Fail-stop-Signaturen und ihre Anwendung

Birgit Pfitzmann, Michael Waidner

Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe
Postfach 6980, D-W7500 Karlsruhe 1, Bundesrepublik Deutschland

Kurzfassung: Die Unfälschbarkeit konventioneller digitaler Signaturen beruht zwangsläufig auf komplexitätstheoretischen Annahmen, d.h. selbst die sichersten Systeme können durch einen unerwartet mächtigen Angreifer gebrochen werden. Daher führen wir Fail-stop-Signaturen ein: Sie sind so unfälschbar wie die besten konventionellen Signaturen, aber wenn doch eine Signatur gefälscht wird, kann der angebliche Unterzeichner unbedingt (d.h. ohne jegliche Annahmen) die Fälschung beweisen, mit beliebig hoher Wahrscheinlichkeit.

Wir konstruieren konkrete Fail-stop-Signatursysteme, die sogenannten Versteckssysteme, aus beliebigen kollisionsfreien Paaren von Permutationen. Als Spezialfall ergibt sich ein relativ praktikables System, in dem Fälschen so schwer ist wie Faktorisierung.

Ausführlich werden Anwendungen in digitalen Zahlungssystemen betrachtet, auf Anwendungen auf zuverlässige Verteilung wird verwiesen.

1 Einleitung

Motivation: Digitale Signaturen sind ein wichtiger kryptograhischer Grundbaustein für sichere Systeme [DiHe_76]. Sie sind dadurch gekennzeichnet, daß der Empfänger einer Signatur jeden beliebigen Dritten von ihrer Gültigkeit überzeugen kann (im Gegensatz zu Authentikationscodes [GiMS_74], wo der Empfänger nur für sich selbst sicher ist, daß eine Nachricht vom behaupteten Unterzeichner stammt). Deswegen sind sie insbesondere in allen Anwendungen nötig, wo Rechtssicherheit herrschen soll, d.h. unterschriebene Nachrichten evtl. einem Gericht vorgelegt werden müssen, z.B. in digitalen Zahlungssystemen.

Die Sicherheit digitaler Signaturen hat in letzter Zeit einige Aufmerksamkeit erfahren, denn das bekannteste System RSA [RSA_78] ist bekanntlich in reiner Form sehr anfällig gegen aktive Angriffe (d.h. im wesentlichen das Bilden neuer Signaturen aus vorher erhaltenen, ohne den eigentlichen Schlüssel zu brechen) (s. z.B. [Denn_84]), so daß z.B. zu Redundanzprädikaten gegriffen werden muß, über deren Sicherheit noch weniger bekannt ist als über RSA selbst [DaPr_85, EkHV_88, Gira_88, JoCh_86]. Gleiches gilt für das System aus [Elga_85], s. [GoMR_88]. Manche anderen Systeme wurden ganz gebrochen (s. z.B. [Odly_84, EAKM_86, BrDe_86]).

In [GoMR_88] wurde daher die optimale Sicherheit für (konventionelle) digitale Signatursysteme definiert und Systeme mit dieser Sicherheit konstruiert. Mit **„konventionelles Signatursystem"** bezeichnen wir eines gemäß dieser Definition (darunter fällt auch RSA mit Redundanzprädikat, nur ist eben seine Sicherheit bisher nicht bewiesen). Insbesondere veröffentlicht jeder Teilnehmer einen öffentlichen Schlüssel $\ddot{O}$, und ein S gilt als seine Signatur unter eine Nachricht N genau dann, wenn es einen Test $test(\ddot{O}, N, S)$ besteht. Dies impliziert, daß das Fälschen von Signaturen komplexitätstheoretisch innerhalb von NP liegt.

Darüber hinaus beruhen alle bekannten Signatursysteme auf allgemein für richtig gehaltenen, aber unbewiesenen komplexitätstheoretischen Annahmen. Der ursprüngliche Vorschlag aus [GoMR_88], GMR genannt, beruht auf der Existenz kollisionsfreier Paare von (Einweg-)Permutationen mit Falltür (claw-free pairs of trap-door permutations). Diese Annahme konnte zunächst auf beliebige Falltür-Einweg-Funktionen (trap-door one-way functions) abgeschwächt werden [BeMi_88], später auf beliebige Einweg-Funktionen [NaYu_89]. Um Signaturen praktisch zu verwenden, muß man eine spezielle Funktion auswählen und

A. Pfitzmann et al. (eds.), *VIS '91 Verläßliche Informationssysteme*

hoffen, daß sie die Einweg-Eigenschaft besitzt. Meist nimmt man die Schwierigkeit des Faktorisierens oder des diskreten Logarithmus in gewissen Gruppen an. (Das effizienteste System ist immer noch der auf Faktorisierung beruhende Spezialfall von GMR aus [GoMR_88]. Sein Aufwand ist vergleichbar mit dem von RSA.)

Fail-stop-Signaturen verbessern die Sicherheit auf andere Weise: Sie ermöglichen es angeblichen Unterzeichnern unbedingt (d.h. ohne jegliche Annahme, nicht einmal die, daß Angreifer nur polynomiale Algorithmen ausführen können), Fälschungen zu beweisen (mit beliebig hoher Wahrscheinlichkeit). Vorteile sind:

- Sobald eine Fälschung auftritt, kann das Signatursystem abgebrochen oder der Sicherheitsparameter erhöht werden.
- Das Risiko gefälschter Signaturen kann beliebig aufgeteilt werden. Meist wird man festlegen, daß eine Signatur ungültig wird, sobald ein Fälschungsbeweis gezeigt wird. Dann sind die Unterzeichner unbedingt sicher.

Wir fordern auch, daß unter kryptographischen Annahmen Fälschungen überhaupt nicht auftreten können, und Unterzeichner nicht fälschlich behaupten können, eine Fälschung sei aufgetreten. Somit ist die Sicherheitsdefinition von Fail-stop-Signaturen echt stärker als die eines konventionellen Signatursystems.

ANMERKUNGEN: Es gab Vorschläge für konventionelle Signaturen, die besagten, daß Unterzeichner ja merken, wenn ihre Signaturen gefälscht werden, oder auch wenn sie ihre geheimen Schlüssel verlieren, und daß sie in diesen Fällen das Signatursystem abbrechen dürfen. Dies würde jedoch vollständige Unsicherheit für die Empfänger von Signaturen bedeuten, da ein Unterzeichner einfach behaupten könnte, eine Fälschung sei aufgetreten, um eine lästig gewordene Signatur abzuleugnen.

Fail-stop-Signaturen haben zusätzliche praktische Vorteile in öffentlichen Anwendungen wie Zahlungssystemen: Erstens ist es zweifelhaft, ob man Personen verpflichten könnte, an Systemen teilzunehmen, wo sie sich auf kryptographische Annahmen verlassen müssen, dazu i.allg. mit Sicherheitsparametern, die sie nicht selbst wählen dürfen. Benutzt man Fail-stop-Signaturen und konventionelle Signaturen zusammen (s. Kap. 3), so kann man den Kunden solcher Systeme unbedingte Sicherheit garantieren.

Zweitens könnten bei konventionellen Signaturen selbst dann, wenn die kryptographischen Annahmen zutreffen, Kunden unwiderlegbar behaupten, ihre Signatur sei gefälscht worden, was beträchtliche öffentliche Unsicherheit auslösen könnte.

Verwandte Arbeiten: Parallel zu dieser Arbeit wurden „unbedingt sichere Signaturen" („unconditionally secure signatures") entwickelt [ChRo_90]. Dies ist eine vorzügliche Idee, aber diese Signaturen unterscheiden sich ziemlich von konventionellen: Jeder Teilnehmer hat eine andere Testfunktion für Signaturen, und sie hängt zusätzlich davon ab, entlang wievieler Vorgänger eine Signatur empfangen wurde (d.h. ob direkt vom Unterzeichner, ob vom ersten Empfänger usw.). Zudem sind aktive Angriffe auf Empfänger möglich. Deswegen können unbedingt sichere Signaturen, im Gegensatz zu Fail-stop-Signaturen, nur in speziellen Protokollen eingesetzt werden, wo jeder Empfänger die Anzahl seiner Vorgänger kennt und wo aktive Angriffe auf Empfänger eingeschränkt werden. Das Hauptsystem aus [ChRo_90] entspricht dem Fall mit nur einem beabsichtigten Empfänger bei Fail-stop-Signaturen (s. Kap. 2). Es ist bisher nicht bekannt, wie lang die Signaturen im allgemeinen Fall sein müssen. (Die Maßnahmen aus [ChRo_90, Kap. 5] helfen nur, wenn man sicher ist, daß der Unterzeichner ehrlich ist.) In vielen Fällen werden Fail-stop-Signaturen effizienter sein als unbedingt sichere Signaturen. Zudem ist der Schlüsselaustausch für unbedingt sichere Signaturen ein komplexes Protokoll.

Eine genaue Sicherheitsdefinition und der Beweis unserer Fail-stop-Signaturen finden sich in [Pfit_89, PfWa_90], unsere BA-Protokolle (und ein erstes, aber ineffizientes Fail-stop-Signatursystem) in [WaPf_89, PfWa1_91]. Ein spezieller Aspekt der Schlüsselerzeugung wurde in [Bleu_90, BlPW_90] diskutiert.