz (vgl. 5.2.1.2.2.1 bzw. 5.2.3.1.1)

- ohne zusätzliche Kennzeichen oder
- mit dynamisch bestimmten Kennzeichen gemäß 5.2.3.1.2.2, was insbesondere für m << g sinnvoll ist und für m=1 das Verfahren aus 5.2.1.2.2.2 als Spezialfall enthält.

Dabei ist noch zu beachten, daß für markierte Standardwerte mit beiden Verfahren gemäß 5.2.3.2 sogar die Anonymität gegen Angreifer des Modelles A3 erreicht werden kann. Der Preis hierfür ist natürlich die Einschränkung der Weitergabestrategien und damit der Verlusttoleranz: nur das einen Vermerk erzeugende Gerät darf diesen weitergeben.

Hinsichtlich der Unterscheidung zwischen einem sicheren Gerät als Partner und der Bank als Partner gilt das bereits in 5.3.1 für Weitergabeverfahren Gesagte.

Hinsichtlich der Sicherheit der Besitzer verlorener Geräte gegenüber Betrugsversuchen durch die Bank sei auf 4.3.1.4 verwiesen: sie ist mit den dort geschilderten Verfahren nur im Angreifermodell A2 (damit natürlich auch A1, A0) gewährleistet, nicht jedoch in A3.

Legt man jedoch statt A3 das abgeschwächte Angreifermodell A3 (vgl. 5.2.3.2) dem Betrüger zugrunde, so kann dennoch ein eingeschränkter Schutz gegen das Hinzuerfinden beliebiger Vermerke durch die Bank erreicht werden: statt einen Signierschlüssel für jedes Gerät (wie für die Weitergabeverfahren) oder einen für alle Geräte (wie bei den markierten Standardwerten für A2) zu wählen, wird einfach jedem Standardwert N bei dessen Ausgabe an ein sicheres Gerät durch dieses ein Signierschlüssel zugeordnet und der entsprechende Testschlüssel der Bank übergeben und veröffentlicht. Dieser Schlüssel wird zwischen den (wirklich oder vermeintlich) sicheren Geräten

zusammen mit N weitergereicht und bei der Übergabe eines Vermerkes über N an die Bank zum Unterschreiben desselben verwendet. Damit kann die Bank nur noch für die Standardwerte neue Einträge erfinden, die eines ihrer sicheren Geräte selbst einmal besaß.

5.3.2.2 Aufwand

Für die einfache Weitergabe ändern sich wie bei den Weitergabeverfahren (5.3.1.2) die prinzipiellen Anforderungen an die sicheren Geräte nicht. Der Speicheraufwand in ihnen steigt ohne Verwendung zusätzlicher Kennzeichen wieder um einen konstanten, durch die Länge der Schlüssel s_G im Vergleich zu den Gerätekennzeichen bestimmten Faktor. Bei Verwendung zusätzlicher Kennzeichen tritt analog ein durch s_G und die Z_V bestimmter Faktor auf.

Entsprechendes gilt für die m-fache Weitergabe ohne zusätzliche Kennzeichen. Mit zusätzlichen dynamisch bestimmten Kennzeichen gemäß 5.2.3.1.2.2 muß jedoch jedes Gerät, das entweder direkt oder indirekt einen Vermerk noch k mal weitergeben kann, k Paare aus Namen und Kennzeichen (wobei statt der Kennzeichen auch deren Index in einer Zufallsfolge stehen kann) speichern.

Bei Verwendung einer deterministischen Weitergabestrategie ist der zusätzliche Speicheraufwand durch m^2 Paare beschränkt, da gemäß 4.3.2.1 ein Gerät höchstens m-1 Vermerke zur Weitergabe bereithalten und zu jedem solchen Vermerk höchstens m Paare speichern muß.

Der genaue zusätzliche Speicherbedarf hängt natürlich von der gewählten Strategie ab, deren Weitergabebaum im folgenden mit WB bezeichnet sei.

Zu jedem inneren Knoten von WB müssen ebenso viele Kennzeichen gespeichert werden, wie dieser Knoten nachfolgende Blätter in WB besitzt. Statt jedoch zur Bestimmung des maximalen zusätzlichen Speicherbedarfes für alle inneren Knoten die nachfolgenden Blätter zu zählen, kann man auch für jedes Blatt die vorangehenden inneren Knoten zählen, d.h. einfach die Tiefen der Blätter addieren. Bezeichnet also t(WB) die Anzahl der insgesamt maximal zu speichernden Kennzeichen, so bezeichnet $\frac{t(WB)}{m}$ die mittlere Tiefe von WB.

Dank dieser Betrachtung erkennt man nun auch leicht die beiden möglichen Grenzfälle, die gerade den beiden in 4.3.2.1 erwähnten Verfahren entsprechen:

- Ist WB zur Liste entartet, so ist

$$t(WB) = (m-1) + \ldots + 1 = \frac{m \bullet (m-1)}{2}$$

  Dies ist gerade der schlechteste Fall: Angenommen, ein nicht entarteter Baum WB' mit m Blättern habe die maximale Anzahl t(WB'). Dann wähle man ein tiefstes Blatt aus WB', genannt b, sowie einen Unterbaum mit einem Vater V und zwei Blättern b1 und b2, die von b verschieden seien. Da WB' nicht entartet ist, existiert ein solcher Unterbaum. Die Tiefe von b sei t_b, die von V t_V.

  Aus WB' konstruiere man nun einen Weitergabebaum WB", indem man die Blätter b1 und b2 von V entferne und an das Blatt b hänge. In WB" wird dadurch V zum Blatt und b zum Vater von b1 und b2, womit WB" wie WB' m Blätter besitzt. Entsprechend dieser Umwandlung von Blättern in innere Knoten und umgekehrt gilt

$$t(WB") = t(WB') - t_b - 2\bullet(t_V+1) + 2\bullet(t_b+1) + t_V = t(WB') + t_b - t_V$$

  Da b ein tiefstes Blatt war, muß gelten $t_b > t_V$, d.h. $t(WB") > t(WB')$, d.h. WB' war kein Baum mit maximalem Wert t(WB').
- Ist WB ein vollständiger Weitergabebaum der Tiefe $t = \log(m)$, so ist

$$t(WB) = 2^t \bullet t = m \bullet \log(m)$$

Allgemein stellen ausgewogene Bäume gerade den besten Fall dar: Angenommen, ein nicht ausgewogener Baum WB' mit m Blättern habe die minimale Anzahl t(WB'). Sei b1 ein tiefstes Blatt darin, t_1 seine Tiefe, b2 sein Bruderblatt und V sein Vater. Da WB' nicht ausgewogen ist, gibt es ein weiteres Blatt b3 mit Tiefe t_3, für die $t_3 \leq t_1 - 2$ gilt.

Aus WB' konstruiere man nun einen Weitergabebaum WB", indem man die Blätter b1 und b2 von V entferne und an das Blatt b3 hänge. Analog zum obigen Fall hat WB" m Blätter und es gilt

$$t(WB") = t(WB') - t_3 + 2\bullet(t_3+1) - 2\bullet t_1 + (t_1-1) = t(WB') - (t_1 - t_3 - 1)$$

Wegen $t_3 \leq t_1 - 2 < t_1 - 1$ folgt $t(WB") < t(WB')$, d.h. WB' war kein Baum mit minimalem Wert t(WB').

Zum Rücksetzen muß die Bank nun in jedem Fall aus den WL-Listen der erhaltenen Vermerke die verlorene Geräte betreffenden herausfiltern, um diese entschlüsseln zu können, womit sie im nicht anonymen Fall, dort allerdings aus Aufwandsgründen, auch begann. Die Liste BL der im Besitz der Bank befindlichen, d.h. nicht verlorenen, Standardwerte ist unverschlüsselt, so daß alle weiteren Schritte wie im nicht anonymen Fall verlaufen. Daher muß, wie bei den Weitergabeverfahren, der Aufwand nur für diesen ersten Schritt neu bestimmt werden, der wiederum leider meist den Hauptaufwand ausmachte.

Da sich die Aufwände bei Verzicht auf eine gleichzeitige Systemterminierung nur durch konstante Faktoren von denen für eine gleichzeitige Systemterminierung unterscheiden, soll von letzterem ausgegangen werden.

Die Bank erhält also m • g • p•z•f Vermerke zur Auswertung. Vermerke, die sie während des Zahlungsprotokolles erhält, erhöhen diese Zahl wieder nicht, sofern in dem (meist wohl sowieso zu speicheraufwendigen) Fall, daß Vermerke beliebig oft weitergegeben werden (also m=g), wieder verlangt wird, daß ein Gerät einen schon an die Bank übergebenen als gelöscht kennzeichnet.

5.3.2.2.1 Verschlüsselung mit Redundanz

Bei Kennzeichnung durch Verschlüsselung mit Redundanz geschieht die Auswahl der verlorene Geräte betreffenden Vermerke durch probeweises Entschlüsseln jedes der erhaltenen Vermerke mit jedem der p•v•g erhaltenen Schlüssel der verlorenen Geräte.

Hierdurch wird gegenüber dem nicht anonymen Fall wieder der in p•v•g logarithmische Suchschritt durch einen linearen ersetzt, so daß sich der Aufwand um den Faktor

$$\frac{p\bullet v\bullet g}{\log(p\bullet v\bullet g)}$$

erhöht, mal einen konstanten Faktor für den Entschlüsselungsaufwand.

Dieser Faktor ist natürlich unabhängig davon, ob die Verschlüsselung vom erzeugenden oder vom aufzeichnenden Gerät vorgenommen wird.

5.3.2.2.2 Pseudozufällige Kennzeichen

Bei Verwendung zusätzlicher pseudozufälliger Kennzeichen muß zur Auswahl der verlorene Geräte betreffenden Vermerke zunächst für jedes der p•v•g verlorenen Geräte jedes seiner möglichen m • c • p•z•f Kennzeichen erzeugt werden. Diese insgesamt p•v•g • m • c • p•z•f Kennzeichen müssen mit den Kennzeichen der g • m • p•z•f erhaltenen Vermerke verglichen werden. Hierzu wird die kürzere der zu vergleichenden Listen wieder vorsortiert.

Dies ist genau dann die der erzeugten Kennzeichen, wenn gilt

$$p•v•g • m • c • p•z•f \le g • m • p•z•f \quad \Leftrightarrow \quad c \le \frac{1}{p•v} \ .$$

Geht man von $c \le 5$ und $p•v \le \frac{1}{5}$ aus, so ist dies erfüllt; bei anderer Festlegung kann das umgekehrte Verfahren noch etwas besser sein.

Damit erhöht sich der Aufwand um den Faktor

$$\frac{\log(p•v•g • m • c • p•z•f)}{\log(p•v•g)} = 1 + \frac{\log(m • c • p•z•f)}{\log(p•v•g)}$$

5.3.2.2.3 Vergleich der beiden Kennzeichnungsverfahren

Die zusätzliche Kennzeichnung erweist sich im asymptotischen Vergleich als vorteilhaft, wenn gilt

$$\log(p•v•g • m • c • p•z•f) \le p•v•g \quad \Leftrightarrow \quad m • c • p•z•f \le \frac{2^{p•v•g}}{p•v•g}$$

Schätzt man $m \le 2•p•v•g$ (da bereits $m=p•v•g+1$ garantiert, daß jeder Vermerk, der tatsächlich an m Geräte weitergegeben werden konnte, aufgefunden wird, noch häufigeres Speichern sich also nicht lohnt), $p•v•g \ge 30$ und $f \le 10$, so genügt

$$c•p•z \le \frac{2^{p•v•g}}{20•(p•v•g^2)} \quad \Leftarrow \quad c•p•z \le \frac{2^{30}}{20•(2^{10})} \approx 50000$$

was meist erfüllt sein dürfte.

5.3.2.2.4 Eingeschränkte Anonymität

Eine, allerdings nur geringfügige, Verbesserung des Aufwandes zum Rücksetzen kann durch eine ebenfalls geringfügige Verschlechterung der Anonymität erreicht werden:

Verzichtet man darauf, in Weitergabevermerken (G,N,z) auch die „harmlosen" Teile (N,z) zu verschlüsseln (womit natürlich auch die Verfahren aus 5.2.3 hinfällig werden), so bietet sich folgende Rücksetzprozedur analog der gegen Ende von 4.3.2.2.1 erwähnten, im nicht anonymen Fall asymptotisch nicht günstigsten, an (wobei der Einfachheit halber von einer gleichzeitigen Systemterminierung ausgegangen werden kann):

- Man erzeugt sich die Liste der n möglichen Standardwerte, in die die BL-Einträge immer sofort einsortiert werden,
- vergleicht die erhaltenen Vermerke mit dieser Liste, Aufwand
  $$g • m • p•z•f • \log(n),$$
  und erhält damit zu jedem Standardwert den neuesten ihn betreffenden Weitergabevermerk.
- Hieraus extrahiert man mit dem Aufwand n die $p•v•n$ verlorenen Standardwerte und
- bestimmt schließlich mit Hilfe der anonymen Kennzeichnung dieser $p•v•n$ Werte deren Besitzer.

Letzteres erfordert bei Kennzeichnung durch Verschlüsselung mit Redundanz

$$p•v•n • p•v•g$$

Entschlüsselungen, bei Verwendung zusätzlicher Kennzeichen

$$p•v•g • m • c • p•z•f • \log(p•v•n)$$

Vergleiche, wobei dieser Aufwand für $p•v • c \le 1$ durch $g • m • p•z•f • \log(n)$ dominiert wird.

Die Verwendung zusätzlicher Kennzeichen ist genau dann günstiger, wenn

$$g • m • p•z•f • \log(n) \le p•v•n • p•v•g$$

$$\Leftrightarrow \quad \frac{m • p•z•f}{(p•v)^2} \le \frac{n}{\log(n)}$$

was, der Divergenz der rechten Seite wegen, für hinreichend große Systeme erfüllt ist.

Verzeihlich ist die Anonymitätseinbuße natürlich nur dann, wenn zur Verbergung des aufzeichnenden Gerätes jeder Vermerk einzeln an die Bank übergeben wird, so daß der Zusammenhang zwischen den nun teilweise lesbaren Vermerken eines Gerätes weitgehend zerstört wird.

Verglichen mit dem Gesamtaufwand

$$g \bullet m \bullet p{\bullet}z{\bullet}f \bullet \log(p{\bullet}v{\bullet}g \bullet m \bullet c \bullet p{\bullet}z{\bullet}f)$$

des völlig anonymen Verfahrens aus 5.3.2.2.2 erweist sich der Anonymitätsverlust bei Verwendung zusätzlicher Kennzeichen als aufwandssenkend, wenn gilt

$$\log(n) \leq \log(p{\bullet}v{\bullet}g \bullet m \bullet c \bullet p{\bullet}z{\bullet}f)$$

Geht man von $g \bullet p{\bullet}z{\bullet}f \geq n$ aus (d.h. jeder Standardwert kann mindestens einmal transferiert werden) und nimmt $p{\bullet}v \bullet c{\bullet}m \geq 1$ an, so ist dies erfüllt.

Da der Gewinn jedoch nur den ohnehin weniger entscheidenden logarithmischen Faktor betrifft, soll diese Ersparnis in der folgenden Zusammenfassung nicht berücksichtigt werden.

5.3.3 Zusammenfassung

Die folgenden Tabellen geben für die vier wichtigsten behandelten Verfahren nochmals Auskunft über den Rücksetzaufwand für vernünftige, große Parameter (Bild 21) und über den Speicherbedarf (Bild 22).

Verfahren	Aufwand zum Rücksetzen		
	Ohne Anonymität	Erhöhung durch Anonymisierung	
		mit Kennzeichen	ohne Kennzeichen
Maximale Weitergabe	$g^2{\bullet}z{\bullet}p \bullet (\log(p{\bullet}v{\bullet}g) + p{\bullet}v \bullet \log(z{\bullet}p))$		
Verteilte Kontostände	$g^2 \bullet \log(p{\bullet}v{\bullet}g)$	$\bullet\left(1 + \frac{\log(c{\bullet}p{\bullet}z)}{\log(p{\bullet}v{\bullet}g)}\right)$	$\bullet \frac{p{\bullet}v{\bullet}g}{\log(p{\bullet}v{\bullet}g)}$
Standardwertüberdeckungen	$g \bullet p{\bullet}z{\bullet}f{\bullet}d \bullet (\log(p{\bullet}v{\bullet}g) + p{\bullet}v \bullet \log(z{\bullet}p{\bullet}f))$		
Markierte Standardwerte	$g \bullet p{\bullet}z{\bullet}f{\bullet}m \bullet \log(p{\bullet}v{\bullet}g)$	$\bullet\left(1 + \frac{\log(c{\bullet}p{\bullet}z \bullet f{\bullet}m)}{\log(p{\bullet}v{\bullet}g)}\right)$	$\bullet \frac{p{\bullet}v{\bullet}g}{\log(p{\bullet}v{\bullet}g)}$

Bild 21 Rücksetzaufwand

Für alle Verfahren ist im allgemeinen die Verwendung zusätzlicher Kennzeichen (links) günstiger als der Verzicht auf diese (rechts), wobei allerdings in allen Weitergabeverfahren die Verwendung zusätzlicher Kennzeichen einen leichten Anonymitätsverlust mit sich bringt. Hinsichtlich der prinzipiellen Aufwandsunterschiede der Verfahren ändert sich durch die Anonymisierung offenbar nichts.

Dies gilt offenbar auch für den Speicherbedarf der sicheren Geräte:

Verfahren	Speicherbedarf der sicheren Geräte	
	Ohne Anonymität	Erhöhung durch Anonymisierung
Maximale Weitergabe	Maximal g•p•z	
Verteilte Kontostände	Maximal g	+ 0
Standardwertüberdeckungen	Maximal g•p•z (im Mittel p•z•f•d)	
Markierte Standardwerte	Maximal c•p•z•f•m	+ m^2

Bild 22 Speicherbedarf der sicheren Geräte

Da maximale Weitergabe und verteilte Kontostände die gleiche Verlusttoleranz bewirken, sind verteilte Kontostände in jedem Fall günstiger.

6 Resümee

Die in den vorangegangenen Kapiteln 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. Hierzu wurden im wesentlichen zwei Klassen von Verfahren vorgestellt, die Weitergabeverfahren (vgl. 4.2) und die markierten Standardwerte (vgl. 4.3), sowie geeignete Anonymisierungsmethoden (vgl. Kap. 5).

Als erwägenswert erwiesen sich beim sinnvollsten Angreifermodell (A2 in 5.1) schließlich ein Weitergabeverfahren, die verteilten Kontostände, sowie die markierten Standardwerte mit m-facher Weitergabe. Die folgende Tabelle soll deren „Qualität" grob bewerten.

Verfahren	verteilte Kontostände	markierte Standardwerte
Autonomie	Uneingeschränkt	Leicht eingeschränkt durch das „Wechselgeldproblem”
Sicherheit	Garantiert	
Sicherheit vor Änderungen der Rücksetzinformation durch die Bank	Beliebig gut einstellbar (aber perfekt nur mit enormem Aufwand)	
Anonymität	Garantierbar	
Verlusttoleranz beliebig	Maximal realisierbare Verlusttoleranz	Durch m-fache Weitergabe einstellbar
Speicheraufwand der sicheren Geräte	Im schlechtesten Fall sehr hoch, im Mittel: unbekannt	Linear in der Anzahl der eigenen Transaktionen und der Anzahl der Weitergaben
Systemterminierung und Wartefrist bis zum Rücksetzen	Alle Geräte terminieren gleichzeitig, Rücksetzen erst nach Ende des gesamten Systems	Terminierung beliebig, die Wartezeit vom Verlustzeitpunkt bis zum Rücksetzen ist etwa 3 • Gültigkeitsdauer eines Gerätes **oder** genauso wie bei den verteilten Kontoständen
Rücksetzaufwand	Erträglich	

Bild 23 Vergleich der Verfahren

Eine eindeutige Entscheidung zwischen den beiden Verfahren ist offenbar nicht möglich.

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.

Teile dieses Berichtes wurden auf der 3. Internationale Tagung Fehlertolerierende Rechensysteme, Bremerhaven 1987 vorgetragen [WaPf_87]. Auch den Gutachtern dieser Tagung gilt unser Dank.

7 Anhang

7.1 Literatur

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

Band_81 C. Bandelow: Einführung in die Wahrscheinlichkeitstheorie; BI Hochschultaschenbücher 798, Bibliographisches Institut, Mannheim 1981

BlBS_86 L. Blum, M. Blum, M. Shub: A Simple Unpredictable Pseudo-Random Number Generator; SIAM J. Comput. 15/2 (1986) 364-383

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, Amsterdam 1988

Chau_85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044

Chau_87 D. Chaum: Sicherheit ohne Identifizierung. Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262-277

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

GaJo_79 M. R. Garey, D. S. Johnson: Computers and Intractability – A Guide to the Theory of NP-Completeness; Freeman, New York 1979

GoGM_84 O. Goldreich, S. Goldwasser, S. Micali: How to Construct Random Functions (Extended Abstract); 25th FOCS 1984, 464-479

GoMR_88 S. Goldwasser, S. Micali, R. L. Rivest: A digital signature scheme secure against adaptive chosen-message attacks; erscheint in: SIAM J. Comput. 17/2 (1988); Vorversionen in: 25th FOCS, IEEE Computer Society 1984, 441-448

GrKn_82 D. H. Greene, D. E. Knuth: Mathematics for the Analysis of Algorithms (2nd. ed.); Birkhäuser, Boston 1982

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

LuRa_87 M. Luby, C. Rackoff: How to Construct Pseudo-random Permutations from Pseudo-random Bits; Entwurf vom 24.3.1987, erscheint in: SIAM J. Comput. 17/2 (1988); Vorversion in: 18th STOC, ACM, New York 1986, 356-363

PfPW_86 A. Pfitzmann, B. Pfitzmann, M. Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Warum und wie?; Datenschutz und Datensicherung DuD Heft 3 (1986) 178-191; Überarbeitung erscheint in: Informatik-Spektrum (1988)

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; Computer und Recht CR Hefte 10, 11, 12 (1987) 712-717, 796-803, 898-904

Riha_85 K. Rihaczek: Der Stand von OSIS; Datenschutz und Datensicherung DuD 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: Verlusttolerante elektronische Brieftaschen; 3. Internationale Tagung Fehlertolerierende Rechensysteme, Bremerhaven 1987; IFB 147, Springer-Verlag, Heidelberg 1987, 36-50; Überarbeitung in: Datenschutz und Datensicherung DuD 10 (1987) 487-497

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

Yao_82 A. C. Yao: Theory and Applications of Trapdoor Functions (Extended Abstract); 23rd FOCS 1982, 80-91

7.2 Mathematische Symbole

Verwendet wurden neben den allgemein üblichen Symbolen der Arithmetik und Mengenlehre:

E(X), V(X) Erwartungswert bzw. Varianz von X [Band_81]

O, Ω, Θ Asymptotischer Vergleich von Funktionen [GrKn_82 Seite 47]:

$f = O(g) \quad :\Leftrightarrow \quad \exists\, N, K\ \forall\, n \geq K: \left| f(n) \right| \leq K \bullet g(n)$

$f = \Omega(g) \quad :\Leftrightarrow \quad \exists\, N, K\ \forall\, n \geq K: f(n) \geq K \bullet g(n)$

$f = \Theta(g) \quad :\Leftrightarrow \quad f = O(g) \text{ und } f = \Omega(g)$