Betrugssicherheit durch kryptographische Protokolle beim Wertetransfer über Kommunikationsnetze*

Michael Waidner

Abstrakt: *Ein* **offenes digitales System** *soll allen Teilnehmern eines Kommunikationsnetzes, z.B. des ISDN, zugänglich sein und spezielle Dienste anbieten, die das Anbieten und Bestellen von Waren aller Art, das Überweisen von Geld, kurz das Abwickeln von* **Rechtsgeschäften** *verschiedenster Art erlauben. Bereits im heutigen BTX-System sind einfache* **Wertetransferprotokolle,** *d.h.* **Zahlungssysteme** *und Protokolle zum Transfer digitaler Waren* **(Warentransferprotokolle),** *im Einsatz.*

Die Benutzung solcher Protokolle muß unter Wahrung der aus dem Alltag gewohnten **Betrugssicherheit** *und* **Anonymität** *erfolgen. Beides muß zwar juristisch geregelt, kann aber nur durch technische Maßnahmen* **sichergestellt** *werden. Die in heutigen Systemen ergriffenen technischen Maßnahmen erfüllen diese Forderung nur sehr* **unzureichend.**

Das dargestellte Projekt „Betrugssicherheit" verfolgt das Ziel, Hilfsmittel und Wertetransferprotokolle zu entwickeln, die beweisbare Betrugssicherheit und Anonymität garantieren, ohne dabei einen nennenswert höheren Aufwand als die heute üblichen unsicheren Protokolle zu verursachen.

Die bisherigen Projektarbeiten führten zu einer abschließenden Spezifikation sicherer und anonymer Wertetransferprotokolle. Ebenfalls abschließend behandelt wurde der die Betrugssicherheit ergänzende Aspekt der Fehlertoleranz für Wertetransferprotokolle.

Noch offen sind hingegen einige Probleme im Bereich der Hilfsmittel (Datenschutz garantierende Kommunikationsnetze, unverkettbare nur einmal gültige Beglaubigungen) und der Verifikation und Realisierung von Wertetransferprotokollen.

0 Einleitung

Das Projekt *„Betrugssicherheit durch kryptographische Protokolle beim Wertetransfer über Kommunikationsnetze"* wird seit September 1986 von der DFG gefördert[1] und am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe durchgeführt.

Die Notwendigkeit der Untersuchung von Wertetransferprotokollen läßt sich sinnvoll nur im Kontext eines **offenen digitalen Systems** verstehen.[2]

Ein solches System soll potentiell allen Benutzern eines Kommunikationsnetzes, z.B. des von der Post geplanten ISDN, zugänglich sein und spezielle Dienste anbieten. Möglichkeiten sind reine Informationsdienste, etwa in der Nachfolge von Bildschirmtext, die ihren Benutzern spezielle Datenbanken zugänglich machen, die Verbreitung von POS-Terminals oder „elektronische Marktplätze", die den Benutzern das Anbieten und Bestellen von Waren, das Überweisen von Geld, kurz das Abwickeln von **Rechtsgeschäften** verschiedenster Art erlauben.

Dies muß einerseits unter Wahrung der aus dem Alltag gewohnten **Rechtssicherheit** erfolgen. Andererseits muß aber auch der **Datenschutz** (im Sinne von **Unbeobachtbarkeit** der Benutzung durch Unbeteiligte und **Anonymität** vor Beteiligten) der Benutzer mindestens ebenso gut gewährleistet sein, wie in den heutigen, nicht-digitalen Systemen. Beides muß zwar *juristisch* geregelt, kann aber durch juristische Maßnahmen alleine nicht sichergestellt werden.

Zur Abhilfe sind daher *technische* Maßnahmen notwendig. Diese umfassen einerseits Maßnahmen zur Sicherstellung der Unbeobachtbarkeit und Anonymität der Benutzung des Kommunikationsnetzes (vgl. Kap. 3), ohne die alle weiteren Anonymisierungsversuche sinnlos wären, sowie **kryptographische Grundsysteme** (Signatursysteme, Kryptosysteme) zur Realisierung der die Rechtsgeschäfte unterstützenden Protokolle.

Ein **Wertetransferprotokoll** soll es den Benutzern des offenen digitalen Systems erlauben, über das Kommunikationsnetz Werte zu übertragen.

Besteht der zu transferierende Wert im Besitz von **Geld,** d.h. einem abstrakten Recht, das durch das Protokoll von einem Benutzer auf den anderen *nachweisbar* (d.h. gegen entsprechende Quittungen) übertragen werden soll, so spricht man von einem **(digitalen) Zahlungssystem.**

Besteht der Wert in einer **digitalen Ware,** d.h. einer Information, die von einem wissenden einem unwissenden Benutzer im Austausch gegen einen entsprechenden Geldbetrag übergeben werden soll, so spricht man von einem **(digitalen) Warentransferprotokoll.** Diese Definition setzt bereits die Existenz eines Zahlungssystems voraus. Mögliche digitale Waren sind z.B. Tageszeitungen oder die Ergebnisse von für den daran Interessierten allzu komplexen Berechnungen.

Ein Wertetransferprotokoll ist **betrugssicher,** wenn ein Benutzer keinen endgültigen materiellen Schaden (z.B. Verlust von Geld) erleiden kann, solange er sich selbst an sein Protokoll hält.

Alle *anderen* Benutzer können beliebig von ihrem Protokoll abweichen. Manches denkbare Verhalten wird jedoch durch das **Angreifermodell** als unmöglich ausgeschlossen,

* Dies ist eine überarbeitete Fassung von [64a].

z.B. das „Brechen" der verwendeten Krypto- und Signatursysteme (vgl. Kap. 5).

Zur Erzielung von Betrugssicherheit muß im allgemeinen die Existenz eines vertrauenswürdigen **Gerichtes** vorausgesetzt werden, das anhand ihm vorzulegender **Beweismittel** den Sachverhalt rekonstruieren und entstandenen **Schaden** innerhalb einer allgemein bekannten Frist **regulieren** soll. Verwendet man z.B. ein Zahlungssystem, bei dem jeder Geldtransfer von einer Bank bezeugt werden muß (vgl. Kap. 2), so könnte man ohne Gericht den Benutzern die Verfügbarkeit über ihr Geld nicht mehr garantieren.

Speziell im *anonymen* Fall ist natürlich darauf zu achten, daß ein „braver" Benutzer sich nicht deanonymisieren muß, um zu seinem Recht zu gelangen, und umgekehrt, daß im Falle einer Schadensregulierung zu Lasten eines anderen anonymen Benutzers genügend Sicherheiten vorhanden sein müssen.

Verwendet ein Benutzer ein Wertetransferprotokoll zwar *irrtümlich*, aber in *formal korrekter* Weise, so kann ihm die Rückholbarkeit einer geleisteten Zahlung oder ein wirksamer Widerruf einer getätigten Bestellung *nicht* garantiert werden. Dies widerspräche einerseits der Forderung nach *garantierter* Schadensregulierung (da ja erhaltenes Geld längst ausgegeben worden sein kann), andererseits kann von einem *anonymen* Partner gegen dessen Willen prinzipiell keine geleistete Zahlung zurückgeholt werden.

Solche Irrtümer müssen daher durch eine geeignete Gestaltung der Benutzerschnittstelle (z.B. mehrfache Abfragen vor „Inkrafttreten" einer Willenserklärung) möglichst vermieden werden.

Das Ziel des Projektes, sichere und anonyme Wertetransferprotokolle zu entwerfen und zu verifizieren, wurde bei der bisherigen Bearbeitung in sechs Teilziele aufgespalten:

1. Die **Systematisierung** der anonymen und betrugssicheren digitalen Wertetransferprotokolle mit dem Ziel, eine allgemein gültige Spezifikation zu erhalten, aus der alle sinnvollen Varianten ableitbar sind.
2. Die Untersuchung der **Sicherheit** der Wertetransferprotokolle im Hinblick auf Geldverlust durch Ausfall beteiligter Rechner und die Anwendung oder Entwicklung geeigneter *Fehlertoleranzmechanismen*.
3. Die Untersuchung des für die Anonymität wichtigen Hilfsmittels der **Datenschutz garantierenden Digitalnetze.**
4. Die Untersuchung der für die Anonymität und Betrugssicherheit wichtigen kryptographischen Hilfsmittel, insbesondere der Möglichkeiten zur **unverkettbaren Verwendung nur einmal gültiger Beglaubigungen.**
5. Die Untersuchung der **Verifikationsmöglichkeiten** anonymer und betrugssicherer Wertetransferprotokolle, insbesondere die Verifikation konkreter Protokolle.
6. Die Untersuchung der **Realisierbarkeit** spezieller Wertetransferprotokolle.

Die Ergebnisse bei der Verfolgung dieser sechs Teilziele sollen in den folgenden Kapiteln jeweils kurz skizziert werden.

Die Veröffentlichungen [39, 64, 41] ergänzen diesen Arbeitsbericht durch eine ausführlichere Darstellung wichtiger Inhalte der Kapitel 1 bis 3.

Gemäß dem Wesen dieses Zwischenberichtes wird nicht angestrebt, die erhaltenen Ergebnisse in sich geschlossen darzustellen, sondern es wird lediglich versucht, dem Leser eine Hilfe bei der Sichtung der während des Projektes entstandenen Arbeiten und der neueren außerhalb des Projektes entstandenen Literatur zum Projektthema zu geben.

1 Systematisierung der Wertetransferprotokolle

1.1 Systematisierung der Zahlungssysteme

Die Bemühungen zur **Systematisierung der Zahlungssysteme** orientierten sich im wesentlichen an der in der Einleitung gegebenen Definition der *Betrugssicherheit*.[3]

Etwas konkreter lautet diese Definition: ein Zahlungssystem ist **betrugssicher**, falls

- B1 ein Benutzer erhaltenes Geld transferieren kann,
- B2 er nur dann Geld verliert, wenn er mit dem Verlust einverstanden ist,
- B3 er nur dann Geld erhält, wenn ihn ein anderer zahlungswilliger Benutzer eindeutig als Empfänger bestimmt hat,
- B4 er jeden vollzogenen Transfer einem Dritten gegenüber nachweisen kann (Quittungsproblem) und
- B5 die Benutzer auch bei Zusammenarbeit ihren Besitz an Geld nicht zu Lasten anderer Beteiligter (Benutzer, Banken usw.) vermehren können.

Da hier nur Zahlungssysteme betrachtet werden, bei denen der gesamte Transfer ausschließlich durch den Austausch digitaler Nachrichten abgewickelt wird (i.allg. über ein Kommunikationssystem), und da digitale Nachrichten beliebig kopiert werden können, das Besitzrecht an Geld aber gemäß B5 nach dem Transfer erlöschen muß, benötigt man einen **Zeugen**, der die aktuelle Gültigkeit des Rechtes garantiert.

Im allgemeinen wird eine zentrale **Bank** oder ein **sicheres Gerät** im Besitz des Benutzers (eine „elektronische Brieftasche"), die Zeugenaufgabe übernehmen. Es ist prinzipiell jedoch auch möglich, im Sinne einer „Aufgebotsprozedur" die Zeugenfunktion auf *alle* Benutzer des Zahlungssystems zu verteilen: ein Transfer eines Rechtes ist genau dann abgeschlossen, wenn jeder Benutzer davon Kenntnis erhalten hat und niemand in befristeter Zeit dagegen Einspruch erhebt.[4] Da dies aber zu unpraktikablen Protokollen führt und gegenüber einem Zahlungssystem mit einem (oder wenigen) zentralen Zeugen keinen offensichtlichen Vorteil bietet, soll diese Möglichkeit im folgenden nicht weiter betrachtet werden.

Um dem Zeugen die Erfüllung seiner Aufgabe zu ermöglichen, muß ihm jeder Geldtransfer bekannt sein, es darf also auch dann, wenn der Zahlungsempfänger dem Zahlenden vertraut, kein Transfer ohne Bestätigung durch den Zeugen stattfinden können. Dies schließt jedoch nicht aus, daß der Zeuge die Bestätigung für einen *bestimmten* Transfer bereits vor dem eigentlichen Transfer dem Zahlenden übergeben kann.

Die Alternative, gelegentlich bei Zahlungen doch auf den Zeugen zu verzichten, aber dafür zu sorgen, daß ein unerlaubt mehrfach ausgegebener Betrag zur Identifizierung und damit zur möglichen Verfolgung des Betrügers führt, ist im obigen Sinne ebenfalls unsicher. Die Regulierbarkeit entstandenen Schadens kann durch Deanonymisierung alleine prinzipiell nicht garantiert werden, was speziell hier noch durch die unbegrenzte Wiederholbarkeit des unerlaubten Weitergebens verschärft wird.

Dies vorausgesetzt, ergeben sich aus den Anforderungen B1 bis B5 diejenigen *Beweismittel*, die die Beteiligten (also Zahlender, Empfänger und Zeuge) vor und nach der Protokollausführung besitzen müssen. Dies kann als **Dienstspezifikation** im üblichen Sinne aufgefaßt werden.

Die in [39] ausführlicher dargestellten Überlegungen führen zum Grundschema (d.h. der **Protokollspezifikation**) eines sicheren und anonymen digitalen Zahlungssystems, aus dem sich alle bisher bekannten Vorschläge durch *Abschwächung* ergeben.

Die tatsächlich erzielte Betrugssicherheit und Anonymität hängt natürlich von der *Implementierung* des Protokolls ab (vgl. auch Kap. 3 bis 6).

1.2 Systematisierung der Warentransferprotokolle

Analog zur Spezifikation der Zahlungssysteme können auch die **betrugssicheren Warentransferprotokolle** beschrieben werden:

Ein solches Protokoll hat sein Ziel genau dann erreicht, wenn am Ende der *Besteller* seine gewünschte Information erhalten hat und der *Lieferant* sein entsprechendes Entgelt. Erhält der Besteller keine Information geliefert, so darf er kein Geld verlieren; will der Lieferant umgekehrt die bestellte Information liefern, so darf ihm der Besteller seine Bezahlung nicht vorenthalten können.[5] Der Warentransfer muß in diesem Sinne **unteilbar** erfolgen.

Voraussetzung für ein Warentransferprotokoll ist neben der Existenz eines im obigen Sinne sicheren Zahlungssystems die Möglichkeit, zumindest im Streitfall effektiv zu entscheiden, ob die gelieferte „Ware" dem Wunsch des Bestellers entspricht.

Die Unteilbarkeit kann zum einen durch Einschalten einer *dritten, nicht-anonymen Partei* erreicht werden, die in jedem Austausch aktiv beteiligt ist und den Austausch „Ware gegen Geld" **treuhänderisch** (und für durch sie verursachte Schäden haftend) koordiniert. Die Anonymität und Betrugssicherheit von Besteller und Lieferant bleiben erhalten ([39], Kap. 4.2).

Die in [39] Kap. 4.1 geschilderte weitere Möglichkeit, vertrauenswürdige, aber im allgemeinen *passive* Dritte vorzusehen, die im Streitfall in der Lage sind, die ansonsten anonymen Partner zu *deanonymisieren* und damit eine normale gerichtliche Verfolgung zu ermöglichen, ist im obigen Sinne nicht betrugssicher. Hierzu müßte zusätzlich garantiert werden, daß entstandener Schaden nach der Deanonymisierung reguliert werden kann, was wiederum nur möglich wäre, wenn die anonymen Partner einander genügend Sicherheiten (im Sinne des Kreditgewerbes) geboten hätten. Da diese Sicherheiten aber wiederum von einer fremden Instanz beglaubigt sein müßten, wäre damit der Vorteil, ohne einen aktiven Dritten auszukommen, dahin.

Zum anderen könnten Besteller und Lieferant die Unteilbarkeit auch durch eine aufwendige **gemeinsame Simulation** der Funktion des Treuhänders ohne dritte Partei garantieren.[6] Voraussetzung hierzu wäre allerdings, die Übereinstimmung zwischen Ware und Bestellung durch eine nur aufgrund des Vorwissens des Bestellers spezifizierte und effektiv berechenbare **Prüffunktion** entscheiden zu können. Dies wird jedoch für viele Waren, z.B. Tageszeitungen, kaum der Fall sein. Geht man davon aus, daß im allgemeinen ein Zahlungssystem mit einem zentralen Zeugen, d.h. einer Bank, verwendet wird, so ist auch bei Existenz einer passenden Prüffunktion der Vorteil, ohne eine aktive dritte Partei auszukommen, vergleichsweise gering und eher von theoretischem Interesse.

1.3 Abschließende Bemerkungen

Die hier (und auch in [39]) aufgestellten Behauptungen über die Betrugssicherheit und Anonymität der Protokolle wurden größtenteils noch *nicht* bewiesen (vgl. Kap. 5).

Außer (und zeitlich vor) dem Artikel [39] entstand im Rahmen der Bemühungen um Systematisierung der Überblicksartikel [54], der einen ersten, eher intuitiven Versuch einer Systematisierung enthielt.

Außerhalb unserer Arbeitsgruppe beschäftigte sich meines Wissens lediglich D. Chaum (CWI Amsterdam, Niederlande) mit dem Thema [9, 10, 55, 56]. Seine Ideen finden sich auch in [39].

2 Fehlertolerante Wertetransferprotokolle

Im Sinne der Fehlertoleranz würde man ein Wertetransferprotokoll dann als **sicher** bezeichnen, wenn ein Benutzer X keinen endgültigen materiellen Schaden erleiden kann, solange *alle* Benutzer (zentrale Instanzen, z.B. Banken und Treuhänder, eingeschlossen) höchstens im Rahmen eines vorgegebenen **Fehlermodelles** von ihrem protokollgemäßen Verhalten abweichen.

Da für die Betrugssicherheit stets von *geplanten Angriffen* auszugehen ist, während ein Fehlermodell üblicherweise von *zufälligen Fehlern* ausgeht, ist natürlich nicht zu erwarten, daß jedes *sichere* Wertetransferprotokoll zugleich auch *betrugssicher* ist.

Umgekehrt schließt der Ausdruck *„alle* Benutzer" bei der Fehlertoleranz auch den Benutzer X selbst mit ein, während die Betrugssicherheit diesen als fehlerfrei voraussetzen muß.

Wie einfach diese *zusätzliche* Sicherheit zu erreichen ist, hängt wesentlich davon ab, ob es den Benutzern möglich sein soll, **autonom** (d.h. ohne Kommunikation mit einer zentralen Instanz, z.B. einer Bank) Zahlungen leisten zu können.

2.1 Fehlertolerante nicht-autonome Zahlungssysteme

Ist dies *nicht* der Fall, so kann jeder Transfer durch die Bank bezeugt werden. Damit kann aber ein Benutzer beliebige Geräte für seine Kommunikation verwenden und auch jede für ihn wichtige Information beliebig redundant speichern. Damit sind alle Standardmethoden der Fehlertoleranz [2] anwendbar (wobei natürlich darauf zu achten ist, daß keine für die Anonymität oder Betrugssicherheit des Benutzers wichtigen Informationen in fremde Hände gelangen).

Fehler des zur Kommunikation verwendeten Datenschutz garantierenden Kommunikationsnetzes sind davon getrennt zu betrachten. Für eine Diskussion der hier anwendbaren Verfahren sei auf [35, 61] verwiesen.

2.2 Fehlertolerante autonome Zahlungssysteme: Verlusttolerante elektronische Brieftaschen

Will man mit einem Zahlungssystem sowohl über ein Kommunikationsnetz als auch *autonom* Zahlungen durchführen können, so ist man auf „elektronische Brieftaschen", sichere Geräte, die für die korrekte Abwicklung digitaler Zahlungen garantieren, angewiesen (vgl. Kap. 1 und [39]). Fällt ein solches Gerät aus oder geht physisch verloren, so ist damit zunächst ein Verlust von Geld verbunden. Insbesondere gegen den physischen Verlust kann man sich natürlich nicht durch zuverlässigere elektronische

Brieftaschen schützen, und auch die Verwendung mehrerer sicherer Geräte löst das Problem nicht.[7]

Zur Tolerierung der möglichen Verluste (**Verlusttoleranz**) erscheint eine Kombination zwischen *Änderungsaufzeichnung* der Transaktionen eines Gerätes und *Rücksetzpunkterstellung* notwendig.

Die Änderungsaufzeichnung kann aufgrund der Forderung nach Autonomie nicht zentral, sondern nur *verteilt* durch die sicheren Geräte selbst erfolgen, so daß hier spezielle **Weitergabeprotokolle** notwendig sind. Insbesondere dürfen diese Weitergabeprotokolle die Sicherheit und Unbeobachtbarkeit des zugrunde liegenden Zahlungssystems nicht gefährden. (So sind die üblichen einfachen wechselseitigen Änderungsaufzeichnungen, bei denen eine Transaktion von genau den beteiligten Partnern aufgezeichnet wird, unsicher: durch das Rücksetzen verlorener Geräte kann die Geldmenge im Zahlungssystem zunehmen!)

Zur Lösung des Problems wurden zwei Klassen von Verfahren vorgeschlagen und untersucht, die als **Weitergabeverfahren** bzw. **markierte Standardwerte** bezeichnete wurden.

In der ersten Verfahrensklasse wird versucht, ohne jede Einschränkung des zugrundeliegenden Zahlungssystems auszukommen. In der naiven, aber maximale Verlusttoleranz garantierenden Version der **maximalen Weitergabe** werden die Aufzeichnungen über Transaktionen möglichst vollständig an alle am Zahlungssystem beteiligten Geräte verteilt. Dies verursacht jedoch einen enormen Speicherbedarf in den sicheren Geräten. Es läßt sich auch zeigen, daß es keine Strategie zur *Einschränkung* der Weitergabe von Vermerken auf eine vernünftig kleine Anzahl von Geräten gibt, die die Sicherheit nicht gefährdet, sondern *jedes* Gerät im für den Speicherbedarf ungünstigsten Fall die *gesamte* Änderungsaufzeichnung des Zahlungssystems speichern muß.

Erste Abhilfe schafft, statt einzelner Vermerke jeweils nur deren Summe aufzuzeichnen, was als Verfahren der **verteilten Kontostände** bezeichnet wurde. Durch dieses wird die maximale Verlusttoleranz garantiert, der Speicherbedarf der sicheren Geräte ist jedoch im ungünstigsten Fall immer noch sehr hoch.

Die zweite Verfahrensklasse geht von einem Zahlungssystem aus, in dem wie im heutigen Bargeldsystem jede Zahlung durch Weitergabe einer Menge von eindeutig bezeichneten **Standardwerten** (≈ numerierte Banknoten) vorgenommen werden muß. Die Änderungsaufzeichnung besteht im einfachsten Fall darin, daß sich jedes Gerät merkt, an wen es welche Standardwerte weitergegeben hat. Ein verlorenes Gerät erhält die Standardwerte zugeschrieben, die ebenfalls verloren sind und deren letzter nachweisbarer Besitzer es war. Zur Erhöhung der Verlusttoleranz können die Vermerke beliebig weitergegeben werden; bei Speicherproblemen kann jedes Gerät hier im Gegensatz zu den Weitergabeverfahren jeden erhaltenen Vermerk ohne Gefahr für die Sicherheit des Zahlungssystems löschen.

Die Unbeobachtbarkeit kann in beiden Verfahrensklassen durch eine Kombination aus kryptographischen Techniken und der Ausnutzung der Unausforschbarkeit der elektronischen Brieftaschen garantiert werden. Hinsichtlich der *Betrugssicherheit* (einschließlich der Möglichkeit, sich vor Manipulationen der Rücksetzinformationen zu schützen) und der Einsatzmöglichkeit zusätzlicher *Rücksetzpunkterstellung* zur Sicherung eigener Änderungsaufzeichnungen sind beide Verfahrensklassen als sehr zufriedenstellend zu bewerten.

Die *Wahrung* der Betrugssicherheit wurde für alle Weitergabe- und Standardwertprotokolle in [64] *bewiesen.*

3 Datenschutz garantierende Kommunikationsnetze

Ein **Datenschutz garantierendes Kommunikationsnetz** garantiert seinen Benutzern, daß der Sender bzw. Empfänger einer Nachricht ohne dessen Mitwirkung nicht festgestellt werden kann, insbesondere auch nicht durch den Betreiber des Kommunikationssystems (was die Hauptschwierigkeit ist) oder den Kommunikationspartner.[8]

Ohne die durch ein solches Kommunikationsnetz geschaffene *Grundanonymität* der Benutzer ist der Versuch, die Anonymität der Benutzer eines Wertetransferprotokolls gewährleisten zu wollen, aussichtslos.

3.1 Überlagerndes Senden und Empfangen

Neben den Bemühungen, bereits bekannte Ergebnisse der Fachöffentlichkeit nahe zu bringen [35, 38, 49, 40, 41], galt das wissenschaftliche Hauptinteresse der Untersuchung der Realisierungsmöglichkeiten einer Methode zum (im Shannonschen Sinne) *informationstheoretisch anonymen Senden* über ein Digitalnetz, dem von D. Chaum 1985 vorgeschlagenen **überlagernden Senden** (DC-Netz [10, 14], vgl. 2.2.3.1 in [41]):

Jede Teilnehmerstation erzeugt für jedes möglicherweise zu sendende Nutzbit zufällig ein oder mehrere Schlüsselbits und teilt jedes genau einer anderen Teilnehmerstation vertraulich mit. Jede Teilnehmerstation addiert (mod2) lokal alle von ihr erzeugten Schlüsselbits, subtrahiert (mod2) davon lokal alle ihr mitgeteilten Schlüsselbits, addiert (mod2), sofern sie ein Nutzbit senden will, lokal ihr Nutzbit, und sendet die erhaltene Summe. Alle gesendeten Bits werden global addiert (mod2) und das Ergebnis veröffentlicht. Da im Ergebnis jedes Schlüsselbit genau einmal addiert und subtrahiert wurde, ist die veröffentlichte Summe gerade die Summe aller gesendeten Nutzbits. Wollte keine Station senden, ist die Summe 0, wollte genau eine Station senden, ist die Summe gleich dem gesendeten Nutzbit. Durch Iteration des Verfahrens lassen sich Nachrichten übertragen.

Dieses Grundverfahren, das auf der Addition in GF(2) basiert, wurde auf *endliche abelsche Gruppen* erweitert und die informationstheoretische Senderanonymität dieser Verallgemeinerung *bewiesen* [61]. Unter **Überlagerung** soll im folgenden die Addition in der verwendeten abelschen Gruppe verstanden werden.

Auf einem DC-Netz werden, falls mehrere Teilnehmerstationen gleichzeitig senden wollen, natürlich (*digitale*) *Überlagerungs-Kollisionen* auftreten. Da jedoch im Gegensatz zu den in Verteilkanälen mit Mehrfachzugriff üblichen und bereits gut untersuchten (*analogen*) *Übertragungs-Kollisionen* (z.B. im Ethernet) bei überlagerndem Senden das Kollisionsergebnis wohldefiniert ist (eben als die Summe aller Nutznachrichten), erschien es lohnenswert, diese Besonderheit genauer zu untersuchen.

Offenbar kann bei überlagerndem Senden jeder, der die Summe von n Nachrichten und n-1 der Summanden kennt, auch die n-te Nachricht rekonstruieren (was **überlagerndes Empfangen** genannt wurde). Nutzt man dies rekursiv aus, so erhält man Anonymität wahrende Zugriffsverfahren, die die Bandbreite des DC-Netzes erheblich besser ausnutzen als die üblichen Zugriffsverfahren: zur Übertragung von n Nachrichten sind bei den günstigsten Verfahren lediglich n Sendungen erforderlich, wobei allerdings

die einzelnen Nachrichten um einige Kontrollinformationen, für die das oben erwähnte verallgemeinerte Schema nützlich ist, erweitert werden müssen.

Die gefundenen Zugriffsverfahren mittels überlagerndem Empfangen sind so effizient, daß ihr Einsatz zumindest im lokalen Bereich auf für Zwecke, bei denen es *nicht* auf Senderanonymität ankommt, zweckmäßig erscheint [68, 61].

Der Schutz des Empfängers wird im DC-Netz durch **Verteilung** realisiert: indem jede Teilnehmerstation jede Nachricht erhält, bleibt der wirkliche Empfänger der Nachricht anonym.

Dies gilt jedoch nur für *passive Angreifer.* Geht man etwa von einer Sterntopologie aus und nimmt an, daß die Zentrale unter der Kontrolle des Angreifers steht und die Verteilung von Nachrichten beliebig manipulieren kann, so ist der Sender einer bestimmten Nachricht mit einigem Aufwand trotz überlagernden Sendens deanonymisierbar.

In [64b] wurden die entsprechenden Angriffe beschrieben und geeignete Gegenmaßnahmen untersucht. Es zeigte sich, daß die aus der Fehlertoleranz bekannten Methoden zur Realisierung einer **zuverlässigen Verteilung** (≈ byzantinische Übereinstimmung [34a, 41a]) aus Gründen der mangelnden Effizienz und der nur gegenüber einem zahlenmäßig stark beschränkten Angreifer informationstheoretischen Sicherheit zur Lösung des Problems untauglich sind. Statt dessen wurde die **fail-stop Verteilung** vorgeschlagen: sie garantiert, daß jeder aktive Angriff auf die Anonymität zu einem Abbruch des DC-Netzes (und ggf. zur Verfolgung des Angreifers) führt. Zu ihrer Realisierung wurden Methoden vorgeschlagen, die gegenüber dem „reinen" überlagernden Senden einen nur geringen Mehraufwand verursachen. Ihre Sicherheit wurde in einer informationstheoretischen Modellwelt bewiesen.

Ein DC-Netz (mit fail-stop Verteilung) stellt, wie jedes Datenschutz garantierende Netz, hinsichtlich seiner Zuverlässigkeit ein Seriensystem dar: erzeugt aufgrund eines Fehlers oder eines aktiven Angriffes eine Teilnehmerstation ihre lokale Summe nicht gemäß Protokoll, so kann keine Teilnehmerstation mehr erfolgreich senden.

Spezielle Verfahren zur Fehlertoleranz in DC-Netzen wurden in [35, 69] untersucht.

Zur Behandlung gezielter Störungen wurde in [14] vorgeschlagen, *nachweislich* nicht sensitive Nachrichten aufzudecken (d.h. alle während einer gewissen Zeit überlagerten Schlüssel und Nachrichten aller Teilnehmer werden offengelegt) und den Angreifer auszugrenzen. Der erforderliche Nachweis der Nichtsensitivität erfolgt in [14] jedoch nicht informationstheoretisch gesichert, so daß die informationstheoretische Senderanonymität verloren geht. In [64b] wurde daher ein Protokoll vorgeschlagen, das die Behandlung aktiver Angriffe ohne Anonymitätseinbuße erlaubt.

3.2 MIX-Netz

Die von D. Chaum in [6] angegebene Implementierung von MIXen mittels RSA und Voranstellen zufälliger Bits vor die Nachricht wurde gebrochen, vermutlich sicherere Implementierungen wurden angegeben [61]. Eine *beweisbar* sichere Implementierung des ursprünglichen MIX-Schemas ist mir nicht bekannt.

Eine solche vorausgesetzt, wurde jedoch in Erweiterung einer Idee aus [60] ein effizientes Verfahren zum Schalten von Kanälen entwickelt, das insbesondere auch dann einsetzbar ist, wenn die verfügbare Bandbreite der Teilnehmeranschlußleitungen nicht wesentlich größer ist als die der gewünschten zu schaltenden Kanäle. Alle anderen bekannten Grundverfahren zum Schutz der Verkehrsdaten sind unter dieser Beschränkung nicht einsetzbar.

Das gefundene Verfahren reduziert zugleich den Umfang der miteinander zu verleichenden Nachrichten erheblich.

4 Möglichkeiten zur unverkettbaren Verwendung nur einmal gültiger Beglaubigungen

Für ein auf zentralen Banken als Zeugen beasierendes Zahlungssystem stellt sich das Problem, daß ein Benutzer in einer Zahlung der Bank gegenüber seine Besitzrechte am zu transferierenden Geld *nachweisen* und dieses Recht nach vollzogenem Transfer *erlöschen* muß. Der jeweilige Zustand des Besitzrechtes muß im Streitfall einem Dritten nachgewiesen werden können: ist das Recht noch nicht erloschen, so muß dies der Benutzer, andernfalls die Bank nachweisen können.

Dies geschieht am einfachsten durch Verwendung eines **digitalen Signatursystems,** das als Ersatz der *eigenhändigen Unterschrift* dienen soll (vgl. Kap. 3.1.2.1 in [39]).

Durch ein solches kann sich jeder Benutzer ein Funktionenpaar (s, t) erzeugen: die **Signierfunktion** s dient zum Unterschreiben einer Nachricht und ist nur dem Erzeuger des Paares (s, t) bekannt, während das **Testprädikat** t dazu dient, zu testen, ob eine Nachricht mit s unterschrieben wurde. Das Testprädikat t kann jedem bekannt sein, insbesondere kann das Signatursystem stets so gewählt werden, daß der signierten Nachricht $s(N)$ sowohl die Nachricht N selbst als auch das Testprädikat t entnommen werden kann. (Im anonymen Fall wird sich ein Benutzer natürlich mehrere verschiedene Paare (s, t) erzeugen. Die verschiedenen Testfunktionen können als die verschiedenen *Pseudonyme* des Benutzers betrachtet werden.)

Ein Signatursystem muß natürlich **sicher** gegen Fälschungen sein, d.h. alleine mit Kenntnis von t darf niemand in der Lage sein, Nachrichten zu erzeugen, die als mit s unterschrieben erscheinen.

Die bekanntesten Signatursysteme sind das *RSA-System* [42] und das *GMR-System* [26, 29, 31]. Während die Sicherheit des ersten nicht bewiesen ist, wurde für das zweite gezeigt, daß das Fälschen einer Unterschrift selbst bei adaptiven aktiven Angriffen polynomial äquivalent der *Faktorisierung* ist [29, 31]. Beide Systeme sind hinsichtlich des Zeitaufwandes zur Erzeugung einer Unterschrift ähnlich zu bewerten.

In einer Zahlung legt nun der zahlende Benutzer der Bank die von ihr *selbst* in einer *früheren* Zahlung *unterschriebene* **Beglaubigung** über den Erhalt der zu transferierenden Besitzrechte vor, und die Bank notiert sich die vorgelegte Beglaubigung als „verbraucht".

Dadurch werden aber Zahlungen hinsichtlich der daran Beteiligten **verkettbar,** was aus Anonymitätsgründen nicht wünschenswert erscheint.[9] Dieses Problem wurde erstmals 1982 von D. Chaum [7] formuliert.[10]

In der folgenden kurzen Darstellung der bekannten Lösungsansätze soll **„Bankquittung"** stets für eine Nachricht stehen, die die Bank einem Zahlungsempfänger als Bestätigung über die erhaltene Zahlung sendet, und **„Banknote"** für eine Nachricht, die ein Zahlender der Bank gegenüber als Nachweis über den Besitz des zu transferierenden Geldes verwendet. In der oben genannten Möglichkeit waren Bankquittung und Banknote identisch.

4.1 Umtauschen von Beglaubigungen durch MIXe

Das *erste Verfahren* basiert auf der Idee, eine größere Menge von Benutzern gemeinsam Bankquittungen gegen Banknoten umtauschen zu lassen, ohne aber die Bank wissen zu lassen, welche Bankquittungen zu welchen Banknoten gehören.

D. Chaum schlug 1981 [6] vor, hierfür **umkodierende MIXe** zu verwenden.[11] Diese dienen den Benutzern dazu, ihre neuen, noch nicht von der Bank unterschriebenen Banknoten in einer *zufälligen* Reihenfolge (z.B. der durch die Sortierung der Banknoten ihrer Größe nach gegebenen) zu veröffentlichen. Nach der Veröffentlichung werden die neuen Banknoten von der Bank unterschrieben und die alten Bankquittungen ungültig. Die Zuordnung von alten Bankquittungen zu neuen Banknoten ist durch die Zufälligkeit der Veröffentlichungsreihenfolge verborgen, solange wenigstens einer der umkodierenden MIXe korrekt arbeitet (was z.B. dann, wenn alle Benutzer zugleich auch MIXe sind, immer der Fall sein wird). Das Verfahren basiert wesentlich auf der Verwendung eines asymmetrischen Kryptosystems.

Vorteil des Verfahrens ist, daß es mit *jedem*, also auch dem sehr sicheren GMR-Signatursystem realisiert werden kann, seine *Betrugssicherheit* also entsprechend hoch ist. Hinsichtlich der *Anonymität* ist jedoch nachteilig, daß

- ein Benutzer immer nur unter der Menge all derjenigen Benutzer verborgen ist, die gleichzeitig mit ihm ihre Banknoten „mixen" lassen,
- daß die Anonymität höchstens so sicher ist wie die des für die Kommunikation mit den MIXen verwendeten asymmetrischen Kryptosystems,
- und schließlich, daß die Anonymität auf der Vertrauenswürdigkeit der MIXe basiert.

Die genannten Nachteile sind zugleich auch die Nachteile eines jeden auf MIXen basierenden Datenschutz garantierenden Digitalnetzes.

Da es aber mit dem **überlagernden Senden** (DC-Netz, vgl. Kap. 3) auch ein Netz gibt, das die Anonymität informationstheoretisch sicher und ohne Rückgriff auf vertrauenswürdige Instanzen garantiert, wurde im Rahmen des Projektes die obige Idee auf das DC-Netz übertragen: Statt die MIXe zur Veröffentlichung zu verwenden, senden alle Benutzer direkt ihre neuen Banknoten unkoordiniert und damit in einer echt zufälligen Reihenfolge über das DC-Netz. Damit wären die letzten beiden der oben genannten Nachteile beseitigt, die Anonymität wenigstens in der Gruppe der gleichzeitig Bankquittungen gegen Banknoten umtauschenden Benutzer informationstheoretisch gesichert.

Die Schwierigkeit der Übertragung auf ein DC-Netz liegt jedoch darin, *Störungen* des Protokolls (z.B. Überlagern von Nachrichten mit Störungen, unerlaubtes Senden einer neuen Banknote) erkennen und ohne Gefährdung der informationstheoretischen Anonymität verfolgen zu können. In [67] wurde hierzu ein Störungen des Nachrichtenaustausches mit hoher Sicherheit erkennender *Code* sowie ein *Protokoll* entworfen, das das Gewünschte unter der Annahme eines vertrauenswürdigen Netzbetreibers leistet.

Durch Kombination mit den Verfahren aus [64b] zur Behandlung aktiver Angriffe kann auf einen vertrauenswürdigen Netzbetreiber verzichtet werden.

4.2 Blind geleistete Unterschriften bei Verwendung von RSA

Das *zweite Verfahren* basiert auf der Idee, die Bankquittungen vor ihrer Verwendung als Banknote in einer neuen Zahlung so **umzuformen**, daß sie zwar als von der Bank unterschriebene Banknoten akzeptiert werden, aber die Bank den Zusammenhang zwischen von ihr unterschriebenen Bankquittungen und ihr vorgelegten Banknoten nicht mehr erkennen kann.

D. Chaum schlug 1985 [55] vor, hierfür die speziellen Eigenschaften des RSA-Signatursystems zu verwenden: bei RSA wird das Testprädikat t durch die Inverse der Signierfunktion, s^{-1}, realisiert, die ohne Schaden öffentlich bekannt sein darf: $t(N,M) :\Leftrightarrow N = s^{-1}(M)$. Direkt aufeinanderfolgende Anwendungen von s und s^{-1} sind *vertauschbar* und beide Funktionen sind *multiplikative Homomorphismen* (in dem durch s bzw. t festgelegten Restklassenring).

Soll duch den Benutzer X der Bank später eine Banknote $s(N)$ vorgelegt werden (wobei s die Signierfunktion der Bank sei), so wählt sich X einen zufälligen Wert r, bildet $s^{-1}(r)$ und läßt sich bei passender Gelegenheit als Bankquittung die Nachricht $s^{-1}(r) \cdot N$ unterschreiben.

Aus $s(s^{-1}(r) \cdot N) = r \cdot s(N)$ kann X leicht die unterschriebene Banknote $s(N)$ gewinnen. Die Bank hat also die Unterschrift unter N *blind* geleistet.

Vorteil des Verfahrens ist, daß der Zusammenhang von $s^{-1}(r) \cdot N$ und N vor der Bank *informationstheoretisch* sicher verborgen ist. Nachteil ist jedoch, daß die Betrugssicherheit auf dem bisher nicht als sicher bewiesenen RSA-Signatursystem beruht und sich das Verfahren natürlich nicht ohne weiteres auf andere Signatursysteme übertragen läßt. ([10] enthält eine detailliertere Beschreibung des Verfahrens.)

4.3 Blind geleistete Unterschriften durch Anwendung universeller Übersetzungstechniken auf den Signaturalgorithmus

Das *dritte* und letzte Verfahren basiert auf der Anwendung **universeller Übersetzungstechniken**[12]: der Signaturalgorithmus läßt sich durch Kooperation des Benutzers und der Bank in einer Weise ausführen, daß der Benutzer ausschließlich seine unterschriebene Banknote erhält und ansonsten weder er noch die Bank zusätzliche Informationen über geheime Bankschlüssel bzw. die zu unterschreibende Banknote erhalten. Auch hier leistet also die Bank die Unterschrift *blind*.

Die Information eines der beiden Beteiligten kann sogar informationstheoretisch sicher vor dem anderen verborgen werden [53, 15]. Ist dies für die Banknote des Benutzers der Fall, so ist die Unverkettbarkeit ebenfalls informationstheoretisch gesichert.[13]

5 Verifikation von Wertetransferprotokollen

Die Verifikation von Wertetransferprotokollen (vgl. Einleitung und Kap. 1) hat das Ziel, folgende Eigenschaften nachzuweisen:

- **Korrektheit**, d.h. die Protokollspezifikation entspricht der Dienstspezifikation. Da der hierzu zu betrachtende

fehlerfreie Ablauf eines Wertetransferprotokolls üblicherweise sehr einfach ist, bereitet dieser Teil kaum Schwierigkeiten und wird im folgenden nicht weiter betrachtet. Sie kann bei Bedarf durch die Standardmethoden der Protokollverifikation nachgewiesen werden.

- **Betrugssicherheit** wie bereits definiert. Hierzu muß nachgewiesen werden, daß zur Protokollimplementierung ein **effektives Gerichtsprotokoll** existiert, d.h. daß im Streitfall durch Auswertung der erreichbaren Beweismittel ein Schuldiger gefunden und Schaden zu dessen Lasten reguliert werden kann.

  Insbesondere sollte der Beweis auch zeigen, daß die im Gerichtsprotokoll verwendeten Beweismittel *korrekt* sind und nicht etwa durch Schwachstellen im Protokoll oder in den verwendeten Kryptosystemen Beweismittel gefälscht und damit Schlußfolgerungen des Gerichtes *fehlerhaft* werden können.

- **Lebendigkeit.**
  Für *Zahlungssysteme* heißt dies, daß ein Benutzer spätestens nach einer beschränkten Zeitspanne über all seine Besitzrechte an Geld verfügen kann.

  Für *Warentransfersysteme* heißt dies, daß das Protokoll nach einer beschränkten Zeitspanne definitiv beendet ist und danach entweder der Austausch stattgefunden hat oder der Besteller wieder über seine dem Lieferanten gegebenen Sicherheiten (im Sinne des Kreditgewerbes) verfügen kann.

- **Anonymität.** Zu zeigen ist, daß jeder Protokollablauf möglichst unabhängig von allen anderen Abläufen erscheint, d.h. keine Verkettungen über mehrere Zahlungen, Warentransfers usw. möglich sind.

  Explizite Nachweise der Wahrung der Anonymität bei Ausführung eines gesamten Wertetransferprotokolls wurden bislang noch nicht erbracht. Die Anonymität der in Kapitel 1 spezifizierten Wertetransferprotokolle erscheint jedoch bei geeigneter Implementierung (vgl. Kap. 2, Kap. 3) unmittelbar einleuchtend.

Zum Nachweis dieser Eigenschaften wird üblicherweise angenommen, daß lediglich *algorithmische* Aspekte zu betrachten sind. Die für betrugssichere autonome Zahlungssysteme notwendige und nur technisch zu gewährleistende Unausforschbarkeit und Unmanipulierbarkeit von Geräten wird ggf. vorausgesetzt. Eher organisatorische Aspekte (z.B. daß man geheime Schlüssel vor Diebstahl oder unbeabsichtigter Bekanntgabe schützen muß) werden nicht betrachtet.

Am überzeugendsten wäre natürlich, die algorithmischen Möglichkeiten des Angreifers überhaupt nicht einzuschränken, d.h. ihm ohne jede Zeit- oder Speicherbeschränkung jedes beliebige Verhalten zu erlauben und trotzdem die gewünschten Eigenschaften zu garantieren. Dies ist das von C. Shannon gefundene **informationstheoretische Modell** [45]. Da es jedoch keine informationstheoretisch sicheren Signatur- oder asymmetrischen Kryptosysteme geben kann [17], wohl aber praktisch sichere, ist dieser Ansatz zur Verifikation von Kryptoprotokollen alleine nicht tauglich.[14]

Daher müssen die algorithmischen Fähigkeiten des Angreifers beschränkt werden. Ziel ist es, die Beschränkung so zu wählen, daß das modellierte **Wissen** des Angreifers mit seinem in der Realität praktisch erreichbaren möglichst gut übereinstimmt. Die Beschränkung der Angreiferfähigkeiten kann auf zweierlei Art geschehen (vgl. ausführlicher [70]):

5.1 Algebraische Modellierung

In der erstmals von D. Dolev und A. Yao vorgeschlagenen **algebraischen Modellierung** [18] werden die prinzipiellen Berechnungsfähigkeiten des Angreifers beschränkt, ohne jedoch den im Modell möglichen Berechnungen komplexitätstheoretische Schranken zu setzen.

Konkret heißt dies, daß als Nachrichtenraum eine möglichst einfache Termalgebra mit Gleichungen [19] genommen wird, wobei die Menge der Grundnachrichten (Konstanten) und evtl. auch die der anwendbaren Operationen auf die am Protokoll beteiligten Instanzen unterschiedlich verteilt wird. Damit soll der unterschiedliche Wissensstand der verschiedenen Instanzen modelliert werden.

Üblich ist etwa, ein asymmetrisches Kryptosystem nur durch Gleichungen der Art

$$d(e(N)) = N$$

zu beschreiben und zu fordern, daß die zur allgemein bekannten Verschlüsselungsoperation e einer Instanz gehörende Entschlüsselungsoperation d dem Angreifer nicht bekannt ist. Werden keine weiteren Gleichungen angegeben, so ist das asymmetrische Kryptosystem in dieser Modellwelt also im idealen Sinne sicher. Ohne Kenntnis der Klartextnachricht N fehlen dem Angreifer sozusagen die zum Brechen notwendigen Operationen.

Da sich ein Angreifer natürlich nicht den Modellbeschränkungen unterwerfen wird, können als sicher bewiesene Protokolle durch Ausnutzen weiterer unberücksichtigter (und eventuell auch gar nicht modellierbarer oder bis heute unbekannter) mathematischer Eigenschaften konkreter Implementierungen unsicher werden [70]. Umgekehrt sind jedoch im Modell durch Angabe eines realisierbaren Angriffes als unsicher bewiesene Protokolle auch in der Realität unsicher.

In einem algebraischen Modell wurden bislang allgemeine Aussagen nur für sehr einfache asymmetrische Kryptosysteme (insbesondere RSA) verwendende sogenannte Ping-Pong-Protokolle bewiesen [18, 20]. In [59, 16] wurden Vertraulichkeitsaussagen über spezielle Protokolle, z.B. die Anonymität eines Wahlprotokolls, nachgewiesen, in [63, 47, 66] die Betrugssicherheit eines einfachen Zahlungssystems, in [13] die Betrugssicherheit eines auf RSA basierenden allgemeinen Beglaubigungsmechanismus.

Auch die bekannten Arbeiten über die automatisierte Sicherheitsanalyse von Kryptoprotokollen bedienten sich implizit einer algebraischen Modellierung, sei es in allgemeinen Protokollverifikationssystemen, z.B. „Ina Jo" [33], sei es in speziell für Kryptoprotokolle entworfenen Systemen, z.B. des Prolog-Programms „The Interrogator" [36, 37]. Aus diesem Grunde sind die entsprechenden Hilfsmittel stets nur für *Unsicherheitsbeweise* von Protokollen geeignet.

Im Berichtszeitraum wurde die beschriebene algebraische Modellierungstechnik in Fortführung der vor Projektbeginn entstandenen Arbeit [63] dazu verwendet, ein einfaches Zahlungssystem zu beschreiben. Hierzu wurde das in [59, 63] angegebene Modell verfeinert und um zeitliche Aspekte erweitert [66].

Um das Zeitverhalten eines Protokolls zu beschreiben, wurde eine in der Spezifikation mit endlichen Automaten übliche Methode verwendet: jeder protokollausführenden Instanz wird eine lokale Uhr zugeordnet, mit der die Instanz über Zeitabfrage, -start und -überwachungsnachrichten kommunizieren kann. Um auch für Nachrichten, deren Ausbleiben die Spezifikation verletzen würde, die Betrugssicherheit zu garantieren, werden dem Empfangen

solcher zeitkritischen Nachrichten zwei lokale Zeitschranken gesetzt: wird die eine erreicht, ohne daß die gewünschte Nachricht erhalten wurde, so wendet sich die betroffene Instanz vorsorglich an das Gericht, die den erhofften Sender zum Senden der Nachricht auffordert. Da das Gericht nun in die Kommunikation aktiv eingeschaltet ist, kann es das Erreichen der zweiten Zeitschranke überprüfen und in diesem Falle den entstandenen Schaden zu Lasten einer vom Protokoll abgewichenen Instanz regulieren.

Zur Festlegung geeigneter Zeitschranken und zum Nachweis diverser Lebendigkeitseigenschaften werden die möglichen Abläufe eines Protokolls zu einer regulären Sprache abstrahiert und die maximale Verzögerungszeit zwischen Nachrichten anhand regulärer (und im korrekten Fall zugleich endlicher) Teilausdrücke bestimmt.

5.2 Kryptographische Modellierung

Im auf Arbeiten von A. Yao basierenden **kryptographischen Modell** kann im Gegensatz zu den algebraischen Modellen der Angreifer jede beliebige indeterministische Berechnung anstellen, solange sie nur in einem bestimmten wählbaren Sicherheitsparameter polynomial viel Zeit benötigt [4, 58, 28, 34, 51].

Damit sind, in Umkehrung zur Situation in algebraischen Modellen, in diesem Modell bewiesene Aussagen darüber, was ein Angreifer ***nicht*** kann, auch in der Realität korrekt, während manches, was dem Angreifer als möglich unterstellt wird, in der Realität an zu hohem Zeitbedarf scheitern kann.[15]

Die Abgrenzung zwischen dem, was der Angreifer kann und dem, was er nicht kann, beruht jedoch auf der ***unbewiesenen*** Behauptung $P \neq NP$ und, mangels geeigneter gleichmäßig harter Probleme, zusätzlich auf ebenfalls ***unbewiesenen*** Annahmen über den Aufwand zur Lösung zahlentheoretischer Probleme, z.B. der Faktorisierung natürlicher Zahlen. Aussagen in diesem Modell gelten damit für all die Angreifer, die das zugrunde gelegte schwere Problem nicht effizient lösen können, was, da z.B. die Faktorisierung seit sehr langer Zeit untersucht wird, auf alle normalen Angreifer zutreffend wird.[16]

In diesem Modell wurden außerhalb des Projektes bislang zahlreiche Kryptosysteme bewiesen. Insbesondere zu nennen ist das relativ effiziente und selbst gegen adaptive aktive Angriffe sichere GMR-Signatursystem [29, 31]. Ein gegen adaptive aktive Angriffe mit gewähltem Schlüsseltext sicheres asymmetrisches Kryptosystem wurde bislang noch nicht gefunden, wohl aber solche, die gegen schwächere Angriffe beweisbar sicher sind [5, 46].

Ebenfalls bewiesen wurden Kryptoprotokolle z.B. zur Identifikation [21, 22]. Dieses Identifikationsschema ist insbesondere ein Beispiel für ein Protokoll, das es einem Benutzer A (dem *Beweiser*) erlaubt, einem anderen Benutzer B (dem *Prüfer*) die Erfüllbarkeit oder Gültigkeit eines bestimmten Prädikates nachzuweisen, ohne B zusätzliche verwertbare Information zukommen zu lassen (*Zero-Knowledge-Proof* [30], *Minimum-Knowledge-Proof* [23]). Dies heißt, daß aus der Sicht von B das gesamte Protokoll durch ein *Orakel* ersetzt werden könnte, welches B nur das Ergebnis des von A vermittelten Beweises mitteilt, ohne daß hierdurch B irgendwelche Möglichkeiten zur Berechnung wesentlicher Informationen genommen würden.

In der Folge dieses und ähnlicher Protokollbeweise wurden aufbauend auf einer Idee von A. Yao [50, 52] von S. Goldwasser, S. Micali, A. Wigderson u.a. allgemeine **Übersetzungstechniken** entwickelt:

Angenommen, f sei eine effizient berechenbare Funktion, für die eine Reihe von Teilnehmern $T_1, ..., T_n$ jeweils einen Teil der Eingabe $e_1, ..., e_n$ beisteuern. Die Teilnehmer wollen zwar alle das Ergebnis erfahren, aber keiner möchte einem anderen Teilnehmer irgendwelche weitere Information über seine Eingabe e_i zukommen lassen. Eine Lösung für dieses Problem wäre, die Berechnung von f einem absolut vertrauenswürdigen Dritten zu überlassen, der alle Eingaben erhält, $f(e_1, ..., e_n)$ berechnet und das Ergebnis an alle Teilnehmer verteilt. Dasselbe Ergebnis kann aber auch durch Anwenden der Übersetzungstechniken aus [53, 15, 24, 57, 25, 27] auch bei Verzicht auf einen aktiven Dritten erreicht werden.

Hierzu wird meist f als boolesches Schaltnetz dargestellt, f gatterweise verschlüsselt und dann von allen Teilnehmern gemeinsam ausgewertet. Dies kann in einer Form geschehen, die das Ergebnis gezielt nur manchen der Teilnehmer bekannt macht und die zugleich die *Fairness* der Berechnung garantiert, d.h. jeder Teilnehmer T_i muß zu jedem Zeitpunkt ungefähr gleichviel Rechenaufwand investieren, um das Ergebnis der Berechnung zu erhalten.

Da nur noch ein Protokollschritt zu betrachten ist, vereinfacht sich durch die Übersetzung von *Wertetransferprotokollen* der Nachweis der Betrugssicherheit (d.h. Korrektheit von Beweismitteln) vermutlich erheblich, so daß hier unmittelbare Auswirkungen der genannten Ergebnisse zu erwarten sind. Können die Gültigkeitsdauern von Beweismitteln geeignet festgelegt werden, so erhält man zudem durch Ausnutzen der Fairness-Eigenschaft in obigem Sinne lebendige Wertetransferprotokolle.

Allerdings ist der zusätzliche Berechnungs- und Kommunikationsaufwand der Übersetzungstechniken so groß, daß diese Möglichkeit zunächst nur von theoretischem Interesse ist. Für die im Projekt eine zentrale Rolle spielenden praktischen Belange erscheint eher ein direkter Beweis der ursprünglichen, mehrschrittigen Protokolle wünschenswert.

Hierfür sprechen auch einige praktische Probleme: In einem *Zahlungssystem* vergrößert sich ständig die Menge der bereits „verbrauchten" Rechte. Jedes neue zu transferierende Recht muß im zu übersetzenden Protokoll mit allen oder doch vielen alten verglichen werden, so daß dieses Protokoll ständig größer wird und zudem von der Bank vor jedem Transfer dem Zahlenden und dem Empfänger mitgeteilt werden muß. Auf die Notwendigkeit, aber fast schon Unmöglichkeit einer *Prüffunktion* für *Warentransferprotokolle* wurde bereits in Kapitel 1 hingewiesen.

In beiden Fällen erscheint eine Aufspaltung des Protokolls in mehrere Schritte sehr sinnvoll. Zur Verifikation mehrschrittiger Protokolle wurde in [57] gezeigt, daß bei Ausführung mehrerer Protokollschritte, von denen jeder in einer „Minimum-Knowledge"-Art erfolgt, sich diese Eigenschaft auf das gesamte Protokoll überträgt.

Innerhalb des Projektes wurde in [70] untersucht, inwieweit sich die recht einfache Folgerungsweise algebraischer Beweise über Signatursysteme in das kryptographische Modell übertragen läßt.

6 Realisierung von Wertetransferprotokollen

Über die für alle Protokolle in verteilten Systemen notwendigen **technischen** Voraussetzungen hinaus benötigt eine **Implementierung** eines Wertetransferprotokolls effiziente

Implementierungen eines *Datenschutz garantierenden Digitalnetzes* und möglichst sicherer *kryptographischer Systeme.*

Implementierungen Datenschutz garantierender Digitalnetze sind mir nicht bekannt (allerdings wurden im Projekt für das DC-Netz und das MIX-Netz einige Verfahren entwickelt, die deren Effizienz erheblich steigern, vgl. Kap. 3).

Soft- und Hardwareimplementierungen von RSA und DES sind im Prinzip verfügbar[17], wobei im Rahmen des Projektes die meines Wissens bisher effizienteste Softwareimplementierung von DES auf einem Mikrorechner entstand (43 kbit/s auf einem Apple Macintosh II, d.h. MC68020 mit 16 MHz, [65]). Sie bietet zahlreiche Modifikationsmöglichkeiten hinsichtlich Schlüssellänge (optionaler Verzicht auf die Schlüsselexpansion im Standard-DES) und Permutationsboxen (Umwandlung der Spezifikation der Permutationen in kurze und effiziente MC68000 Programme). Implementierungen *beweisbar* sicherer Systeme sind mir nicht bekannt, stellen jedoch keine prinzipiell neuen Probleme dar.

Mündlichen Informationen entsprechend wurde der in Kapitel 4.2 genannte Umformungsmechanismus am CWI, Amsterdam, implementiert und zur Realisierung eines anonymen Zahlungssystems verwendet. Entsprechende Arbeiten sind an der Universität von Trondheim, Norwegen, geplant [62].

Die in Kapitel 1 spezifizierten sicheren und anonymen Wertetransfersysteme sind noch nicht implementiert.

Die **juristischen** Voraussetzungen für den **Einsatz** von Wertetransferprotokollen wurden in [39] diskutiert.

7 Zusammenfassung

Das *Fernziel* dieses Projektes ist es, Wertetransferprotokolle zu entwerfen und zu realisieren, die zugleich *beweisbar betrugssicher, beweisbar anonym* und hinsichtlich ihres Aufwandes mit den heutigen i.allg. unsicheren und nicht anonymen Protokollen vergleichbar sind.

Diesem Fernziel wurde in den ersten zwei Jahren, über die hier berichtet wird, in vielen Punkten näher gerückt; ebenso häufig zeigten sich aber auch neue Fragen und Probleme.

Abschließend behandelt wurde die Frage nach der **Systematisierung** und damit der Eingrenzung der zu untersuchenden Protokolle.

Hierzu wurde die Klasse der betrugssicheren und anonymen Wertetransferprotokolle durch am juristischen Begriff des Beweismittels orientierte *Dienstspezifikationen* beschrieben. Für diese wurden entsprechende *Protokollspezifikationen* angegeben, die bei Verwendung beweisbar sicherer Hilfsmittel vermutlich zu ebenso sicheren und anonymen Wertetransferprotokollen führen.

Das Problem der von der Betrugssicherheit nicht mit erfaßbaren **Tolerierung lokaler Fehler** in Wertetransferprotokollen wurde selbst für den Fall der autonomen und daher auf sicheren Geräten basierenden off-line Zahlungssysteme zufriedenstellend gelöst.

Die Untersuchung der **Datenschutz garantierenden Kommunikationsnetze,** die eine Grundvoraussetzung für anonyme Protokolle darstellen, führte sowohl zu einigen Erfolgen wie auch zu neuen offenen Problemen.

So wurde die Leistungsfähigkeit des DC-Netzes durch Angabe des *überlagernden Empfangens,* die des MIX-Netzes durch Angabe eines auch für Kanäle bei schmalbandigen Teilnehmeranschlußleitungen geeigneten MIX-Schemas wesentlich erhöht. Durch Angabe der *fail-stop Verteilung* wurde das DC-Netz zu einem Schema erweitert, das Anonymität auch gegenüber aktiven Angreifern beweisbar sicherstellt. Ebenso wurde das Problem der Behandlung gewollter Störungen unter Wahrung der informationstheoretischen Anonymität gelöst.

Andererseits wurde gezeigt, daß das ursprüngliche (d.h. auf RSA mit zufälligen vorangestellten Bitfolgen basierende) MIX-Schema gegen aktive Angriffe unsicher ist. Für dieses Problem wurden erste Lösungsansätze entwickelt.

Dasselbe gilt für die Untersuchung der Möglichkeiten für **unverkettbare, nur einmal gültige Beglaubigungen.**

Hier wurde mit dem in 4.1 genannten auf überlagerndem Senden basierenden Umtauschmechanismus ein interessanter Ansatz entwickelt.

Ebenso interessant ist der in 4.3 beschriebene Ansatz, der auf der Anwendung universeller Übersetzungstechniken auf den GMR-Signaturalgorithmus beruht. Sein Nachteil ist der sehr hohe Aufwand zur „blinden" Leistung einer Unterschrift, so daß hier nach direkteren Umsetzungen des GMR-Algorithmus zu suchen sein wird.

Hinsichtlich der **Verifikation** konzentrierten sich die Arbeiten einerseits auf den Nachweis der Lebendigkeit angesichts von Angriffen, andererseits auf die Untersuchung der Möglichkeiten, im (mittlerweile allgemein als das der Realität am nächsten kommende akzeptierten) kryptographischen Modell *effiziente* Protokolle zu verifizieren.

Unmittelbar möglich erscheint die Anwendung *universeller Übersetzungstechniken,* was aber zu unpraktikablen und ineffizienten Lösungen führt. Umgekehrt wäre eine Implementierung der oben erwähnten Protokollspezifikationen bei Verwendung geeigneter Hilfsmittel sowohl effizient als auch intuitiv betrugssicher und anonym. Dies zu beweisen ist sicher lohnend.

Die algebraische Modellierung wurde in ihrer reinen Form verworfen, das Ziel, auf ihr aufbauend ein automatisiertes Verifikationshilfsmittel zu entwickeln, aufgegeben (gleichwohl es als Validierungshilfsmittel durchaus seine Berechtigung hätte). Es wurden jedoch Überlegungen angestellt, innerhalb der algebraischen Modellwelt die Lebendigkeit (insbesondere angesichts von Angriffen) von Wertetransferprotokollen zu beweisen. Weitere Untersuchungen beschäftigten sich mit der Frage, unter welchen Bedingungen in der algebraischen Modellwelt bewiesene Aussagen auf die kryptographische Modellwelt übertragen werden können.

Für ihre Kritik und Diskussionsbereitschaft danke ich Birgit Baum, Birgit Pfitzmann, Dr. Klaus Echtle, Prof. Dr.-Ing. Winfried Görke und Andreas Pfitzmann recht herzlich. Der Deutschen Forschungsgemeinschaft (DFG) danke ich für ihre freundliche Unterstützung.

Stichwörter: Anonymität, unverkettbare nur einmal gültige Beglaubigungen, Betrugssicherheit, elektronische Brieftasche, technischer Datenschutz, DES, Fehlertoleranz, GMR, Datenschutz garantierende Kommunikationsnetze, MIX-Netz, algebraische Modellbildung, kryptographische Modellbildung, Rechtssicherheit, RSA, überlagerndes Senden und Empfangen, Signatursystem, blind geleistete Unterschriften, Verifikation, Verlusttoleranz, Warentransfer, Wertetransfer, Zahlungssystem.

Literatur

In Zeitschriften oder Tagungsbänden veröffentlichte Arbeiten

[1] C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine 22/9 (1984) 15–21

[2] T. Anderson, P. A. Lee: Fault Tolerance – Principles and Practice; Prentice Hall, Englewood Cliffs, 1981

[3] AT&T: Einchip-Prozessor zur Verschlüsselung digitaler Signale; Design & Elektronik, Markt & Technik, Ausgabe 21 vom 14.10.1986, 8–11

[4] M. Blum, S. Micali: How To Generate Cryptographically Strong Sequences of Pseudo Random Bits; 23rd FOCS 1982, 112–117

[5] M. Blum, S. Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Crypto '84, LNCS 196, Springer-Verlag, Heidelberg 1985, 289–299

[6] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84–88

[7] D. Chaum: Blind Signatures for untraceable payments; Crypto '82, Plenum Press, New York 1983, 199–203

[8] D. Chaum: A New Paradigm for Individuals in the Information Age; IEEE Symposium on Security and Privacy, Oakland 1984, 99–103

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

[10] D. Chaum: Sicherheit ohne Identifizierung. Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262–277; Datenschutz und Datensicherung DuD 1 (1988) 26–41

[11] D. Chaum: Demonstrating that a Public Predicate can be Satisfied Without Revealing Any Information About How; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 195–199

[12] D. Chaum: Blinding for Unanticipated Signatures; Eurocrypt '87, LNCS 304, Springer-Verlag, Heidelberg 1988, 227–233

[13] D. Chaum, J.-H. Evertse: A secure and privacy-protecting protocol for transmitting personal information between organizations; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 118–167

[14] D. Chaum: The Dining Cryptographers Problem. Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65–75

[15] D. Chaum, I. B. Damgard, J. van de Graaf: Multiparty Computations ensuring privacy of each party's input and correctness of the result; Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, 87–119

[16] R. DeMillo, M. Merritt: Protocols for Data Security; Computer, IEEE, 16/2 (1983) 39–51

[17] W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory, IT-22/6 (1976) 644–654

[18] D. Dolev, A. C. Yao: On the Security of Public Key Protocols; IEEE Trans. on Information Theory, IT-29/2 (1983) 198–208

[19] H. Ehring, B. Mahr: Fundamentals of Algebraic Specifications 1; EATCS Monographs on Theoretical Computer Science, Band 6, Springer-Verlag, Berlin 1985

[20] S. Even, O. Goldreich, A. Shamir: On the Security of Ping-Pong Protocols When Implemented Using the RSA (extended abstract); Crypto '85, LNCS 218, Springer-Verlag, Heidelberg 1986, 58–72

[21] U. Feige, A. Fiat, A. Shamir: Zero Knowledge Proofs of Identity; 19th STOC 1987, 210–217

[22] A. Fiat, A. Shamir: How to prove yourself: Practical solutions to identification and signature problems; Crypto '86, LNCS 263, Springer-Verlag, Heidelberg 1987, 186–194

[23] Z. Galil, S. Haber, M. Yung: A private interactive test of a Boolean predicate and minimum-knowledge public-key cryptosystems (extended abstract); 26th FOCS 1985, 360–371

[24] Z. Galil, S. Haber, M. Yung: Cryptographic Computation: Secure Fault-Tolerant Protocols and the Public-Key Model; Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, 135–155

[25] O. Goldreich, S. Micali, A. Wigderson: How to play any mental game – or – a completeness theorem for protocols with honest majority; 19th STOC 1987, 218–229

[26] O. Goldreich: Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme; Crypto '86; LNCS 263, Springer-Verlag, Berlin 1987, 104–110

[27] O. Goldreich, R. Vainish: How to Solve any Protocol Problem – An Efficiency Improvement (extended abstract); Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, 73–86

[28] S. Goldwasser, S. Micali, P. Tong: Why and How to establish a Private Code On a Public Network; 23rd FOCS 1982, 134–144

[29] S. Goldwasser, S. Micali, R. L. Rivest: A "Paradoxical" Solution to the Signature Problem; 25th FOCS 1984, 441–448

[30] S. Goldwasser, S. Micali, C. Rackoff: The Knowledge Complexity of Interactive Proof-Systems; 17th STOC 1985, 291–304

[31] S. Goldwasser, S. Micali, R. L. Rivest: A digital signature scheme secure against adaptive chosen-message attacks; SIAM J. Comput. 17/2 (1988) 281–308

[32] S. Herda: Authenticity, Anonymity and Security in OSIS. An Open System for Information Services; 1. GI Fachtagung Datenschutz und Datensicherung, IFB 113, Springer-Verlag, Berlin 1985, 35–50

[33] R. A. Kemmerer: Analyzing encryption protocols using formal verification techniques; Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, 289–305

[34] E. Kranakis: Primality and Cryptography; Wiley-Teubner Series in Computer Science; B. G. Teubner Stuttgart, John Wiley & Sons, Chichester, 1986

[34a] L. Lamport, R. Shostak, M. Pease: The Byzantine Generals Problem; ACM TOPLAS 4/3 (1982) 382–401

[35] A. Mann, A. Pfitzmann: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen; GI-NTG Fachtagung „Kommunikation in verteilten Systemen" 1987, IFB 130, Springer-Verlag, Heidelberg 1987, 16–30; Überarbeitung in: Datenschutz und Datensicherung DuD 8 (1987) 393–405

[36] J. K. Millen: The Interrogator: A Tool for Cryptographic Protocol Security; IEEE Symposium on Security and Privacy, Oakland 1984, 134–141

[37] J. K. Millen, S. C. Clark, S. B. Freedman: The Interrogator: Protocol Security Analysis; IEEE Trans. on Software Engineering SE-13/2 (1987) 274–288

[38] A. Pfitzmann, M. Waidner: Networks without user observability – design options; Eurocrypt '85, LNCS 219, Springer-Verlag, Heidelberg 1986, 245–253; Überarbeitung in Computers & Security 6/2 (1987) 158–166

[39] B. Pfitzmann, M. Waidner, A. Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht CR Okt./Nov./Dez. (1987) 712–717, 796–803, 898–904

[40] A. Pfitzmann, B. Pfitzmann, M. Waidner: Weitere Aspekte fernmeldetechnischer Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 11/1 (1988) 5–7

[41] A. Pfitzmann, B. Pfitzmann, M. Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik-Spektrum 11/3 (1988) 118–142; eine frühere Fassung erschien in: Datenschutz und Datensicherung DuD 3 (1986) 178–191

[41a] R. Reischuk: Konsistenz und Fehlertoleranz in Verteilten Systemen – Das Problem der Byzantinischen Generäle; 17. GI Jahrestagung, IFB 156, Springer-Verlag, Berlin 1987, 65–81

[42] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120–126

[43] H. Sedlak: The RSA Cryptography Processor; Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin 1988, 96–105

[44] H. Sedlak, U. Golze: Ein Public-Key-Code Kryptographie-Prozessor; Informationstechnik it 28/3 (1986) 157–161

[45] C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656–715

[46] U. V. Vazirani, V. V. Vazirani: Efficient and Secure Pseudo-Random Number Generation (extended abstract); Crypto '84, LNCS 196, Springer-Verlag, Heidelberg 1985, 193–202

[47] M. Waidner, A. Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung, IFB 113, Springer-Verlag, Heidelberg 1985, 128–141; Überarbeitung in: Datenschutz und Datensicherung DuD 1 (1986) 16–22

[48] M. Waidner, B. Pfitzmann: Verlusttolerante elektronische Brieftaschen; "3rd International Conference on Fault-Tolerant Computing-Systems", IFB 147, Springer-Verlag, Heidelberg 1987, 36–50; Überarbeitung in: DuD 10 (1987) 487–497

[49] M. Waidner, B. Pfitzmann, A. Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD 6 (1987) 293–299

[50] A. C. Yao: Protocols for Secure Computations; 23rd FOCS 1982, 160–164

[51] A. C. Yao: Theory and Applications of Trapdoor Functions; 23rd FOCS 1982, 80–91

[52] A. C. Yao: How to Generate and Exchange Secrets; 27th FOCS 1986, 162–167

Interne Berichte und Vorveröffentlichungen

[53] G. Brassard, D. Chaum, C. Crépeau: Minimum Disclosure Proofs of Knowledge; July 1987

[54] H. Bürk, A. Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, 4th International Conference on Computer Security, Monte Carlo 1986, A. Grissonnanche (ed.); erscheint bei North-Holland, Amsterdam 1988; eine erweiterte Version erschien als: Interner Bericht 2/87 der Fakultät für Informatik, Universität Karlsruhe 1988

[55] D. Chaum: Privacy Protected Payments. Unconditional Payer and/or Payee Anonymity; Draft May 1985

[56] D. Chaum: A Convenient, Economical, Auditable, Secure, and Yet Untraceable Payment System; SECURICOM 87, Paris 1987

[57] Z. Galil, S. Haber, M. Yung: Minimum-Knowledge Interactive Proofs for Decision Problems; Draft April 1988

[58] S. Goldwasser, S. Micali: A Bit by Bit Secure Public-Key Cryptosystem; Electronics Research Laboratory, College of Engineering, University of California, Berkeley, CA 94720, Memorandum Nr. UCB/ERL M81/88, 4 December 1981

[59] M. Merritt: Cryptographic Protocols; Ph. D. Dissertation, School of Information and Computer Science, Georgia Institute of Technology, February 1983

[60] A. Pfitzmann: How to implement ISDNs without user observability – Some remarks; Interner Bericht 14/85 der Fakultät für Informatik, Universität Karlsruhe 1986

[61] A. Pfitzmann: Diensteintegrierende Kommunikationsnetze mit Teilnehmer-überprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, 1988, Dissertation (eingereicht)

[62] N. Stol: Privacy protected payments – A structure for an implementation and some capacity investigations; Securicom '88, Paris, March 15–17, 1988

[63] M. Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmaßnahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe 1985, Interner Bericht 19/85 der Fakultät für Informatik

[64] M. Waidner, B. Pfitzmann: Anonyme und verlusttolerante elektronische Brieftaschen; Interner Bericht 1/87 der Fakultät für Informatik, Universität Karlsruhe 1988

[64a] M. Waidner: Betrugssicherheit durch kryptographische Protokolle beim Wertetransfer über Kommunikationsnetze – Arbeitsbericht über das DFG-Projekt „Betrugssicherheit", September 1986 bis April 1988; Interner Bericht 7/88 der Fakultät für Informatik, Universität Karlsruhe 1988

[64b] M. Waidner: Unconditional Sender and Recipient Untraceability in the Presence of Active Attacks; Universität Karlsruhe, Fakultät für Informatik, 1988

Studien- und Diplomarbeiten

[65] R. Aßmann: Effiziente MC 68000 Assembler-Implementierung von verallgemeinertem DES; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1988

[66] H. Bürk: Modellierung und Verifikation der Sicherheit und Lebendigkeit von Kryptoprotokollen; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1987

[67] A. Burandt: Informationstheoretisch unverkettbare Beglaubigung von Pseudonymen mit beliebigen Signatursystemen; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1988

[68] E. Marchel: Leistungsbewertung von überlagerndem Empfangen bei Mehrfachzugriffsverfahren mittels Kollisionsauflösung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1988

[69] A. Niedermaier: Bewertung von Zuverlässigkeit und Senderanonymität einer fehlertoleranten Kommunikationsstruktur; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1987

[70] B. Pfitzmann: Vergleich der algebraischen und kryptographischen Modellierung von Kryptoprotokollen; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1988

Anmerkungen

1 DFG Projekt Go 347/6-1 „Betrugssicherheit"

2 Das Folgende ist ausführlicher in der Arbeit *„Rechtssicherheit trotz Anonymität in offenen digitalen Systemen"* [39] beschrieben.

3 Das Folgende ist ebenfalls ausführlicher in der Arbeit *„Rechtssicherheit trotz Anonymität in offenen digitalen Systemen"* [39] beschrieben.

4 Im Gegensatz zu allen anderen Zahlungssystemen können hier alle Benutzer *zusammen* ihren Besitz an Geld beliebig vermehren. Da jedoch niemand (auch keine Bank) für das vermehrte Geld garantieren muß, ist die Bedingung B5 auch für diesen Fall erfüllt.

5 Eine *unbestellte* Lieferung darf natürlich zu keiner Zahlungsverpflichtung für den Empfänger führen. Überlegungen zu einer verpflichtenden Rückgabe bei Nichtbezahlung erübrigen sich bei digitalen, also beliebig kopierbaren Waren.

6 Die hier anzuwendenden **universellen Übersetzungstechniken** werden ausführlicher in Kap. 5.2 erläutert.

7 Für eine sehr ausführliche und aus meiner Sicht abschließende Diskussion der hier anzuwendenden **Verlusttoleranzmaßnahmen** sei auf die Arbeit *„Anonyme und verlusttolerante elektronische Brieftaschen"* [64] verwiesen. Teile von [64] sind auch in [48] zu finden.

8 Die bekannten Konzepte für Datenschutz garantierende Kommunikationssysteme und ihre Realisierbarkeit werden in der Arbeit *„Datenschutz garantierende offene Kommunikationsnetze"* [41] ausführlich geschildert.

9 Auch ohne Vermeidung dieser Verkettbarkeit von Zahlungen lassen sich jedoch die Auswirkungen auf die Anonymität sehr reduzieren. Dies wurde erstmals in [54] bemerkt. Vgl. hierzu [39], Kap. 5.3.

10 Ebenfalls D. Chaum formulierte 1984 in [8] ein verwandtes Problem, das der *unverkettbaren Beglaubigungen* (Credentials). Dieses Problem erscheint einerseits allgemeiner als das obige, ist aber andererseits etwas einfacher, da eine solche Beglaubigung beliebig oft und nicht nur einmal gültig sein darf. Lösungsvorschläge für dieses Problem sind kurz in [39] erwähnt. Für die bekannten Lösungsmöglichkeiten gilt im wesentlichen das im folgenden für „Banknoten" Gesagte, d.h. es gibt drei Ansätze, die genauer z.B. in [67, 6] bzw. in [10, 12, 13] bzw. in [53, 11] beschrieben werden. Die ersten beiden Ansätze sind für beide Beglaubigungsprobleme ähnlich, während der dritte für die allgemeineren Beglaubigungen wesentlich einfacher ist als für nur einmal gültige Beglaubigungen, da im ersten Fall die Verwendung von Signatursystemen nicht zwingend ist.

11 Da diese zugleich auch ein Hilfsmittel zur Realisierung eines Datenschutz garantierenden Digitalnetzes bilden, sei zur ausführlichen Beschreibung des MIX-Mechanismus auf [41], Abschnitt 2.2.1, verwiesen. In [6] wird die Anwendung auf Zahlungssysteme nicht explizit genannt, wohl aber die auf die Umrechnung beliebiger Nachweise.

12 Da die anzuwendenden Übersetzungstechniken zugleich auch von großer Bedeutung für die Verifikation von Kryptoprotokollen sind, soll auf sie erst in Kap. 5.2 näher eingegangen werden. Die Idee der Anwendung auf das Beglaubigungsproblem wurde auch von Ivan Damgard auf der Tagung Crypto '88 konkretisiert. Seine Arbeit wird voraussichtlich erscheinen in: Crypto '88, LNCS, Springer-Verlag, Heidelberg 1989.

13 Statt dessen die Eingabe der Bank informationstheoretisch sicher vor dem Benutzer zu verbergen, ist sinnlos. Die einzig zu schützende Eingabe, der Signierschlüssel, ist bereits durch die Bekanntgabe des zugehörigen Testschlüssels im informationstheoretischen Sinne „verraten".

14 Anzumerken ist jedoch, daß einzelne Teilaussagen über Kryptoprotokolle sehr wohl informationstheoretischer Art sein können. So sind etwa die Anonymität des überlagernden Sendens (vgl. Kap. 3.1) und die Unverkettbarkeit des auf RSA basierenden allgemeinen Beglaubigungsmechanismus (vgl. Kap. 4.2) als informationstheoretisch sicher bewiesen.

15 Ein Kryptosystem wäre in der Realität z.B. auch dann noch sicher, wenn der Aufwand eines optimalen Brechalgorithmus durch das Polynom n^{10} nach unten und oben begrenzt wäre, während es im kryptographischen Modell dann natürlich als unsicher betrachtet werden müßte.

16 Für konkrete Implementierungen muß natürlich der Sicherheitsparameter und damit die „Größe" der für einen erfolgreichen Angriff zu lösenden Probleme *festgeschrieben* werden. Mangels Kenntnis über brauchbare untere Schranken der verwendeten Probleme muß dies durch „Ausprobieren" geschehen.

17 Eine Softwareimplementierung von RSA entstand z.B. bei der GMD [32], Hardwareimplementierungen von DES bzw. RSA sind in [1, 3] bzw. in [44, 43] beschrieben.

Computer Ripoffs and Foul-Ups: Is Management To Blame?

Alan R. Krull

Abstrakt: *Verbrecher, die sich zu bereichern oder zu rächen versuchen, können großen Schaden stiften, aber ehrliche Mitarbeiter, die unbeabsichtigte Fehler begehen, können möglicherweise noch größere Schäden verursachen. Dazwischen liefern exzentrische Einstellungen zur menschlichen Gesellschaft verschiedenerlei wechselnde Motive. Computer sind üblicherweise gegen diese Gefahren nicht ausreichend geschützt; insbesondere nicht vernetzte Personal Computer. Man muß den Gefahren mit Kontrollen begegnen. Dazu muß der Betreiber erst sein System und diejenigen Personen kennenlernen und überprüfen, die mit dem System umgehen, um danach die erkannten Probleme meistern zu können. Das sind Management-Aufgaben. Dazu gibt es eine Check-Liste von Fragen, auf die man sich Antwort verschaffen sollte.*

1 The Changing Computer Environment

Whatever security exposures we have had in the past have been amplified by the growth in use of micros (personal computers, PCs) and computer communications.

More computing power is now being shipped by manufacturers in the form of micros than in the form of large(r) computers and this has been true for a numbers of years.

The addition of communications to most computers – particularly dialup lines which can "call" from anywhere there is a phone – potentially opens up computers to penetration by anyone with a phone.

There are a host of new users and new applications; processing power is now at everyone's desk. An increasing amount of processing, critical to the conduct of business, takes place under the stewardship of end users.

Data security involves the protection of information against its unauthorized destruction, modification, disclosure or use whether intentional or accidental. And we must also protect our ability to process information in a timely fashion.

The user, the application "owner", is now the de facto "DP manager", with custody of and responsibility for computer-related information assets. There is a "DP shop", a micro, sitting on the desk. We are dependent upon the individual to carry out information asset protection measures.

Control in the end-user environment cannot be as tight as it is for the traditional environment, without losing much of the benefit. We cannot be watching every action of every individual user of DP. We are obliged to trust people a good deal. We must trust them to observe good practices.

2 Crackpots and Scoundrels Attack Planet Earth

Whatever is popular in computer abuse now will no doubt fade; then a new "fad" or cycle will prevail. This parallels our society and its fads and cycles.

Some fads are relatively harmless and not particularly anti-social – flagpole sitting, goldfish eating, cramming the greatest number of people into a small space such as a VW or a phone booth, and streaking – all of these peaked and then faded.