Anonymität in Offline-Münzsystemen

Thomas Demuth
Fachgebiet
Kommunikationssysteme
Universität Hagen
Feithstr.142/TGZ
D-58084 Hagen
thomas.demuth@fernuni-hagen.de

Heike Neumann
Mathematisches Institut
Universität Gießen
Arndtstr. 2
D-35392 Gießen
Heike.B.Neumann@math.uni-giessen.de

24. März 2000

Zusammenfassung

Existierende digitale (Offline-)Münzsysteme sichern dem Kunden Anonymität zu. Diese Form der Anonymität bezieht sich jedoch nur auf die Relation einer digitalen Münze zu einer Person, ausschließlich anhand der Münze kann ihr Besitzer nicht ermittelt werden. Bei diesen Betrachtungen wird jedoch vernachlässigt, daß zum einen bei einer Geschäftsbeziehung Händler und Kunde miteinander bekannt sind und zum anderen einem Münzsystem in der technischen Realisierung ein Kommunikationsnetz (z. Bsp. das Internet) zugrunde liegt, bei dem sich die Kommunikationspartner leicht ermitteln lassen. Dieses Papier stellt ein System vor, das es einem Kunden gestattet, von einem Händler anonym Waren zu beziehen und zu bezahlen. Weiterhin verhindert ein eingesetzter Mechanismus die Aufdeckung der Kommunikationsbeziehung zwischen Kunde und Händler. Das vorgestellte System dient dabei als Grundlage, prinzipiell ist jedes beliebige Offline-Münzsystem integrierbar.

1 Einführung

Bei Betrachtungen von elektronischen Geschäftsprozessen (*Electronic Commerce* oder *ECommerce*) spielt der Schutz des Kunden eine größer werdende Rolle (s. dazu [Fandri96] für einen Vergleich existierender Systeme in puncto Anonymität). War zu Beginn der Entwicklung des ECommerce die Sicherheit des Anbieters einer Ware oder Dienstleistung das primäre Ziel, so bekommt im Sinne einer mehrseitigen Sicherheit die gleichberechtigte Berücksichtigung der Sicherheitsanforderungen aller Beteiligten zunehmend an Gewicht ([MuePfi97])
.

Entwickler von ECommerce-Protokollen behaupten, daß ihre Systeme ,,Anonymität für den Kunden" bieten, sie vereinfachen jedoch dabei die analysierte Situation und vernachlässigen, daß diverse Anforderungen erfüllt sein müssen, um die Anonymität des Kunden zu schützen. Dieses sind u.a.:

- Ein Händler darf die Identität seines Kunden nicht kennen,
- kein Außenstehender darf in der Lage sein, geschäftliche Transaktionen des Kunden zu beobachten und
- die Bank des Kunden darf die Zahlungsvorgänge ihres Kunden nicht nachvollziehen können.

Die aufgeführten Anforderungen sind voneinander unabhängig. So kann ein Kunde ein Pseudonym benutzen, um den Händler über seine wahre Identität im Unklaren zu lassen, jedoch ist es in offenen Netzen leicht möglich, den Weg einer Nachricht zu verfolgen und damit den Absender, in diesem Falle den Kunden, zu ermitteln. Selbst wenn der Kunde ein Pseudonym benutzt und sich bei der Transaktion für die Übermittlung von Nachrichten eines speziellen Mechanismus' bedient, der die Kommunikationsbeziehungz zwischen Teilnehmern verschleiert (z. Bsp. mittels eines sogenannten *Mix-Netzes*), so kann die beteiligte Bank Informationen über den Kunden erlangen, falls ein Zahlungssystem verwendet wird, das identitätsbasiert arbeitet (Kreditkarten- oder Schecksystem). So erscheint es naheliegend und notwendig, verschiedene Mechanismen zu kombinieren, um das Ziel der Anonymität des Kunden zu erhöhen (Zu diesem Schluß kommt auch M. Waidner in [Waidne98]).
Dieses Papier präsentiert ein solches System, das ein Offline-Münzsystem und die Eigenschaften von Mix-Netzen miteinander kombiniert, um die oben erwähnten Nachteile existierender Systeme zu eliminieren (Eine weitere Methode wird in [DaFrTs97] beschrieben). Die politischen oder sozialen Aspekte von Anonymität werden nicht betrachtet, da es in demokratischen Staaten im allgemeinen akzeptiert wird, daß ein Individuum das Recht an seinen eigenen Daten besitzt. Trotzdem darf nicht vernachlässigt werden, daß durch den Einsatz von Verfahren des ECommcere auch der Mißbrauch von Anonymität steigen kann. Die Autoren von [SolNac92] zeigen derartige Möglichkeiten auf.

Das folgende Kapitel beschäftigt sich mit den Grundlagen von Anonymität und entsprechenden Verfahren (Mixen) sowie digitalen Offline-Münzsystemen. In Kapitel 3 wird das eigentliche Verfahren erläutert sowie der Schutz des Kunden analysiert. Zwei mögliche Wege der Aufhebung der Anonymität zeigt Kapitel 4. Mit einer Zusammenfassung in Kapitel 5 schließt dieses Papier.

2 Grundlagen

2.1 Anonymität

2.1.1 Definitionen

In der Literatur werden derzeit unterschiedliche Termini verwendet, um die Eigenschaften kryptologischer Mechanismen in puncto Anonymität zu beschreiben ([Pfitzm90], [ReiRub97], [PfiWai87]). In diesem Artikel werden sie wie folgt verwendet:

Eine Person oder Instanz ist *anonym* in einer Rolle und bzgl. einer Gruppe von n Mitgliedern in Hinsicht auf ein Ereignis, wenn ein Angreifer nur mit der Wahrscheinlichkeit $P = 1/n$ von dem Ereignis auf die Rolle der Person oder Instanz innerhalb der Anonymitätsgruppe schließen kann. Das Ereignis heißt in diesem Fall *unbeobachtbar*.
Stärker noch ist die Anforderung, daß kein Angreifer feststellen kann, ob zwei (oder mehrere) Nachrichten von derselben Person stammen oder zwei (oder mehrere) Ereignisse von derselben Person ausgelöst worden sind. In diesem Falle bezeichnen wir die Nachrichten, bzw. Ereignisse als *unverkettbar*.

Bei *unbedingter Anonymität (Informationstheoretisch sichere Anonymität)* ist die Aufdeckung der Anonymität ist nicht einmal für einen Angreifer mit unbeschränkter Rechenkapazität möglich.
Rechnerische Anonymität (Komplexitätstheoretisch sichere Anonymität) bezeichnet eine Eigenschaft, bei der die Aufdeckung der Anonymität äquivalent zur Berechnung der Lösung eines rechnerisch schweren Problemes (z. Bsp. des diskreten Logarithmus') ist.
Weitere Definitionen der Anonymität sind in [KesBue99] und [KeEgBu98] zu finden.

2.1.2 Anforderungen

Da in dem Szenario einer geschäftlichen Transaktion der Kunde zum einen durch die Nachrichten, die er sendet, bzw. deren Inhalt, und zum anderen durch die Aktionen, die er durchführt (Senden und Empfangen von Nachrichten), identifiziert werden kann, müssen an ein sicheres System folgende Anforderungen gestellt werden:

1. Die Nachrichten, die der Kunde versendet, sind unverfolgbar und unverkettbar. Dieses bedeutet insbesondere, daß die Zahlungen unverfolgbar sein müssen, womit bei dem vorgestellten Verfahren die identitätsbasierten elektronischen Zahlungsysteme ausscheiden, da in diesen die Bank jederzeit Zahlungen verfolgen kann.
   Es werden daher weiterhin ausschließlich digitale Münzsysteme betrachtet.

2. Der Vorgang des Sendens und Empfangens muß unverfolgbar und unverkettbar sein.

2.1.3 Schwächen aktueller Systeme

Obwohl das Kriterium der Unverkettbarkeit wesentlich ist, kann es nicht in jedem Fall erfüllt werden: Falls ein Kunde innerhalb einer Transaktion mit mehr als einer digitalen Münze bezahlt und diese innerhalb eines Protokollschrittes übermittelt, wissen sowohl Händler als auch die Bank, daß diese Münzen denselben Ursprung haben.

Sollte innerhalb des Münzsystemes ein weiteres Gerät zur Speicherung der digitalen Münzen oder privater Informationen eingesetzt werden (z. Bsp. eine *SmartCard*), so besteht eine weitere Gefahr für die Anonymität des Kunden: Das Gerät sollte nicht in der Lage sei, Informationen über geschäftliche Transaktionen zu speichern, da diese, wie bei der *GeldKarte* der deutschen Banken, von jedem Händler ausgelesen werden kann oder aber, bei anderen Systemen, das Gerät nach Nutzungsablauf dem Betrieber zurückgegeben wird [ChaPed93].

Weiterhin sind in den gängigen Münzsystemen sämtliche Parteien (Bank, Kunde, Händler) miteinander bekannt. Einzig die digitale Münze, die vom Kunden an die Bank gesendet wird, ist anonym.

Die geschäftlichen Transaktionen werden in der Regel über offene Netze wie dem Internet abgewickelt. In diesem Falle sind beide Partner untereinander per IP- oder email-Adresse bekannt. Damit zumindest einer der Partner dem anderen gegenüber anonym sein kann, müssen zusätzliche Mechanismen eingesetzt werden.

2.1.4 Motivation

Neben dem Aspekt, daß jedermann die Kontrolle über die Verbreitung seiner persönlichen Daten besitzen sollte, gibt es weitere Argumente und Szenarien, die die Anonymität eines Kunden in bezug auf einen Händler und die Unbeobachtbarkeit von geschäftlichen Transaktionen für Außenstehende motivieren:

- Eine Person möchte eine politische Zeitschrift auf elektronischem Wege beziehen, will aber vermeiden, über seine email-Adresse identifizierbar zu sein. Er muß also eine spezielle Form der Übermittlung wählen.

- Im Jahre 1992 tauchte ein Angebot der Firma Siemens an die koreanische Regierung bezüglich des Hochgeschwindigkeitszuges Transrapid bei der konkurrierenden französischen Herstellerfirma des TGV auf und konnte somit unterboten werden.
  Es wird angenommen, daß diese Firma die Kommunikationswege von Siemens beobachtete und das Angebot abfing ([Hoffma98], [Hartma97]).

2.1.5 Mixe

Die Anforderungen, die sich aus den vorherigen Unterkapiteln herauskristallisiert haben, beschreiben eine Kommunikationsbeziehung zwischen zwei Teilneh-

mern, bei der der Sender gegenüber dem Empfänger anonym bleiben möchte und gleichzeitig diese Beziehung von Außenstehenden nicht erkannt werden kann.

David Chaum zeigt in seinem Grundlagenartikel von 1981 eine Lösung für dieses Problem auf [Chaum81]. Sein Aufsatz beschreibt unter anderem ein System für den Nachrichtenaustausch, das die Verkettung der Endpunkte einer Kommunikationsbeziehung verhindert, so daß die Teilnehmer innerhalb einer Anonymitätsgruppe geschützt sind. Die Nachrichten werden über Zwischenstationen, sogenannte *Mixe*, transportiert. Jeder Mix ist in der Lage, den Weitertransport von Nachrichten zu verzögern, die Reihenfolge eingehender Nachrichten zu vertauschen oder deren Länge zu verändern und gibt die Nachrichten schubweise weiter. Weiterhin kann ein Mix Nachrichtenattrappen erzeugen, falls zu wenige Nachrichten eingehen. Nachrichten werden von einem Mix nur ein einziges Mal weitertransportiert um Wiederholungsangriffe (*replay attacks*) zu vereiteln. In Mix-Netzen passieren die Nachrichten aus Effizienzgründen in der Regel nicht jeden Mix des Netzes. Stattdessen wählt der Sender einer Nachricht einen Weg durch das Netz und codiert seine Nachricht entsprechend. Um die Vertraulichkeit des Inhaltes der Nachrichten zu wahren, werden sie mit einem Public-Key-Verfahren verschlüsselt (meistens RSA).
Seit der Veröffentlichung von Chaums Artikel haben sich Forschungen intensiv mit der Modellierung und Implementierung von Mixen beschäftigt (u.a. [FeJeMu97], [FeJePf97], [FrGrJe98], [Jakobs98]). Im weiteren wird daher nicht weiter auf die reale Umsetzung eines Mix-Netzes eingegangen, die Autoren gehen bei ihren Annahmen von einem funktionsfähigen Mix-Netz aus, das bekannten, in den zuvor erwähnten Veröffentlichungen aufgezeigten, Angriffen gegenüber robust ist.

Zwei Anwendungen des Chaumschen Verfahrens werden durch das vorgestellte Verfahren genutzt:

1. Unverfolgbare email (*untraceable electronic mail*)
   Ein Benutzer eines email-Systemes bereitet eine Nachricht M vor, die er an den Empfänger A_R senden will. Dazu maskiert er die Nachricht mit einer Zufallszahl R_A und signiert sie mit dem öffentlichen Schlüssel P_A des Adressaten. Dann konkateniert er dazu die Adresse A_R sowie eine weitere Zufallszahl R_1, verschlüsselt das Ergebnis mit dem öffentlichen Schlüssel des ersten Mixes der gewählten Route durch das Mix-Netz, P_1, und sendet es diesem.
   Der Mix wendet seinen geheimen Schlüssel S_1 an, erhält die Zahl R_1, die er verwirft, und die Adresse A_R, an die er die innere Nachricht sendet (die aus der mit R_0 verschlüsselten Nachricht M besteht):

   $$P_1(R_1, P_{A_R}(R_0, M), A_R) \rightarrow P_{A_R}(R_0, M)$$

   Zur Erhöhung der Sicherheit durchläuft eine Nachricht in der Regel mehr als einen Mix; bei einer Sequenz von n Mixen ist die Sicherheit selbst bei

Korrumpierung von $n-1$ Mixen zwischen Ein- und Ausgang des Mix-Netzes gewährleistet. Bei Nutzung einer derartigen Route durch das Netz bereitet der Sender die Nachricht derart auf, daß er die oben beschriebene Methode für jeden Mix der Sequenz sukzessive anwendet; in jedem Schritt nutzt er den speziellen öffentlichen Schlüssel des jeweiligen Mixes.

2. Unverfolgbare Rückadressen (*untraceable return addresses*)
   Der Adressat A soll in der Lage sein, auf die so übermittelte Nachricht zu antworten, ohne die wahre Adresse des ursprünglichen Senders zu kennen. Zu diesem Zweck übermittelt der Sender eine unverfolgbare Rückadresse mit einer Nachricht in der oben beschriebenen Form an A_R: $P_1(R_1, A_S), P_S$ mit P_1 und R_1 wie oben, A_S ist die reale Adresse des Senders, P_S ein öffentlicher Schlüssel, den der Sender für diesen Zweck erzeugt. A_R erzeugt seine Nachricht an den Sender:

   $$P_1(R_1, A_S), P_S(R_0, M) \rightarrow A_S, R_1(P_S(R_0, M))$$

   Der erste Mix ist in der Lage, diese Struktur mit seinem geheimen Schlüssel aufzulösen und erhält die Zufallszahl R_1, die er benutzt um den Nachrichtenteil $P_S(R_0, M)$ (symmetrisch) zu verschlüsseln. Dann sendet er das Produkt an A_S, der als einziger Beteiligter den korrespondierenden geheimen Schlüssel kennt und somit die Nachricht dechiffrieren kann.
   Auch diese Methode wird bei Nutzung einer Sequenz von Mixen mehrfach angewendet.

2.2 Elektronische Offline Münzsysteme

Zur Realisierung der Eigenschaften realer Münzen in einem digitalen Umfeld existieren verschiedene Ansätze ([CFN88], [Brands92]). Wie bei realen Münzen müssen Nichtfälschbarkeit, Offline-Überprüfung[1] und Unverfolgbarkeit[2].
Die Nichtfälschbarkeit und Unverfolgbarkeit können durch die Anwendung folgender kryptographischer Mechanismen erreicht werden:

- Die Nichtfälschbarkeit der digitalen Münzen wird durch eine digitale Signatur der Bank garantiert. Keine Partei außer der Bank selbst kann Münzen generieren, jeder andere Beteiligte ist aber in der Lage, die Korrektheit der Münzen zu überprüfen. Da das Fälschen einer Münze ebenso schwierig wie das Brechen des Signaturschemas ist, kann in diesem Punkt von komplexitätstheoretischer Sicherheit ausgegangen werden.

- Um die Unverfolgbarkeit der Münzen zu erreichen, werden sie von der Bank blind signiert, um von dieser nicht identifiziert werden zu können.

[1] Aus Effizienzgründen werden im folgenden ausschließlich Offline-Systeme betrachtet.
[2] Eine weitere typische Eigenschaft realer Münzen, die Übertragbarkeit, kann nur mittels eines erheblichen Effizienzverlustes erzielt werden ([ChaPed92]).

Ein wesentliches Problem von Offline-Münzsystemen ist die Gefahr des doppelten Ausgebens (*double-spending*). Nach dem Abheben einer digitalen Münze kann ein Bankkunde diese beliebig oft vervielfältigen und in verschiedenen Geschäften ausgeben. Zwar kann jeder Händler die Gültigkeit einer digitalen Münze überprüfen, nicht jedoch, ob sie zuvor bereits schon einmal ausgegeben wurde. Da die Münzen selbst bedingungslos anonym in puncto ihres Besitzers sind, kann nicht einmal die Bank feststellen, wer der betrügerische Kunde war.

Eine Lösung für dieses Problem besteht darin, die Identität des Besitzer einer Münze innerhalb dieser in einer Form einzubeziehen, die es der Bank ermöglicht, sie bei *double-spending* zu berechnen ([CFN88]). Mit der Bezahlung einer Ware durch Senden der Münzen an den Händler übermittelt der Kunde also implizit einen Teil seiner Identität. Formal gesehen bedeutet dieses, daß die Bank einen Prüfwert eines verifizierbaren Secret-Sharing-Schemas signiert ([Feldma87]), wobei das aufgeteilte Geheimnis der Identität des Kunden entspricht. „Verifizierbar" bedeutet, daß der Händler (und letztlich auch die Bank) sicher sein können, daß das geteilte Geheimnis korrekt ist.

Um diese Technik zu illustrieren, wird im folgenden das Münzschema von Stefan Brands ([Brands92]) erläutert. Die Sicherheit dieses Verfahrens basiert auf der Schwierigkeit, diskrete Logarithmen zu berechnen.

Es wird dabei angenommen, daß jeder Kunde eine persönliche Identitätsnummer ID besitzt, die sowohl dem Kunden als auch der Bank bekannt ist. G_q sei eine Gruppe der Ordnung q und g ein Generator von G_q, in der Form, daß die Berechnung diskreter Logarithmen in G_q schwer ist. Die Bank veröffentlicht diese Werte G_q und g.

Um seine Identitätsnummer ID aufzuteilen, wählt der Kunde zwei Polynome des Grades eins, das eine, um die maskierte Identitätsnummer (s sei der Maskierungswert), das andere, um den Wert s aufzuteilen:

$$\begin{aligned} f(x) &:= ID \cdot s \cdot x + b_1 \\ g(x) &:= s \cdot x + b_2 \end{aligned}$$

Während des Abhebens einer Münze generieren Bank und Kunde eine blinde Signatur auf dem Tupel $(g^{ID \cdot s}, g^{b_1}, g^s, g^{b_2})$[3] Die Bank erzeugt die blinde Signatur derart, daß sie nichts über die Münze oder die Signatur weiß, außer daß die Münze tatsächlich Teilgeheimnisse der Identitätsnummer des Kunden enthält (s. a. [Brands92]). Eine Münze besteht aus drei Teilen:

- $(g^{ID \cdot s}, g^{b_1})$, eine Festlegung des Teilgeheimnisses der maskierten Identitätsnummer.

[3]Die beiden Polynome werden aus folgendem Grund benötigt: Angenommen, die Identität wird unmaskiert aufgeteilt. Dann enthält jede Münze den Wert g^{ID}, der so von der Bank erkannt werden kann; Anonymität wäre also nicht gegeben. Falls aber auf der anderen Seite der Kunde nicht den Maskierungswert s aufteilt, so kann die Bank zwar nicht ID, aber $s \cdot ID$ berechnen. Daher muß der Kunde sowohl die maskierte ID als auch den Maskierungsfaktor mit je einem Polynom aufteilen.

- (g^s, g^{b_2}), die Festlegung des Maskierungsfaktors.
- Die Signatur sig der Bank, die beide Teilgeheimnissse bestätigt und verbindet.

Im durchzuführenden Protokoll wird die Münze $(g^{ID \cdot s}, g^{b_1}, g^s, g^{b_2}, sig)$ vom Kunden zum Händler übertragen. Dieser verifiziert die Gültigkeit der Signatur der Bank und wählt einen Wert c (*Challenge*). Die Antworten (*Responses*) des Kunden sind die Werte der Polynome an der Stelle c. Der Händler kann die Korrektheit der beiden Teilgeheimnisse wie folgt überprüfen (er hat $f(c)$ und $g(c)$ als Antwort erhalten):

$$\begin{aligned} g^{f(c)} &= (g^{ID \cdot s})^c \cdot g^{b_1} \\ g^{g(c)} &= (g^s)^c \cdot g^{b_2} \end{aligned}$$

$(g^{ID \cdot s}, g^{b_1}, g^s, g^{b_2}, sig)$ repräsentiert den Prüfwert, mit dem der Händler die Korrektheit der Teilgeheimnisse überprüfen kann, ohne Informationen über die gewählten Polynome oder die Identität des Kunden zu erlangen.

3 Vorgehensweise

Das im folgenden beschriebene Protokoll gewährleistet Unbeobachtbarkeit von geschäftlichen Transaktionen sowie die Anonymität eines Kunden gegenüber einem Händler.

3.1 Voraussetzungen

Bei dem vorgestellten Verfahren wird von zwei Voraussetzungen ausgegangen:

1. Von einem Offline-Münzverfahren, das die Unverfolgbarkeit und Unverkettbarkeit von Münzen, aber per se nicht die Anonymität des Kunden gegenüber dem Händlers garantiert.
2. Ein funktionsfähiges Mix-Netz, das in seinen Eigenschaften dem heutigen Stand der Forschung in puncto Sicherheit entspricht (wie u.a. in [Chaum84] und [PfiWai87] beschrieben).

Weiterhin wird davon ausgegangen, daß jeder Kunde bei einer Bank ein Konto besitzt (zur Vereinfachung wird in dem Szenario von einer einzigen Bank ausgegangen).

In der Regel besteht ein Zahlungssystem aus drei Einzelprotokollen:

- Abhebung von Münzen: Der Kunde generiert eine digitale Münze, die er von der Bank signieren läßt (genauer: die Bank signiert blind einen verifizierbaren Teilwert der Identitätsnummer des Kunden (*Secret Sharing*-Verfahren)).

- Geschäftsvorgang zwischen Kunde und Händler: Kunde und Händler führen ein *Challenge-and-Response*-Protokoll durch; der Händler erhält obigen Teil der Identitätsnummer des Kunden.

- Einzahlung der Münzen: Der Händler übermittelt die Münzen und den Teilwert an die Bank.

Jeder Teilnehmer besitzt einen zertifizierten öffentlichen und den korrespondierenden geheimen Schlüssel. Alle Teilnehmer besitzen dieselbe symmetrische Verschlüsselungsfunktion E.

Der Fokus der Betrachtungen liegt auf dem zweiten Einzelprotokoll, dem eigentlichen Geschäftsvorgang zwischen Kunde und Händler, da nur dieser Schritt der vollständigen Anonymität bedarf. Der Vorgang läuft in drei Schritten ab:

1. Der Kunde initialisiert den Vorgang durch eine Angebotsanfrage nach (digitaler) Ware an den Händler. Der Händler reagiert mit einem detaillierten und digital signierten Angebot.

2. Der Kunde bestellt, übermittelt die Münzen; der Händler stellt eine *Challenge*.

3. Der Kunde antwortet mit der entsprechenden *Response* und erhält die Ware, falls diese digital vorliegt, anderenfalls eine überprüfbare Quittung des Händlers.

3.2 Protokollschritte

Die Phase der Bezahlung besteht aus vier Schritten, die im Anschluß detailliert betrachtet werden:

- Initialisierung durch den Kunden (Angebotsanfrage)

- Angeboterstellung des Händlers

- Bestellung (Wahrnehmung des Angebotes/Übergabe der Münzen)

- Auslieferung der Ware

3.2.1 Initialisierung

Der Kunde leitet die gesamte Transaktion durch eine anonyme Anfrage nach einem Angebot ein; es wird gefordert, daß die Nachricht und ihr Transport unverfolgbar sind. Diese Anfrage soll einerseits vertraulich sein, um Beobachtern, rsp. Angreifern, keine Informationen zu liefern, das heißt, sie wird verschlüsselt, auf der anderen Seite soll sie auch anonym und unverfolgbar sein
Zur Notation:
m ist eine Nachricht im Klartext.

M bezeichnet den Händler, C den Kunden.
P_X ist der öffentliche Schlüssel des Teilnehmers X, S_X der korrespondierende geheime Schlüssel.
Adr_x ist die Adresse des Teilnehmers X.
$\{m\}_K$ bezeichnet die Verschlüsselung der Nachricht m mit dem Schlüssel K.

1. Der Kunde wählt eine beliebige Anzahl von Mixen und eine Route aus, die die Nachricht durch die Mixe durchlaufen soll. Diese Mixe werden in der Reihenfolge des Durchlaufens numeriert: $M_1, M_2, \ldots, M_n$.

2. Der Kunde wählt für jeden Mix i, der durchlaufen werden soll, zwei symmetrische Schüssel K_i, K_{2i} $(i = 1, \ldots, n)$, K_i zur Bildung der anonymen Rückadresse und K_{2i} zur Verschlüsselung der Nachricht.
   Würde für diese beiden Operationen ein gemeinsamer Schlüssel verwendet werden, so könnte der Mix anhand dieses Schlüssels eine Zuordnung zwischen Hin- und Rücknachricht feststellen, eine Information, die er nicht kennen muß, um seine Funktion zu erfüllen, aber auch nicht kennen darf, damit er keine Koinzidenz erkennen kann.

3. Um dem Händler eine Antwort zu ermöglichen, muß der Kunde an die Nachricht eine verschlüsselte und damit nicht zurückverfolgbare Rückadresse anhängen[4]. Dazu verschlüsselt er sukzessive seine eigene Adresse: $ara(C) =$

   $$[\{\{\ldots\{Adr_C\}_{K_1}, P_{Mix_1}(K_1), Adr_{Mix_1}\}_{K_2}\ldots\}_{K_n}, P_{Mix_n}(K_n), Adr_{Mix_n}]$$

   ($ara(C) = A$nonyme Rück$a$dresse des Kunden C)

4. Die Klartextnachricht mit der verschlüsselten Rückadresse wird mit einem Sitzungsschlüssel K verschlüsselt, dieser Sitzungsschlüssel wiederum mit dem öffentlichen Schlüssel des Händlers.

5. Der Kunde verschlüsselt sukzessive:

   $$[\{\ldots\{\{anfr_C\}_{K_{2n}}, P_{Mix_n}(K_{2n}), Adr_{Mix_n}\}_{K_{2n-1}}\ldots\}_{K_2}, P_{Mix_1}(K_2)]$$

   mit $anfr_C = [\{ara(C), m\}_K, P_M(K), Adr_M]$ als Anfrage des Kunden.
   Diesen Datensatz schickt der Kunde an den ersten Mix.

Der erste Mix kann dann zunächst seinen Sitzungsschlüssel K_1 entschlüsseln und erhält dadurch die Adresse des zweiten Mixes und eine neue verschlüsselte Nachricht. Auf diese Weise erhält jeder Mix die Adresse seines Nachfolgers sowie eine neue chiffrierte Nachricht und kann diese somit weiterleiten. Der letzte Mix entschlüsselt die Adresse des Händlers und sendet ihm die verbliebene Nachricht zu. Der Händler kann seinen Sitzungsschlüssel und damit die Nachricht entschlüsseln.

[4]Damit ist die Identität des Kunden gegenüber dem Händler anonym in dem Sinne, daß die Rückadresse für letzteren keinen Aufschluß über den Kunden gibt.

3.2.2 Angebotserstellung

Der Händler stellt sein Angebot für den Kunden zusammen, er generiert eine neue Klartextnachricht m_1. Sollte der Kunde auf dieses Angebot eingehen wollen, so muß der Händler dieses als Reaktion auf sein Angebot identifizieren können und versieht es dazu mit einer Identitätsnummer *id*. Angebote müssen nach gesetzlicher Festlegung für einen gewissen Zeitraum gültig sein[5]. Für diese Verbindlichkeit versieht er es mit einem Zeitstempel zs.

$$[ang = \{id, m_1, zs, S_M(hash(id, m_1, zs))\}_K]$$

Selbst wenn der Händler sein Angebot weder mit einem Zeitstempel versehen noch signieren würde, so gewährte der wiederverwendete Sitzungsschlüssel K die Authentizität der Nachricht; der Kunde kann somit sicher sein, daß kein Wiederholungsangriff stattgefunden hat.

Damit erhält der letzte Mix der gewählten Sequenz vom Händler die folgende Nachricht:

$$[\{\ldots\{\{Adr_C\}_{K_1}, P_{Mix_1}(K_1), Adr_{Mix_1}\}_{K_2}\ldots\}_{K_n}, P_{Mix_n}(K_n), Adr_{Mix_n}, \{ang\}_K]$$

Der Mix kann den Sitzungsschlüssel K_n berechnen und damit die Adresse des nächsten Mixes bestimmen. Um auch die Nachricht $\{ang\}_K$ zu verändern, verschlüsselt er sie mit seinem Sitzungsschlüssel K_n. Das Chiffrat sendet er an den nächsten Mix.

Der erste Mix der Sequenz, der logisch dem Kunden am nächsten liegt, sendet dem Kunden:

$$[\{\ldots\{\{ang\}_K\}_{K_{n-1}}\}\ldots\}_{K_1}]$$

Da dem Kunden alle verwendeten Sitzungsschlüssel bekannt sind (er hat sie selbst generiert), kann er das Angebot des Händler entschlüsseln.

3.2.3 Bestellung und Auslieferung der Ware

Diese beiden Schritte werden methodisch äquivalent zum ersten (Anfrage) und zum zweiten (Angebotsübermittlung) durchgeführt. Der Kunde generiert erneut $2n$ symmetrische Schlüssel und einen neuen Sitzungsschlüssel K'. Er benutzt nicht erneut dieselben Schlüssel, da dadurch eine Verbindung zwischen verschiedenen Transaktionen erzeugt werden könnte.
Der Händler sendet die Ware (falls digital) oder eine verbindliche Quittung auf demselben Wege wie sein Angebot an den Kunden.

3.3 Analyse

Zu untersuchen ist die Anonymität des Kunden. Der Kunde signiert keine Nachricht und hinterläßt (mit Ausnahme bei der Erzeugung der Münzen) keine

[5] Zumindest nach deutscher Gesetzgebung.

persönlichen Informationen. Weiterhin sind nach Voraussetzungen die Münzen unverfolgbar, so daß geschlossen werden kann, daß auch die Nachrichten unverfolgbar sind. Für die meisten bekannten Münzsysteme ist die Unverfolgbarkeit berechenbar; beispielsweise ist sie in dem System von Brands ([Brands92]) äquivalent zur Berechnung des diskreten Logarithmus'. Jedoch sind dort die Nachrichten nicht unverkettbar, da eine Transaktionsnummer verwendet wird.

Die übermittelten Nachrichten selbst sind unbeobachtbar unter der Annahme, daß in einem Mix-Netz mindestens ein korrekt arbeitender Mix existiert. Die Unbeobachtbarkeit ist nicht unbedingt, sondern berechenbar, da sie auf der Sicherheit des verwendeten Verschlüsselungsverfahrens basiert.

Die Mixe sind nicht in der Lage, Anfragen und Antworten zu verbinden, da der Kunde unterschiedliche Schlüssel für jeden Pfad durch das Mix-Netz wählt. Dieses bedeutet, daß außer dem Händler niemand diese Nachrichten verknüpfen kann.

Als Schluß aus diesen Feststellungen resultiert, daß für den Kunden komplexitätstheoretisch sichere Anonymität gilt.

4 Aufhebung der Anonymität

In dem oben präsentierten System existieren zwei Möglichkeiten, die Anonymität eines Kunden aufzuheben: Auf der einen Seite kann die Unbeobachtbarkeit des Kommunikationskanales aufgehoben werden, auf der anderen Seite kann ein Verweis auf die Identität des Kunden in die Münze aufgenommen werden (über jenen hinaus, der das doppelte Ausgeben einer Münze verfolgen läßt); dieser Verweis könnte ausschließlich durch eine dritte, vertrauenswürdige Instanz (*Trusted Third Party, TTP*) verfolgt werden (s. a. [StPiCa95]). Münzsysteme, die diese Eigenschaft besitzen, werden auch als „fair" bezeichnet.

4.1 Fairness durch überprüfbare Verschlüsselung

Eine einfache, aber trotzdem elegante Lösung, um einen verdeckten Verweis in die Münze mit aufzunehmen, ist die überprüfbare Verschlüsselung des homomorph Inversen ([AsShWa98]), hier anhand des diskreten Logarithmus' demonstriert. G_q sei eine Gruppe der Ordnung q und g ein Generator, so daß es schwer isst, den diskreten Logarithmus in G_q zu berechnen. Der Teilnehmer A hat $y := g^x$ veröffentlicht und hält x geheim. x ist das homomorph Inverse von g^x, wobei die diskrete Exponentialfunktion der entsprechende Homomorphismus in G_q ist. A sendet Daten an B und will B überzeugen, daß dieser damit ausreichend Informationen besitzt, daß eine von B eingeschaltete TTP den Wert x berechnen kann. Die TTP veröffentlicht ein asymmetrische Verschlüsselungsschema, daß sicher gegenüber adaptiven Klartextangriffen (*Chosen-Plaintext-Attack*) ist; der Verschlüsselungsalgorithmus wird mit $E(\cdot, \cdot)$ bezeichnet. Um

eine Nachricht m zu verschlüsseln, wählt die TTP eine Zufallszahl r und berechnet $E(r, m)$. Weiterhin publiziert sie zwei Hash-Funktionen h_1 und h_2:

$$\begin{aligned} h_1 &: \Sigma^n \to \{0,1\} \times G_q \\ h_2 &: \text{ bildet } range(E) \times Z_q \text{ auf eine kurze Zeichenkette ab} \end{aligned}$$

Sei N die Sicherheit der als *Cut-and-Choose* bezeichneten Prozedur[6]. Die folgenden Schritte werden parallel für $i = 1, \ldots, N$ ausgeführt:

- A wählt zufällig $w \in \{0,1\}^l$, berechnet $(u, v) := h_1(w)$ und überträgt $b := h_2(E(u, v), g^v)$ an B.
- B wählt ein $c \in \{0, 1\}$ als Prüfwert (*Challenge*).
- Falls $c = 0$ ist, sendet A den Wert w an B. Anderenfalls wird von A der Wert $\epsilon := E(u, v)$ und $w' := v + x \, mod \, q$ gesendet.
- Falls $c = 0$ ist, berechnet B das Paar $(u', v') := h_1(w)$ und prüft, ob $b \stackrel{?}{=} h_2(E(u', v'), g^{v'})$. Anderenfalls prüft B, ob $b \stackrel{?}{=} h_2(\epsilon, g^{w'} \cdot y^{-1})$.

B sollte den Wert 1 zumindest einmal wählen, da er sonst nichts über das Geheimnis erfährt. Falls B nun seine Informationen über A an die TTP sendet, kann diese x mit einer hohen Wahrscheinlichkeit berechnen. In einem Münzsystem kann die überprüfbare Verschlüsselung nun wie folgt verwendet werden: Der Kunde sendet $(g^{ID \cdot s}, g^{b_1}, g^s, g^{b_2}, sig)$ an den Händler. Dieser überprüft die Signatur und erhält so durch das *Challenge-and-Response*-Protokoll ein Teilgeheimnis der maskierten Identität und des Maskierungsfaktors. Da $ID \cdot s$ und s die homomorph Inversen zu $g^{ID \cdot s}$ und g^s sind, kann eine überprüfbare Verschlüsselung von $ID \cdot s$ und s durchgeführt werden. Dieses bedeutet, daß der Händler mit hoher Wahrscheinlichkeit ausreichend Informationen erhält, um die TTP zu befähigen, $ID \cdot s$ und s zu ermitteln. Diese kann daraufhin die Anonymität des Kunden aufheben.

4.2 Aufhebung der Unverfolgbarkeit

Ein weiterer Weg, die Anonymität des Kunden aufzuheben, besteht darin, den Weg, den die Nachrichten und damit auch die Münzen durch das Mix-Netz nehmen, aufzudecken. Falls die TTP von einem klagenden Händler die Daten des ausgeführten Protokolles erhält, kann sie die beteiligten Mixe auffordern, die korrespondierenden Sitzungsschlüssel zu entschlüsseln, damit der Weg der Nachrichten bis zum Kunden nachverfolgt werden kann. Diese Möglichkeit ist ein spezieller Vorteil des oben beschriebenen Verfahrens: Die Mixe müssen nicht ihre privaten Schlüssel aufdecken, es reicht aus, die Sitzungsschlüssel zu entschlüsseln.

[6] Die Wahrscheinlichkeit, daß ein ehrlicher Überprüfer betrogen wird, liegt bei ungefähr 2^{-N}.

5 Zusammenfassung

In diesem Papier wurden die Nachteile von ECommerce-Protokollen betrachtet, die als Eigenschaft die „Anonymität für den Kunden" angeben. Das Problem dieser Systeme liegt jedoch in der Umgebung, in der sie ablaufen. Die Basis für die Transaktionen sind Netze, speziell das Internet; in solchen Netzen sind die Kommunikationspartner jedoch per se nicht unbekannt.
Weiterhin wurde der Begriff der Anonymität spezifiziert und ein System für Offline-Münzsysteme vorgestellt, das obigen Nachteil eliminiert.

Die Autoren danken dem Fachbereich Kommunikationssysteme unter der Leitung von Prof. Dr.-Ing. Firoz Kaderali und speziell Prof. Dr. rer. nat. Werner Poguntke für die Unterstützung.

Literatur

[AsShWa98] N. Asokan, V. Shoup, M. Waidner, ,,Optimistic fair exchange of digital signatures" Advances in Cryptology - EuroCrypt 98, Lecture Notes in Computer Science, Springer-Verlag

[Brands92] S. Brands, ,,Untraceable off-line cash in wallets with observers" Advances in Cryptology - EuroCrypt 93, Lecture Notes in Computer Science, Springer-Verlag

[CFN88] Chaum, Fiat, Naor, ,,Untraceable electronic cash" Advances in Cryptology - Crypto 88, Lecture Notes in Computer Science, Springer-Verlag

[ChaPed92] D. Chaum, T. Pedersen, ,,Transferred cash grows in size" Advances in Cryptology - EuroCrypt 92, Lecture Notes in Computer Science, Springer-Verlag

[ChaPed93] D. Chaum, T. Pedersen, ,,Improved Privacy in Wallets with Observer" Advances in Cryptology - EuroCrypt 93, Lecture Notes in Computer Science, no. 765, Springer-Verlag

[Chaum81] D. Chaum, ,,Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" Communications of the ACM, February 1981, Vol. 24, No. 2

[Chaum84] D. Chaum, ,,A New Paradigm for Individuals in the Information Age" 1983 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, pp. 99-103

[DaFrTs97] G. Davida, Y. Frankel, Y. Tsiounis, M. Yung, ,,Anonymity Control in E-Cash Systems" Financial Cryptography 97, pp. 1-16

[Fandri96] D. Fandrich, ,,How private are "private" electronic payment systems?" http://www.npsnet.com/danf/emoney-anon.html

[Feldma87] P. Feldman, ,,A practical scheme for non-interactive verifiable secret sharing", Proc. of the 28. th IEEE Symposium on Foundations of Computer Science (FOCS), 1987

[FeJeMu97] H. Federrath, A. Jerichow, J. Müller, A. Pfitzmann, ,,Unbeobachtbarkeit in Kommunikationsnetzen", VIS97 - Verlässliche Informationssysteme, 1997, pp. 191-210

[FeJePf97] E. Franz, A. Jerichow, A. Pfitzmann, ,,Systematisierung und Modellierung von Mixen", VIS97 - Verlässliche Informationssysteme, 1997, pp. 171-190

[FrGrJe98] E. Franz, A. Graubner, A. Jerichow, A. Pfitzmann, ,,Modelling mix-mediated anonymous communication and preventing pool-mode attacks", Global IT Security, Proceedings of the XV IFIP World Computer Congress, 1998, pp. 554-560

[Hartma97] S. Hartmann, ,,Vernetzung bietet Spionen neue Wege", Die Welt, 11.11.1997

[Hoffma98] W. Hoffmann, ,,Leichtes Spiel", Die Zeit, 28/1998

[Jakobs98] M. Jakobsson, ,,A Practical Mix", Advances in Cryptology - EuroCrypt 98, Lecture Notes in Computer Science, no. 1403, Springer-Verlag

[KesBue99] D. Kesdogan, R. Büschkes, ,,Klassifizierung von Anonymisierungstechniken", Konferenz Sicherheitsinfrastrukturen 1999, pp. 321-332, Vieweg

[KeEgBu98] D. Kesdogan, J. Egner, R. Büschkes, ,,Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System", Information Hiding, pp. 83-98, Springer, 1998

[MuePfi97] G. Müller, A. Pfitzmann, ,,Mehrseitige Sicherheit in der Kommunikationstechnik", Addison-Wesley, 1997

[Pfitzm90] A. Pfitzmann, ,,Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz", Informatik-Fachberichte 234, Springer-Verlag, 1990

[PfiWai87] A. Pfitzmann, M. Waidner, ,,Networks without User Observability", Computer & Security, Vol. 6 (1987), pp. 158-166

[ReiRub97] M. Reiter, A. Rubin, ,,Crowds: Anonymity for Web Transactions", DIMACS Technical Report 97-15, AT&T Labs-Research, April 1997

[SolNac92] S. von Solms, D. Naccache, ,,Blind Signatures and perfect crimes", Computer & Security, Vol. 11 (1992), pp. 581-583

[StPiCa95] M. Stadler, J.-M. Piveteau, J. Camenisch, ,,Fair blind signatures" Advances in Cryptology - EuroCrypt 95, Lecture Notes in Computer Science, Springer-Verlag

[Waidne98] M. Waidner, ,,Open Issues in Secure Electronic Commerce", IBM Research Report 93116, October 1998